DM 56 RS GP

Efficiently Boost Up Your Entrance Management

Hikvision Smart Parking Lot Solution is A Perfect System for Productivity and Parking Security

With the help of Hikvision Automatic Number Plate Recognition (ANPR) technology being employed at the vehicle entrance gate, the smart parking lot system can recognize and analyze license plate numbers. It also helps security teams to systematically manage videos and locate individual vehicles in a given period of time, greatly accelerating post-event investigation. The system integrates Smart IP cameras, NVRs, and video management software, providing around-the-clock protection for parking lots.

- Smart detection
- Low-Light performance
- Comprehensive management
See Farther than the Others

A Detail-Oriented Camera: 2MP 36x Optical Zoom

See your world up close like never before with the 36x optical zoom. Your dimly lit environment is no longer a problem. The new 2MP 36x ultra-low-light smart PTZ camera from Hikvision captures rich, colorful, high-quality images — even in the dark. This advanced PTZ camera, which already comes equipped with a wide spectrum of smart features, boasts 2MP real-time resolution and picks up fine details over expansive areas thanks to a 36x optical zoom day/night lens. Improve security efficiency and see your world up close like never before with Hikvision’s latest smart PTZ camera.
REGULARS

04 From the editor’s desk
06 Calendar of events
08 News & events
15 Training & education
54 System integrators’ profiles
63 IT infrastructure in security
67 Fire & safety
71 Cyber security
73 Access control & identity management
78 CCTV, surveillance & remote monitoring
83 Product news

FEATURES

Opinion: The changing nature of CCTV surveillance and the demands of crisis handling 16
Dr Craig Donald looks at the challenges managers and staff in surveillance control rooms are facing.

Employee verification 20
Employee verification covers a lot of ground as it confirms people’s identities, qualifications and more, but perhaps it’s time to look a bit deeper.

Sector focus: Security in the financial industry 26
The use of security solutions can extend beyond security in financial organisations.

Fraud prevention in the workplace 30
Increased screening solutions incorporate a variety of methods and processes.

Securex 2017 Preview 34
Hi-Tech Security Solutions lists a few of the 2017 exhibitors and what they will be doing at Securex.

Intelligent intruder detection & perimeter security 58
What systems are there to keep criminals in check, whether for a home or a large, open environment?
Now Available over COAX
Leading end-to-end 4K Ultra HD over Coax

- 4K Box Camera: superior clarity with Starlight+ 4/3” sensor
- 4K Bullet and Dome Cameras: 100m/50m IR distance, IP67 & IK10 compliant
- 4K Multi-sensor Camera: 180° panoramic view & 3x2MP image simultaneously
- 4K Fisheye Camera: 360° panoramic view, 10 modes dewarping with HCVR
- HCVR: backward compatible with existing HDCVI cameras, protect your investment
- Up to 500m transmission over RG59 & 300m over CAT5e, realizing seamless upgrade

HAC-HFW3802E-Z
4K HDCVI WDR IR-Bullet Camera

HAC-PFW3601-A180
4K HDCVI Multi-sensor Panoramic IR-Bullet Camera

HAC-EBW3802
4K HDCVI IR-Fisheye Camera

HAC-HDBW3802E-Z
4K HDCVI WDR IR-Dome Camera

HCVR7000
4K HDCVI Recorder

DAHUA TECHNOLOGY SOUTH AFRICA (PTY) LTD
21 Woodlands Drive, Woodmead, JNB, ZA
E-mail: fritz.wang@global.dahuatech.com
http://www.dahuasecurity.com
Never too old to learn

In this issue of Hi-Tech Security Solutions we look at employee verification, but go a bit further into what employers are doing these days when it comes to making employment decisions. One thing that is fast becoming standard is social media vetting.

In the article on employee verification, readers will gain a little insight into what real social media vetting is about. I was surprised when the company mentioned (Farosian, which partners with iFacts) did a profile on me. With scant information about me, I received a report of over 20 pages.

The results show I’m a low-risk hire so let the offers roll in. Or it could mean that I’m just good at hiding the facts. . . What the report showed me was how open and transparent all social media sites are. My exposure to the physical and virtual security worlds have left me a touch paranoid so my profiles are reasonably secure, without being inaccessible. What that really means is that they are not secure at all.

It doesn’t matter how secure you think you have made your social media, if you’re linking and interacting with other people, you’re an open book without really knowing who you really are – according to Facebook, Twitter and all the other sites. Virtually every process that is so simple and fast you can expect from them at the show. As is always the case, there is too much information and too few pages so we couldn’t include everyone and everything in the preview.

Another vetting process is behavioural vetting which determines the kind of person you are and whether you would fit into a particular job and culture. In itself, behavioural analysis is nothing new, but the company responsible, PDA-Africa, has a process that is so simple and fast you wonder what they would be able to find about you. Again, there’s a surprise in store when you receive the report. In my experience it was unnervingly accurate. You can even get an automated voice to talk you through the results.

So no matter how right you think you are, expressing an opinion on social media could be the worst thing you do as it can come back to haunt you years later – free speech be damned.

On a more security-related note, this issue once again sees our annual ‘Securex Preview’. We have a bunch of pages with snippets from many of the exhibitors, telling you what you can expect from them at the show. As is always the case, there is too much information and too few pages so we couldn’t include everyone and everything in the preview.

Nevertheless, we hope you enjoy the preview and the magazine as a whole, and for those attending Securex, we hope you enjoy the show. For those exhibiting or speaking at the event, Hi-Tech Security Solutions wishes you all the best. Be sure to stop by our stand!

Andrew
TALK EVERYWHERE!!

- Stun Revive Facility
- Extended Battery Life
- Private Calls
- Group Calls
- Voice recording
- Global Positioning System
- Dispatcher
- Unlimited Coverage

SMART PTT RADIO
SS 388

CONTACT DEON SWANEPOEL
- Tel: +27 (0)12 997 7107 • deon@halotechnology.co.za
- www.halotechnology.co.za
- Address: 568 Melkbos Str, Moreleta Park, Pretoria, South Africa
CALENDAR OF EVENTS

EXHIBITIONS, CONFERENCES, SPECIALISED EVENTS

Events

IoTAS & Smart Expo 2017
24-25 May 2017
Johannesburg
The second Internet of Things Africa Summit & Smart Expo will discuss will discuss the local, regional and global state of the industry with its progress, challenges and outlook.
For more information contact Clever Soko, +27 (0)61 923 1466, register@iotafricasummit.net, www.iotafricasummit.net.

Securex 2017
30 May -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 6 000 visitors and over 160 exhibitors representing 13 countries.

ESDA member breakfast
30 May 2017: 07.30
Securex 2017: Gallagher Convention Centre, Midrand
The legal and reputational risks of social media. Presented by Emma Sadleir, media law consultant based in Johannesburg. Emma’s areas of expertise include all aspects of print and electronic media law, with a particular focus on defamation, privacy and social media law. This prestigious, free of charge event is exclusively for ESDA members. Book now as space is limited and seats are reserved on a first-come first-served basis.
To book, contact shirley@esda.org.za.

ESDA 2017 Charity Golf Day
6 September 2017
Glendower Golf Course
The ESDA 2017 Charity Golf Day will be held at the Glendower Golf Course on 6 September 2017.
For further information or to book a 4-ball contact shirley@esda.org.za.

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.

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 3 to 6 September 2017.
For more information on the full programme, go to www.camprosa.co.za.

ESDA 2017 Charity Golf Day
6 September 2017
Glendower Golf Course
The ESDA 2017 Charity Golf Day will be held at the Glendower Golf Course on 6 September 2017.
For further information or to book a 4-ball contact shirley@esda.org.za.

iLegal 2017
14 September 2017
Johannesburg
Hosted by Hi-Tech Security Solutions in association with Dr Craig Donald, iLegal is back in 2017, better than ever before. Keep an eye out for more information in future editions of Hi-Tech Security Solutions.
For details contact Dominique on +27 (0)11 543 5800 or dominique@technews.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
EXTREME SERIES
Access & Time fingerprint terminal for harsh operating conditions

Safran Identity & Security is a global leader in identity and security solutions, deploying solutions in more than 100 countries. Backed by more than 40 years of experience in biometrics, we develop innovative technologies for a wide range of markets and applications for people, governments and business.

safran-identity-security.com

@SafranIDSec

SAFRAN
April 2017 saw the international launch of Morpho’s (or Safran Identity & Security’s) MorphoAccess SIGMA Extreme. Morpho SA’s Paul Jeremias also took the opportunity to speak about the future of the company following its acquisition by Advent International.

Taking over from the successful Outdoor MorphoAccess range, the Extreme has been designed for use in the most rugged environments and is rated IP66 to protect it from the elements, as well as IK09 to ensure it can handle rough treatment.

Speaking on the product, the company’s Nicolas Garcia said the Sigma Extreme’s polycarbonate housing made it a tough device able to withstand UV and weathering, as well as vandalism. This includes the capacitive touch screen, which is unharmed when a 500 g steel ball is dropped on it from a height of 2 m.

To cater for damaged fingerprints or potential dirt on individual’s fingers when using the scanner, the Extreme sports a 23 mm x 23 mm optical sensor, which the company says is the biggest on the market. The sensor is FBI PIC IQS certified. The Extreme also includes a loudspeaker in case instructions need to be given to users in noisy environments and a microphone, allowing for 2-way communication.

In cases where additional security is required, the system can also include a camera. This will allow companies to set up the system to only recognise a fingerprint if someone is standing in front of the reader, or it can be used for situational awareness as a control room can access the camera to view a situation at an entrance, for example. The Extreme can also be used as an IP videophone.

A full web server is also onboard. This will allow administrators to connect to the device directly to set it up, enrol fingerprints or access transactional logs. The Extreme can also be set up remotely from a central server. Morpho has also made it easy to integrate the product into existing access or time-and-attendance scenarios with various software options.

For organisations still using card access, either as stand-alone or multi-factor security solutions, the Extreme has the option to use a variety of contactless cards as well. The card options include Prox, iClass, MiFare/DESFire/NFC.

Opportunities ahead

Jeremias addressed the future of the company briefly in light of the news last year that Advent International was going to be the new owner after its 2.4 billion euro acquisition. He stated that there would be changes to the company due to Advent also having Oberthur in its stable, but reassured customers that it was business as usual and that Morpho SA would still be focusing on its customers and users to ensure a seamless transition. As proof of this commitment, he noted the new employees Morpho has brought on board over the past year, who were present at the event.

Oberthur Technologies is a global player in digital security solutions for the mobility space. The company provides end-to-end solutions in smart transactions, mobile financial services, machine-to-machine, digital identity and transport and access control fields, employing over 6 000 employees worldwide. The technologies from the two companies are therefore complementary and Jeremias said the companies would spend the next couple of months strategising on the road ahead and how to optimise the strengths of both companies.

A new entity will emerge, with a new name, but this will only be announced later this year. Jeremias also noted that the changes would only provide additional benefits to clients and the combination of two market leaders would only serve to enhance the confidence customers have in the products and services available.

For more information contact Morpho South Africa, +27 (0)11 286 5800, sec.san.morpho@morpho.com, www.morpho.com

**Morpho goes extreme**

**By Andrew Seldon.**

Panasonic Distributors now distribute by Akhanani

Akhanani Distributors has been appointed as a supplier of Panasonic’s wide range of security solutions in South Africa and SADC. Panasonic’s local slogan, “You Deserve Better” is the driving force behind the company’s push to improve on existing technologies and lead the way in new product development.

“Akhanani Distributors is the perfect company for us to align ourselves with. They have over 60 years’ combined experience in the CCTV market and therefore are more than well established in the security industry,” said Franz Kersten from Panasonic.

Morné van der Helde, from Akhanani, echoed the sentiments. “By aligning ourselves with Panasonic, there is no doubt we will be bringing our customers the best security solutions to satisfy their needs.”

Focusing on large project-based sales, Akhanani has supplied equipment throughout Africa with its footprint extending to Kenya, Nigeria, Mozambique, Botswana and Zambia, including the Zambian Parliament.

Panasonic has launched its new range of security systems called the i-PRO Extreme Series. “Security solutions and technology are constantly evolving and there is a need for industry players to join forces with technology partners to ensure that modern solutions are available in both the commercial and private sectors,” said Kersten.

For more information contact Akhanani Distributors, +27 (0)11 613 7299, sales@akhanani.com, www.akhanani.com

Akhanani launches its Panasonic distribution.

**For more information contact Morpho South Africa, +27 (0)11 286 5800, sec.san.morpho@morpho.com, www.morpho.com**

**Akhanani Distributors now distribute by Akhanani**

Akhanani Distributors has been appointed as a supplier of Panasonic’s wide range of security solutions in South Africa and SADC. Panasonic’s local slogan, “You Deserve Better” is the driving force behind the company’s push to improve on existing technologies and lead the way in new product development.

“Akhanani Distributors is the perfect company for us to align ourselves with. They have over 60 years’ combined experience in the CCTV market and therefore are more than well established in the security industry,” said Franz Kersten from Panasonic.

Morné van der Helde, from Akhanani, echoed the sentiments. “By aligning ourselves with Panasonic, there is no doubt we will be bringing our customers the best security solutions to satisfy their needs.”

Focusing on large project-based sales, Akhanani has supplied equipment throughout Africa with its footprint extending to Kenya, Nigeria, Mozambique, Botswana and Zambia, including the Zambian Parliament.

Panasonic has launched its new range of security systems called the i-PRO Extreme Series. “Security solutions and technology are constantly evolving and there is a need for industry players to join forces with technology partners to ensure that modern solutions are available in both the commercial and private sectors,” said Kersten.

For more information contact Akhanani Distributors, +27 (0)11 613 7299, sales@akhanani.com, www.akhanani.com
SETA accreditation for Crest’s training academy

Crest Advisory Africa has announced that its Training Academy has been evaluated, quality assessed and been through various stages of assessments to determine if it will be accredited as a SETA-approved service provider.

“We are proud to share that as from the 8th March 2017, Crest’s Training Academy has been approved by the Services SETA as an approved service provider with Provider Accreditation Number: 12236,” says Crest’s CEO, Nico Snyman.

He explains that the accreditation process is long and complex, involving three phases. The first was an audit of Crest’s Quality Management System (QMS), which included its policies, capabilities, facilitators, assessors and moderators, and more. The second phase was an inspection of the company’s documentation for its courses, done by SETA as well as an independent verification company. And the third phase was a quality assurance audit.

The accreditation means the company’s courses offer real benefits to attendees as it means the Crest Training Academy complies with South African Qualifications Authority (SAQA) standards and that South Africa’s official government training and development structure approves of its Training Quality Management System.

“This gives clients the assurance that we are not only speaking about quality, but we implement, drive and provide a combined assurance approach to quality,” adds Snyman. “Crest’s training has also been endorsed by the Institute of Risk Management South Africa (IRMSA) and the Association of Internal Control Practitioners (AICP (UK)).”

Risk management and risk assessment skills are in demand throughout the country, and the world, in a variety of industries. Crest has courses available in areas such as warehousing and logistics, facilities management, security, cyber security, PoPI (the Protection of Personal Information Act) and more. The list of companies that have attended courses from Crest, including Hollard, SA Reserve Bank, Armscor, Anglo American, AngloGold Ashanti, Sibanye Gold, Royal Bafokeng Platinum and others, attests to the quality of the material and teaching provided.

Crest courses have also been sourced to be provided in Dubai, India, Kenya and other countries, with further international courses scheduled for later in 2017. Crest Training Academy has also been approached by

Monash University (South Africa) to provide Short Leaning programmes (SLP). The first of these courses are provided under the banner of Monash University, with a group of risk and audit managers from Nigeria.

With King IV directly addressing risk in companies, more business leaders are realising there is a vast difference between security and risk management. This has led to a need for quality education that provides those responsible for risk with real skills and tools to effectively assess and manage their organisations risks.

For more information contact Crest Advisory Africa Training Academy, +27 (0)11 534 8454, training@crestadvisoryafrica.com, www.crestadvisoryafrica.com/training.
New appointments at Naxian

Naxian Systems, officially launched in May 2017, provides smart solutions for both end users and system integrators. The team has been carefully handpicked to add value to client propositions, leveraging over a cumulative hundred years of knowledge, expertise and experience in the commercial and security engineering sectors.

- **Bernard Senekal, MD:** With more than 22 years as entrepreneur, Bernard spent eight years in the commercial and industrial video, information technology and business information systems markets. He has spent the past 14 years in the electronic security market, building and selling a successful distribution company, acquiring and turning around Geutebruck Southern Africa before founding Naxian Systems. Bernard is responsible for the strategic vision of Naxian and ensures that the daily behavior and activities of his team are aligned with the company’s long-term objectives. Bernard lives by the motto that opportunities multiply as they are seized!

- **Charl Wolfaardt, financial director:** As entrepreneur himself, Charl has been instrumental in the successful build of all businesses where Bernard has been involved over the years. He has ensured stable administrative, logistics and financial processes and disciplines, and continues to do so in his role at Naxian.

- **Duncan Gordon, business development:** Duncan has the ability to get the right audience around the table, although relatively new to the physical electronic security industry, his passion and drive is a breath of fresh air. Having spent the bulk of his career in the ISP and telecoms industries (and a short stint in the green energy space), he comes with a wealth of knowledge, technical networking abilities and strong B2B relationships as well as an excellent nose for picking up new opportunities.

- **Gerhard Furter, head of innovation:** A technology veteran of 22 years, Gerhard has achieved success in projects across diverse markets: defence, financial, manufacturing, distribution and communications. Gerhard lives by his maxim that impossible is only an opinion, and there is always a way to achieve the objective, even if that way is completely outside the usual method. An innovator, futurist, and avid gamer, Gerhard contributes to the superior technical ability of Naxian with a tactless disregard for industry limitations that have gained him a reputation as the blunt instrument that gets the job done.

- **Wayne Bosch, solutions engineer:** Wayne has 16 years’ experience within the security industry. Starting as a technician and excelling through the ranks in almost all aspects within the security industry, during the years of transition from analogue to IP technologies, has given him the ability to associate and identify all manner of technical (and other) requirements that are applicable for certain environments. He also has the ability and driving force to complete any project to perfection with a passion for new and innovative ways of completing projects more efficiently.

For more information contact Naxian, +27 (0)87 820 0620, bernard@naxian.co.za, www.naxian.co.za

Cameron Abraham joins Axis Communications

Axis Communications has announced the appointment of Cameron Abraham as sales engineer in the company’s Durban office. Cameron’s primary role and responsibility will focus on the ongoing growth in the KwaZulu-Natal region, offering customers in this region product expertise and tailored solutions, with guided industry knowledge and consultation.

Cameron has worked in the security industry for the last nine years in various sales and technical roles, as a systems integrator.

“We are thrilled to have Cameron in our Durban office, his skills and experience will be of great benefit to the Axis team, partners and customers,” says Roy Alves, country manager at Axis Communications.

For more information contact Axis Communications, +27 (011) 548 6780, sasha.bonheim@axis.com, www.axis.com

Cameron Abraham.
Paxton

Net2 Entry Touch
Smart, Simple Door Entry with a Premium Touch

Durable 7” colour touch screen

Personalise with multiple theme options

Fully compatible with Net2 access control

For more information:
paxton.info/2852
Smart services reduce costs

As-a-service: Lower maintenance costs, fewer resources.

Naxian Systems is the dynamic fusion of the accumulated knowledge, experience, resources and intellectual property of two industry specialists. Officially launched in May 2017, Naxian Systems is driven by owners Bernard Senekal and Gerhard Furter.

Recognising a need in the market to adapt to the increasing trend towards the Internet of Things (IoT), Furter’s work on PSIM (Physical Security Information Management) and Senekal’s involvement in providing advanced physical security systems, led to the development of Naxian’s core smart services solution. This Service-Oriented Architecture (SOA) is underlined by its modularised design and collaborative abilities, created for maximised flexibility and scalability.

“We believe that as things get smarter with the dogged march of IoT, there is a definite point of departure between physical security for electronic security devices and cyber security. The basic SNMP (Simple Network Management Protocol) and ICMP (Internet Control Message Protocol) used by the electronic security industry is nowhere near the functionality of the latest technology used in the IT industry. Unfortunately, physical security systems are open to the relatively easy gathering of system information and subsequently are vulnerable to attacks. The solution Naxian offers addresses this divide and provides for optimised system and device health,” says Senekal.

Furter explains that the Naxian platform works on basic network protocols with the addition of their own ‘secret sauce’. It firstly takes the information collected from devices and attaches processes to them which are followed automatically, and furthermore it instructs operators on what actions to perform.

Therefore, in the event of a security incident, Annie – Naxian’s artificial intelligence (AI) agent – looks for the closest resource available using resources such as Google Maps to factor in traffic and possible delays. This then allows the system to match resources to needs by deploying the most suitable response.

Smart Services

Annie is a classic example of an adaptive organic machine learning system. As an example, if ‘x’ is identified as the problem, then Annie knows that ‘y’ is the probable solution. Therefore Annie creates probabilities based on accumulated learning for the quickest and most expeditious solution.

In addition to consistently learning about systems and probable solutions, Annie also learns about the people used to support a site in terms of their capabilities. Thus, Annie not only selects route optimisation for response to an event, but also selects the best skills to resolve the event. If the selected human resource is not currently available, then Annie searches for and selects the next best available human resource. Furthermore, if Annie detects ongoing deficiencies in a particular person, it will pull this data into an e-learning platform, highlighting issues and creating constructive ideas and recommendations for addressing these deficiencies.

Not only does the Naxian Systems solution benefit end users directly but it also provides system integrators (SIs) with an opportunity to increase their profits. “Typically, when SIs increase their service revenue, their expenses concurrently grow. By using Naxian to manage the sites, the SI is able to focus on their core competency – installation – thereby reducing the number of resources required for servicing clients. By intelligently analysing and managing each site, Naxian is able to correctly advise on the resources and parts required for each maintenance event,” says Senekal.

By using Naxian’s smart services, SIs can generally achieve an increase in profit margins from between 9 and 11%, up to in excess of 40%. Naxian’s managed site services entail the system performing continual checks on the site devices and informing Naxian that there is a problem or that a specific part is needed, thereby allowing the right person and part to be dispensed in order to quickly rectify the problem.

The system is completely agnostic to technology disciplines and brands. It currently supports most key electronic security brands, including but not limited to, Geutebruck, Avigilon, Hikvision, Dahua, Arteco and Uniview surveillance equipment; as well as Impro, Saflec, Softcon, ViRDI and Morpho access control products. It also allows integration with Texecom, Paradox, IDS and DSC alarm panels and various building management and fire systems. A mobile app – Everywhere – allows users to access information remotely and the geolocation tool lets them see exactly where their resources are situated at any given time.

Other than system and device health services, Naxian also offers total process visualisation solutions. As an example, in warehousing supply chain and logistics environments, video analytics are combined with business process, linking into warehouse management systems such as SAP or RedPrairie. For example, linking a warehouse management system with scanning and video allows for a business to immediately be notified, with video evidence, should 10 boxes have been ordered, but only nine are scanned. When the truck is dispatched to the warehouse, the system will scan its licence plate and as it enters the delivery area, the licence plate is once again scanned to ensure that the delivery is correctly scheduled.

The system can also be programmed to instruct the vehicle to park in a specific docking bay and the management system can then scan the boxes and provide instructions on where they should be offloaded. Complete control by combining traditionally standalone systems into a singular operating and reporting interface such as this allows companies to quickly identify the needle in the haystack, mitigating risk and increasing bottom line profits.

Everything as a Service

Naxian Systems employs the Everything as a Service (XaaS) principle and by using secure, managed and always available Cradlepoint LTE
technology the company is able to ensure that networks operate at optimum efficiency. Furter points out that XaaS is very disruptive in the market since the company is now selling a service rather than a product, allowing users to change expenses from CAPEX to OPEX, providing obvious tax relief and operational benefits.

**Successful solutions**

Senekal says that the company’s first sites are live, with installations at Melrose Arch and 104 sites for Bidvest Bank. Bidvest Protea Coin has also invested in Naxian’s Synapse and PSIM for its control rooms. Bidvest has reported a phenomenal cost saving in site servicing since Naxian took over the management of the sites.

Data security is completely ensured as Naxian never has direct access to a customer’s site information within its SAIDSA-approved control room. This is achieved by using a secure staging area between both end user client and Naxian, from which Naxian extracts the required information.

Naxian is currently engaged in over 30 proof of concept (POC) projects with key security industry players inside almost every vertical market sector in the economy. Senekal says that the company has developed a dedicated team of specialists to perform POCs. “Anything related to security and the maintenance of sites is commonly perceived as a grudge purchase, but by offering a POC, we are able to demonstrate the real value of our system. In essence, we are able to clearly indicate what it would costs a client to not have a management system in place.”

In one POC example, a number of retail stores are using Naxian’s smart services to provide counting of people entering stores, heat maps, as well as scales which are integrated with video coverage, to provide additional return on investment. Senekal says applications like video verification allow stores to reconcile the video footage to actual orders and deliveries to ensure that the two match, and in cases where there is a dispute, credits can be issued to the wronged party.

The stores are also integrating the service with their POS database to provide prediction of trends with each event recorded and to alert to events like sweet hearting as it occurs. This is a good example of integrated video coverage from the warehouse to the store’s POS, allowing more control over what is received and dispatched. Clients are able, in real-time, to access a web portal that allows them to view any issues and their resolution progress.

**Coming up**

“The services concept makes perfect sense since fewer resources are required by the SI due to the fact that they can now leverage Naxian’s resources and infrastructure, at a much lower cost. In addition to managed services, we will continue to market our Synapse IoT-PSIM platforms and Synapse will be released as a PaaS (platform as a service) platform at the end of 2018. Therefore, instead of buying and installing PSIM in one’s control room, end users will be able to use it as a service via Naxian,” says Senekal.

While it’s artificial intelligence and deep learning technologies are now patented, Naxian will expand on this to include cognitive abilities in the future. This will allow the company to expand far beyond just the security environment.

For more information contact Naxian,

+27 (0)87 820 0620, bernard@naxian.co.za, www.naxian.co.za
ESDA talks social media

Emma Sadlier.

The Electronic Security Distributors’ Association (ESDA) will again be hosting a breakfast event at Securex, to be held at the Gallagher Convention Centre in Midrand at 7am on 30 May 2017. The guest speaker at the event will be Emma Sadlier, a media law consultant based in Johannesburg. The talk will focus on the legal and reputational risks of social media.

Social media is very much part of our lives and is used extensively by companies and their employees. While there are benefits in using social media, incorrect usage can have serious implications for both the company and the employee. Claiming ignorance is no defence or protection. Join us to gain a better understanding of the legal and reputational risks of social media within the business environment.

Emma’s areas of expertise include all aspects of print and electronic media law, with a particular focus on defamation, privacy and social media law. Her presentation will cover the social media landscape in South Africa as well as the legal considerations of using social media, including defamation, privacy, hate speech and intellectual property. She will also touch on common social media disclaimers (such as “tweets are not endorsements”, “I tweet in my personal capacity” etc.).

After the breakfast, guests are invited to visit the exhibition and stop by the ESDA stand.

The breakfast is free of charge and exclusively for ESDA members. To book, contact shirley@esda.org.za.

Seagate Integration is Milestone Certified

Milestone Systems has announced that Seagate Technology RealStor is now a Milestone Certified Solution. Milestone Certified IT infrastructure components provide the assurance that they will function, operate, perform and easily integrate with Milestone XProtect VMS. With Milestone’s open platform architecture, users have endless possibilities to continually add more value through customisations and extensions of their video surveillance capabilities. Integrations with third-party systems and devices enable incorporating new innovations as they come to market.

For Milestone Solution Partners, the certification guarantees the interoperability of their tested solution with Milestone XProtect VMS, and it is a distinguishing feature of the solution. This distinction stems from the solution’s documented certification process with the Milestone XProtect platform. A proven, certified solution delivers confidence to those specifying, implementing and operating it.

The certification focuses on testing the solution’s architecture, functionality, performance impact and usability. The documentation, including test parameters and results summary as well as specifications, states the tested versions of the products and components from both Milestone and Seagate which were included in the solution certification: Milestone XProtect Corporate 2016 R3 video management software in operation with Seagate’s RealStor RAID storage platform. The certification applies for use with the entire XProtect product line.

The Seagate RealStor RAID storage array is compliant for meeting stringent telecommunications and military requirements for shock and vibration. The Seagate RealStor 6000 series used in the Milestone Certification Tests can scale to 448 terabytes in a single array and reach 1.9 petabytes with additional expansion shelves. Performance of up to 250 000 IOPS per disk is possible along with 12 gigabytes per second sequential reads and 5.7 gigabytes per second sequential writes. The Seagate RealStor chassis supports a hybrid solution of HDD and SSD devices to provide tiered storage for demanding environments.

“This is the first 4K-ready storage solution that we have certified. The video stream sizes that we were using in this testing were extremely large: a 12 Mbps stream is basically a 4K video stream size. And we were recording over 700 video streams of that size to the RealStor solution,” said Mike Tarras, solutions integrations engineer, Milestone Systems.

Based on the conclusive test results, Seagate Technology’s RealStor Storage Platform is proven to be a highly qualified and scalable storage solution for Milestone Systems’ video surveillance installations because it reliably meets large video surveillance requirements with no performance impact.

For more information contact Milestone Systems, +27 (0)82 377 0415, arms@milestoneys.com, www.milestoneys.com

M.A.S.S Solutions is a member of Camprosa

M.A.S.S Solutions (Management and Supply of Security Solutions), joined Camprosa in March 2017 as an associate member. To be an associate member of Camprosa generally means that you are involved in the annual meetings, conferences and workshops with the view of exchanging ideas and knowledge pertaining to all facets of campus protection services and other related matters.

Camprosa and M.A.S.S have similar objectives when it comes down to security solutions, which makes it a great fit when it comes to solving particular issues regarding crime prevention, solving disturbances and creating specific solutions. Camprosa promotes and co-operates with local and international institutions or interest groups with similar goals and aspirations for the prevention of crime, campus protection, occupational safety, access control and other risk services.

M.A.S.S is looking forward to this partnership in 2017 because it can assist Camprosa and other parties involved with security solutions, sponsorships and education on security solutions, trends, products and services.

The next Camprosa conference will be held at the Kwa Maritane Bush Lodge in the North West province on 3 – 6 September where M.A.S.S will be looking to possibly present its products and services while networking and giving its expert opinion on the topic of the year, which is ‘Security within the norm.’

For more information contact Management and Supply of Security Solutions (MASS), +27 (0)12 142 0000, info@mass-solutions.co.za, www.mass-solutions.co.za
SAIDSA Technical Certificate Courses (5 days)
Suitable for new and current technicians
SAIDSA Certified Technician
The highest qualification from SAIDSA
Technical Sales Course (1 day)
Teaches salespeople to identify and select correct products, correctly assess a risk and place detectors
Course dates: Variable
Venue: Johannesburg, Gauteng
Cheryl Ogle, +27 (0)11 845 4870
saidsa@mweb.co.za
www.saidsa.co.za

Reditron will be running various training days from 22 May 2017 to 25 May 2017 in the Johannesburg region, on basic & advanced CCTV, NUUO Main Console and Dahua products & practical.
Course dates: 22 – 25 May 2017
Venue: Johannesburg, Gauteng
Neil Marks, +27 (0)87 802 2288
training@reditron.co.za
www.reditron.co.za

AC1 Foundation Access Control
The course provides the fundamental skills required to design, operate, install and commission access control systems. Ideal for new and experienced practitioners. Completion of Tavcom’s Electronic Principles course may prove useful as prior learning for some students.
Course dates: 25 – 27 July 2017
Venue: Elvey Head office
Neil Gillespie, +27 (0)11 401 6700
neil.gillespie@elvey.co.za
www.elvey.co.za

CCTV surveillance skills and body language training
A 2-day in-company course delivered by Dr Craig Donald focusing on enhanced CCTV observation, recognising and reading incident body language, a greater understanding of CCTV surveillance targets and evidence gathering, and significantly increased detection of crime incidents.
Course dates: Variable
Venue: Throughout southern Africa
Dr Craig Donald, +27 (0)11 787 7811
sales@leaderware.com
www.leaderware.com

Advertise security training courses
to over 5 500 security and risk managers, installers, system integrators, security service providers, sales executives etc through the Hi-Tech Security Solutions 3-in-1 training package

Package includes:
- Listing in the print edition
- Listing and banner advert in the training news briefs
- Listing in the training section of the Hi-Tech Security Solutions website

All for only R4 500 excl. VAT per month

Contact Vivienne on +27 (0)11 543 5800
vivienne@technews.co.za
The changing nature of CCTV surveillance and the demands of crisis handling

By Dr Craig Donald.

Many managers and staff in surveillance control rooms are facing new challenges.

The early introduction of CCTV along with things like emergency response services saw a strong differentiation in South African city centre sites. On one hand you had a surveillance facility staffed by specialist surveillance personnel, while on the other hand response personnel, mainly police, would take over once an incident had been detected and would coordinate and manage the response process in order to apprehend the suspect.

This suited the fact that surveillance is typically done best by more introverted personnel who enjoy working with systems, are capable of sustained concentration, and are good at visual analysis. Demands of communication, interaction with others, and emergency situations were then left to the response function within the control room.

In the South African situation, however, surveillance environments have seen a substantial shift in nature. The level of potential violence along with armed robbery in places from shopping centres to town centres and other work related sites has increased dramatically. Protests have moved beyond communication of grievances to physical confrontation and aggression in anything from community protests with service delivery issues to universities.

Security and police members have become targets themselves by being in such environments, and control rooms have been the focus of attack, and in some cases actual destruction. The potential for violence during strikes has also increased, with protection of personnel and property become key priorities.

While the differentiation in town centres has continued with police still bearing ultimate responsibility for reaction situations, for a range of other business and public environments, the environmental changes have led to a shift in the need for capacity of surveillance operator staff. South Africa is not alone in this, but the country is probably one of those who are experiencing this phenomenon more than any other, despite terrorism being relatively low in its occurrence here compared to other countries.

Observe, detect and manage
The criteria for effective surveillance operators has moved from surveillance ‘per se’ to the ability to observe, detect and warn, and handle and manage crisis situations through constant communication to a range of parties to keep people informed and able to act. In some cases in the industry, the developments in environmental conditions outside the control room have left the capacity to cope inside the control room behind.
While used to traditional physical security responses to threats in outside areas, many managers and staff in surveillance control rooms are facing not just new challenges in dealing with these within a control room environment, but vastly increased dangers to property and people, including the need to protect lives. At the same time, there remains a need to protect the reputation of organisation where ongoing media sensationalism remains an ongoing issue.

This phenomenon of environmental threat is not applicable to all surveillance control rooms. However, it is increasingly becoming an issue and is something that most surveillance operations are standing a chance of encountering. Ironically, while operators are needing to increase their skills base to deal with the new threats, the need for more effective surveillance and detection itself is increasing.

**Interpret, predict and anticipate**
The ability to recognise body language issues and situational conditions is critical in dealing with early warning and active management of conditions. Operators don't just need to observe, there is an increasing need to interpret, predict and anticipate. Along with this, as part of the crises management needs there is a strong need for greatly increased communication skills, the ability to work under pressure and to keep calm and collected. Operators need to look at things rationally and systematically, to coordinate and provide information, and to evaluate the potential risk to both people and settings.

The surveillance operator plays an indispensable role in these kinds of challenges and it means that selection of such personnel is more important than ever. The ability to communicate needs to be recognised as critical.

Training in surveillance and crises communication need to be integrated in situations where personnel are going to have to deal with issues. It also means that management need to consider a broad range of scenarios that need to be catered for, and have response procedures and policies in place. Further, ongoing simulations or stress testing with apparent live situations are necessary for giving exposure, development and confidence building in handling of crises situations. You don't want the first crises situation to be the first occasion where operators have to think about the skills and processes to deal with and resolve it.
Powell Tronics goes to the Extreme with new Morpho products at Securex

Powell Tronics geared up for Securex with the latest products and a dynamic new stand.

According to Powell Tronics CEO John Powell, Securex provides the company with the opportunity to not only present new technologies to the market, but furthermore to interact with its existing customers and suppliers. This year marks the company’s sixth consecutive presence at Africa’s largest security and fire exhibition.

“We have redesigned our stand to act as a dynamic background to the new products we will be launching at Securex. In addition to Impro’s Portal range of products, IP intercom equipment and our own range of bespoke solutions and time and attendance software, we will also be introducing two new products from Morpho,” says Powell.

SIGMA Extreme
The MorphoAccess SIGMA Extreme access and time fingerprint terminal replaces the MorphoAccess and Bioscrypt 4G legacy ranges. Based on the same platform as the entire SIGMA product line, the outdoor MA SIGMA Extreme is specifically designed to operate in the harshest conditions. Not only does it resist rain, snow, dust and salt mist but it is also capable of withstanding strong impacts and is resistant to vandalism.

The SIGMA Extreme features a bright capacitive touchscreen with very responsive controls and a biometric sensor, and is claimed to be the largest single fingerprint sensor on the local market. Other notable features that enhance the robustness of the terminal include the IP65 enclosure, the sturdy wall mounting and the tempered glass screen.

MorphoTablet 2
The second generation MorphoTablet2 secure biometric tablet is the perfect partner for Powell Tronics’ ATOM T&A and PT-Rollcall software solutions. The 8-inch touchscreen Android device offers 4G high-speed data transfer, complete credential acquisition/reading capabilities, plus enhanced usability and robustness to ensure seamless enrolment, ID verification and identification on the spot.

Powell says that the second generation’s predecessor has been used, together with PT-Rollcall, in a well-known South African tertiary educational facility to verify the identity of a specified group of first-year students at the 2015 year-end examinations.

The device’s 13 MP camera with dual LED for face capture, 1D/2D barcode and MRZ reading ensures complete accuracy, making the device perfect for instances where complete identification verification is required. Applications include elections, ID document issuance, criminal identification, time and attendance, access control, border control and registration/rollcall.

Powell Tronics has experienced a steady growth since its inception, a fact that Powell attributes to the highly motivated and experienced sales, technical, development, administration and management teams. “We have also invested heavily in ensuring that we stay abreast of new technological developments in the market and strategically incorporate them into the software products we develop in-house.”

By proactively monitoring the market instead of reacting to technology trends, Powell Tronics differentiates itself from being merely a supplier of products and moves into the realm of innovation facilitator. A strength which sets the company apart is its ability to ascertain, through intense customer involvement and relationship building, exactly what the market requires.

Confirmation of the company’s customer-centric philosophy is evident in the large number of Powell Tronics’ visitor management systems currently deployed at a number of premier residential estates in the country. Added to this is an increasing penetration into the educational sector, where products such as PT-Rollcall are enhancing the reliability of register-taking for examinations.

Powell explains that the company’s latest software offering – the ATOM time and attendance suite of products – is finding favour with a number of industries. Most recently, enquiries have been received for portable solutions from the construction industry and the farming community, to use the mobile clocking version of ATOM software for employees that do not report to a centralised point.

Powell Tronics will be running regular business card draws with attractive prizes on its Securex stand. The sales team will be on hand to demonstrate all of the company’s products and to discuss solutions.

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

More than verification

By Andrew Seldon.

Employee verification covers a lot of ground as it confirms people’s identities, qualifications and more, but perhaps it’s time to look a bit deeper.

There are a few trends in this risk aversion strategy, and one focuses on social media. With billions of social media accounts around the world, and hundreds of millions active in South Africa – including Facebook, Twitter, Google Plus, LinkedIn and many more – the implications of what people do on social media are vast. We only need to look at Chris Hart or Penny Sparrow (and the list goes on) to understand what one careless post can do to a person as well as the company they work for.

Social media screening
Social media screening goes beyond simply looking at someone’s Facebook or Twitter page. This service, which iFacts offers in partnership with Farosian, measures the potential risk an individual could pose to a company. An example of this risk Reid offers is that of an individual who seemed an ideal candidate for a position of responsibility. An overview of her social media account backed this view up, until a more in-depth study was made. It was then found that she had posted highly controversial comments in the past that were homophobic, among other things. If the company had hired her, it could have faced significant reputational and potentially financial damage at a future date.

The problem, Reid says, is that people are more open on social media that they would in real life, and often inadvertently (or purposefully) publish things they would not want out in the open. The screening service iFacts offers looks beyond a few posts and delves below the surface most people see. To be fair, it also considers multiple factors when running the profile search, such as age and the situation in which posts where made to ensure the risk assessment is fair and relevant to the person’s potential position.

Reid also notes that iFacts always obtains the individual’s permission to do the social media screening in advance to avoid any legal grey areas.

Farhad Bhyat

Wade Cooper

Jenny Reid

More than a scan
It’s safe to say that social media screening is not new. Many companies have in-house staff to do these types of jobs, but Farhad Bhyat, CEO of Farosian says they are often based on inadequate information or done by simply browsing someone’s feed. “There are no qualitative or quantitative rules involved to ensure the job is done professionally and in the required depth.”

He provides an example of a company in the USA where an individual was given a letter of appointment, but then told she would not be getting the job when she arrived for her first day of work. It turns out that after the position was offered to her, someone in HR did a social media scan and found a mugshot of someone with the same name. That was enough for the company to withdraw the offer. Unfortunately, while the
Have you closed the backdoor?

The protection of your security system is our number one priority. That's why American Dynamics, Illustra Pro and C-CURE 9000 products are shielded by the Tyco Security Products Cyber Protection Program which has successfully provided security from hackers for countless access control and video surveillance systems around the world.

- Our vigilance begins at the concept and design stage for each new product
- We continually test and evaluate
- We use the skills of cyber security experts to rapidly respond to any new threats
- We ensure only you have access to your confidential data

The Cyber Protection Program from Tyco Security Products helps protect YOUR business.

Download the free TSP App from www.tyco-tsp.com

Are you Cyber Safe?
Using our TSP App, scan the Cyber Protection logo opposite to watch a video and find out how Tyco Security Products Helps Protect YOUR Business
Continued from page 20

names were the same, it was not this particular individual in the mugshot. She then sued the company and won a large amount of money.

Farosian looks beyond simple page scanning or Google searches (and makes sure it has the right person). The company uses automated processes for the majority of its screening, which covers multiple social media sites, but Bhayt says there are always some manual processes involved to ensure the profile is accurate and reflects the actual level of risk the individual may pose to the company.

This result of the profile will not give away any personal details of the individual, but will simply offer the level of risk they pose for the company based on their score. The risk levels range from ‘Very Low Risk’ up to ‘Extreme Risk’, while the scores are awarded in various criteria, including the individual’s creativity, communications skills, professional image, teamwork and collaboration, critical thinking and more.

Another differentiator in Farosian’s screening is that it looks at both the positive and negative issues of the individual. Context is also important in this respect. If someone has a few drinks at his birthday party that is acceptable, but if he has a few for breakfast that could indicate a problem. Other issues the company looks for could include if the person can engage in arguments constructively. This may indicate if they are likely to cause conflict in the workplace and if they would be a good team player.

For those who think social media screening is a little dramatic and that a social media scandal would simply be a bit of a controversy without any real impact on the company, Bhayt explains that this simply is not true. Even though the individual may not have been posting on behalf of the company, they are still associated with the company and the online reaction will impact the company.

In one incident, he notes that the individual’s employer, a national real estate agency, did not make a sale for six weeks after the scandal began despite having 600 agents on its payroll. People just avoided the company because of the scandal. Bhayt states that the cost of South African social media scandals in 2016 is around R450 million.

More recently, United Airlines in the USA became the latest company hit by a social media scandal after a doctor was dragged off a flight. Within a few hours of the incident, around $900 million had been wiped off its valuation. Much of this loss was recovered, but at the time of writing, it was still $250 million down on its pre-incident value. Moreover, three of its competitors saw an upturn in their stock prices during the same period.

Farosian does not tell employers to hire a person or not. It simply fills a gap in the traditional screening processes by highlighting potential risks associated with the person. The company also provides training to assist companies in developing social media policies which are comprehensive and able to deal with any surprises their employees or anyone on social media may throw at them.

“We all need to realise there are no secrets,” Bhayt concludes. “Even if you try to restrict access to your social media posts, there are always ways to see what you’re doing, even for people who are not friends or followers. And there is no delete key; once it’s published it’s available for those who know where to look.”

It’s not all bad news, however. Reid explains that people with a low-risk social media profile will find it adds value to their CVs, increases the chance of a successful job interview, and can even enhance job security.

Oh behave!

Another trend in verification and screening focuses on behaviour. Reid notes that we are all different and are motivated differently. Simply look at millennials and you will understand that motivation and behavioural characteristics differ.

When hiring someone, a company wants to know that the person they are going to invest time and money into is a good fit for the company and its culture, and is able to do the job. This is where a PDA (Personal Development Analysis) comes into the picture. The PDA is a tool that through a simple, yet accurate and scientific methodology, allows you to describe and analyse the behavioural profile of individuals.

iFacts partners with PDA Africa to conduct personal development analysis on individuals to determine their behaviour profiles. Wade Cooper, CEO of PDA Africa explains that PDA assessments allow companies to hire the right person for the job, make sure the best talent works together in teams, develop leadership skills and assist in succession planning, and identify areas where employees or potential employees need to be trained to deliver the optimal performance.

PDA Africa is part of PDA International, which offers its services globally. The local company offers its services in 18 African countries out of the 47 countries served internationally. It has hundreds of partners globally that take its assessments to market, with iFacts operating as a partner in Africa.

Cooper says that the assessment conducted by PDA is scientifically based with a 90% reliability coefficient. This means employers can rely on its findings to determine people’s behavioural characteristics. The report, which can be produced in various languages (the assessment is also available in multiple languages) can assess areas such as leadership or business style, strengths and limitations, motivation, compatibility with key competencies of the job being applied for and assists in improving productivity.

The assessment is not a test with right or wrong answers, it simply measures each individual’s behavioural characteristics. Cooper says the benefit of PDA Africa’s approach to assessments makes it the easiest way to create a behavioural profile of an individual.

The assessment is called the PDA Human

Social media statistics. Source: iFacts
Capital Management System and is completely online. It takes an individual 10 to 15 minutes to complete. In cases where individuals may not have access to the Internet, the assessment can be completed with pen and paper. PDA Africa does not charge a licence fee to access its site, but limits the costs by charging per report. Cooper notes that each ‘PDA credit’ allows a person to conduct one assessment and receive a full report – the company does not charge for different aspects of the report.

To administer the assessment and understand the report, companies like iFacts need to send the relevant staff on a three-day course to attain a certification.

**Customised reports**

Cooper adds that the assessments are not vanilla assessments that are provided for every potential employee. It is a scientific way to look at behaviours in comparison to the job description the individual is applying for as well as the competencies required. The report provided to the company will compare the individual’s personal behaviour profile to the job and competency profile provided, allowing the employer to make informed decisions as to the person’s fit to the job and the company.

He also notes that traditional verification and screening processes are still required, but should be combined with PDA profiling to ensure the right person is employed in the right job and the right environment.

“All too often we hear that people are hired for their technical skills, but fired for their faulty behaviour,” he notes. “The PDA assessment overcomes the behavioural ‘unknowns’ and allows companies to hire people they know will fit into their culture and are capable of performing the job.”

He adds that many educational institutions are also using the PDA assessment as a means to make their graduate development programmes more effective. These organisations can now scientifically identify issues graduates may have in the workplace and deal with them before the students get a rude awakening or hiring companies wonder why they hired them.

The PDA is also a good method for individuals to assess themselves in terms of how their particular behavioural patterns will fit in as well as provide insights into any personal development they may require.

When this reporter completed the assessment, provided by PDA Africa, the process took only 10 minutes and the report provided concise insights into the personal and role-based behaviours pertinent to my job. It would offer managers and HR administrators keen insights into the type of environment suited to the individual, as well as the ways to manage and motivate the person most effectively.

PDA Africa is also committed to social development in Africa. Cooper says 80% of the company’s partners in Africa are women owned and the company was awarded the first runner-up position in the category of Women Empowerment in the Workplace at the 2015 Gender Mainstreaming Awards (http://www.genderawards.co.za/the-awards/the-winners-2015).

While the verification of people’s identities and other information is still a critical aspect of the hiring process, the world we live in today has made it a risk to hire people without additional information to assist in deciding if they will be a good fit for the company and are likely or unlikely to cause the company any brand or reputational harm in the long run. If one takes the *New York Times* seriously, its recent article ‘The Utter Uselessness of Job Interviews’ (www.securitysa.com/*nyt1) highlights the need for additional mechanisms to assist in deciding who fits in a job and who doesn’t.

Social media screening and behavioural assessments are two candidates with a good background in providing useful and usable information to companies and individuals.

For more information contact iFacts,
+27 (0)11 453 1587, jenny@ifacts.co.za, www.ifacts.co.za

<table>
<thead>
<tr>
<th>Employee background screening</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D&amp;K Management Consultants</strong> offers clients a vetting service providing both basic background checks and comprehensive searches. When choosing a screening service, D&amp;K’s Kyle Condon explains the service provider should operate within the following parameters:</td>
</tr>
<tr>
<td>1. <strong>Experience</strong> – Investigation experience is preferable as it provides a mindset of questioning. Searching for information can be difficult and inexperienced people may well come up short.</td>
</tr>
<tr>
<td>2. <strong>International sources</strong> – In the world we live in today, we are more than ever a global society. Many prospective employees may have trained, lived and worked in foreign countries, therefore your service provider should have sources and capabilities across the globe.</td>
</tr>
<tr>
<td>3. <strong>Accuracy</strong> – All information should be quality controlled and personally verified. Final reports should stand up to all checks and queries.</td>
</tr>
<tr>
<td>4. <strong>Sources</strong> – Service providers’ sources should be their own and not a third party. Stay away from intermediary sources. A reputable and professional screening agency will have direct contact with relevant sources.</td>
</tr>
</tbody>
</table>

For more information contact D&K Management Consultants,
+27 (0)11 824 0334, saint@intrigue.co.za, www.investigators.co.za
Where background screening matters


The best predictor of future behaviour is past behaviour.

Background checks are arguably one of the most essential steps in human resource management and staff recruitment today. They help root out unsuitable candidates by assisting with red flagging criminal behaviour, unverified qualifications, fabricated experience and more. This aids in ensuring that informed decisions can be made regarding one of the most important assets of an organisation - its employees.

One should therefore never finalise an employment contract until all the relevant checks are concluded and the results are available for clear and factual assessment. This is especially important because an employee/employer relationship is legally binding and employees cannot simply be fired in the event of certain behaviour patterns showing up only after they are hired.

Dealing with money and customers

In a corporate environment, employees dealing with finances or providing customers with financial advice should be checked in accordance with the Financial Advisory and Intermediary Services Act. These checks include the FSB Fit and Proper check, credit check and criminal check. Together they go a long way in identifying undesirable behaviour such as involvement in crime and past and present issues with credit.

The Association of Certified Fraud Examiners (ACFE) 2016 Report to the Nations showed that more than three quarters of fraud incidents were committed by individuals working in seven key departments: accounting, operations, sales, executive/upper management, customer service, purchasing, and finance. The banking and financial services, government and public administration, and manufacturing industries were the most represented sectors in the cases examined.

The ACFE Report also showed that the most common behavioural red flags in 78.9% of fraud cases were: living beyond means, financial difficulties, excessive control issues, recent divorce or family problems, unusually close association with a vendor or customer or a general ‘wheeler-dealer’ attitude involving unscrupulous behaviour.

This is not a situation any employer wants to face, especially when early detection is possible.

Fabricated qualifications

Some of the most prominent forms of CV fraud are fabricated academic qualifications and experience. These gross misinterpretations may assist the candidate with appearing more qualified for the job. However, once hired – their failure to perform can quickly turn disastrous for the employer. There have been numerous, high profile cases of qualifications fraud in South Africa, where candidates were found to have lied on their CV yet they managed to obtain senior positions.

Recruiters should never accept the information on CVs as is. Always verify the authenticity of the candidate’s qualification as well as their experience.

Conflict of interest

Employees who are involved in the procurement process are more disposed to conflicts of interest than others. Despite laws and frameworks, there have been numerous incidents in which procurement professionals were found guilty of allowing their personal lives to interfere with their professional responsibilities and duties. Common incidents include: having direct ownership or shares supplier businesses; offering private services to the employer’s clients; accepting gifts, money in exchange for discounts, preferential treatment or goods/service; the use of company resources for personal enrichment and the abuse of decision-making authority regarding purchases.

Conflicts of interest are able to thrive because of unregulated environments, which is why businesses must ensure that strict policies and vetting practices are in place to deter incidents.

Background screening solutions, such as Lexis RefCheck, can assist employers with employee due diligence and auditing by verifying a wide range of personal information, including the identity of the candidate, information held by credit bureaux, criminal records, driver’s licences, global academic qualifications and professional association memberships. In addition, Lexis ProcureCheck, helps to independently identify conflicts of interest within your supply chain via thorough employee and vendor screening.

For more information, visit: www.lnrisk.co.za.

Rudi Kruger, GM for LexisNexis Risk Management.
EMPLOYEE VERIFICATION

Testing integrity

By Johlene Selemela, ZKTeco.

Integrity testing has become the new age thing for companies recruiting potential employees. Although it has been in use for over three decades in other parts of the world, in South Africa the demand for integrity employee testing has only started growing in recent years.

Now one needs to take into account what actually happens when such a test is being performed. Firstly, integrity tests in the past used self-report paper and pencil formats and these did not prove to be effective. Today’s tests include at least one measurement of psycho-physiological parameter like voice analysis, to ensure higher reliability. They come in two forms: an overt integrity test is designed to find ‘undesirable’ traits in a person’s behaviour, past crimes, and dishonesty. Personality-oriented tests include items that assess personality characteristics that have been shown to relate to counterproductive work behaviour. The test items assess dependability, social conformity, thrill seeking, and conscientiousness, in order to sort out potential candidates.

As an employer, you would ask how such a test is of benefit to your business. Well, the answer is simple, integrity tests are designed to assess honesty, dependability, trustworthiness, conscientiousness, and reliability. Therefore, integrity tests foresee counterproductive work behaviour in employees and also help employers make rational decisions when employing someone.

Employers should consider integrity testing as an integrated strategy as it has more chance of identifying a dishonest employee, and this can be done through pre-employment screening from employers. The best benefit of an integrity test is that it will measure the suitability of a candidate for a position, and they are also more reasonably priced than a polygraph test, thus ensuring the company saves more money and time during recruitment processes.

Integrity testing also creates a positive experience for potential employees. Knowing that their integrity is being tested and validated brings about greater consciousness of expected values and behaviours. It creates a platform for transparency, accountability and fairness within a company.

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

MORE PRODUCTS, MORE SOLUTIONS, MORE FLIR.

THE NEW PT-SERIES HD

The most powerful pan tilt security camera systems, available with a cooled or uncooled thermal camera optimized with up to a 12x optical zoom and a 30x HD visible camera.

THE NEW UNITED VMS 8.0

Versatile, ease of use performance with tough cyber security, and the largest integration of thermal cameras and third party technologies.

Learn More at flir.com/security

WINNER
Video Surveillance Management Systems
2017 ISC WEST

FLIR® The World’s Sixth Sense®
Security beyond security

By Andrew Seldon.

The use of security solutions can extend beyond security in financial organisations.

Convergence is an overused term in the technical sector as it is used to describe a variety of trends and changes. In the security market we have become used to the term convergence describing the move to IP-based systems, and more recently the convergence between physical and cybersecurity.

Now we are also seeing a convergence in the benefits physical security provides. Companies and individuals are well aware of the security benefits of alarms, cameras, access control and so forth (or we hope they are), but lately we have also started seeing results from security equipment that benefits non-security areas.

The simplest example is from the retail industry. Today, while keeping tabs on all aspects of security, properly installed technology allows retailers to increase the efficiency and planning of their stores, measure demographics etc. via heatmaps, people counting and other analytical applications that determine demographics and so on.

But what about the financial industry? We know these companies are more paranoid about security than most, but are they making full use of their security systems?

Hi-Tech Security Solutions asked Sasha Bonheim from Axis Communications for more insight into what the financial markets are or could be doing to extract additional value from their security systems.

Bonheim says facial recognition is a perfect complement to an existing surveillance system, enhancing security and/or customer experience in real time. “It works by matching faces taken from real-time video with a database of previously stored images of faces. You categorise the faces in the database based on your application need – be it access control, VIP detection, or wanted individuals.

“When a face is captured on the camera, the matching takes place in real time, and a match or non-match either allows or denies access, or triggers an alarm alerting pre-determined stakeholders to take appropriate action. Together with our wide range of various Axis ADP partners (application development partners) we can offer financial institutions add-ons to their surveillance systems such as people counting, queue management and identifying VIP customers to enhancing the customer experience.”

More importantly, she adds that these types of value-added analytics sit on the

Banking security from Dahua

With millions of banking transactions every day, banking and financial institutions are exposed to significant crime. At the same time, improving customer experience and management efficiency has emerged as a task for facing competition in the modern world. Innovation in security with both technological breakthroughs and business integration has been an important enabler for banking and financial institutions to reduce their vulnerability and improve management efficiency.

Dahua offers a number of advanced technologies to secure banking and financial institutions:

1. 4K UHD cameras with face recognition can identify suspicious objects with clear images to prevent potential risks,
2. Overlay the transaction information on the video footage to avoid potential disputes and improve customer experience,
3. People counting, VIP recognition, remote authorisation etc. to integrate security with business process to further improve business and management efficiency, and
4. Data safety. Sophisticated backup measures to ensure critical data safety.

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

advances in video analytics capabilities that will impact both the security and non-security market. As noted above, Bonheim expects new compression technology for storage and bandwidth savings to make more of an impact going forward. This will be complemented by systems for health and safety risk monitoring and clever analytics utilisation for streamlined business practices.

So while security is converging in on itself, it’s also converging with other operational areas of business, opening new doors to security, efficiency and productivity, and new avenues for revenue generation among those who lead the way.

For more information contact Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com
Banks are still the source of money for criminals, even though the target has expanded to include ATMs and bank cards which are robbed via various mechanisms, and companies and individuals.

Kalyani Pillay, CEO of the South African Banking Risk Information Centre (SABRIC) says that criminals follow the money and as many of our transactions have shifted online, they have followed and are well versed in how to keep on stealing money, not only directly from banks, but also from companies and individuals.

Pillay notes that identity theft is still an important aspect of criminals’ efforts. This type of crime can be used to access personal and corporate bank accounts without even requiring a gun.

SABRIC has embarked on numerous efforts to assist banks and their customers in preventing financial crime over the years. One long-running project has been conducted in collaboration with the Department of Home Affairs (DHA) and the major banks in South Africa. This project saw many banks starting to use fingerprint biometrics as part of the process of identifying people.

When discussing the various ways criminals try to get their hands on money these days, excluding the armed approach, Pillay explains that there are various methods they use and that these seem to come in phases. As soon as one method meets more resistance, criminals opt for another that’s a bit easier.

Some of these methods include phishing, where an email that looks as if it comes from someone you know asks or authorises you to make a payment or pass on some sensitive information (like bank access information).

Then there’s vishing, where someone calls you pretending to be from your bank or a company and asks for similar information over the phone. These days, Pillay adds that we can add Smishing to the collection, where criminals use SMS messages to try the same tricks.

Pillay says criminals are constantly trying new ways to get information that would get them into other people’s bank accounts. Many victims of such crimes blame bank or other companies’ insiders for selling or giving away their information to these crooks, but all too often people provide the information themselves without realising it – even through simple behaviours like clicking on an email. And criminals are well informed, able to target specific people in a company with specific requests that make their attempts look quite professional.

And then there’s the old favourite used to collect card information, skimming. A simple and quick swipe of a debit or credit card, even while appearing to pay for something is enough to collect information criminals can use.

SABRIC runs various campaigns throughout the year to create awareness of the above and other crimes, assisting people in making the right decisions when it comes to corporate and personal financial information. The organisation’s website is regularly updated with new information about the latest scams and what to be on the lookout for.

Find out more at www.sabric.co.za

By Andrew Seldon.

Criminals are always at work – are you?
Secure your disruption

By Neil Cameron, Johnson Controls area general manager, building efficiency – Africa.

Financial organisations need security solutions that can keep pace with disruption.

Financial institutions are typically large, complex entities. They have one key requirement when it comes to security – the solutions they select have to last the distance. This means they need to be able to evolve rapidly, integrate easily with other systems and be flexible, adapting to the changing needs of the business. In a sector where change and disruption are key factors, and technology and cyber threats are advancing apace, these are critical requirements.

Financial institutions have a substantial footprint with lots of real estate, large distribution networks, a sizeable staff complement and multiple huge data centres, the engine rooms at the core of their business. A high level of digital disruption in this sector has seen new business models emerge, ushering in new, more digital and virtual means of engaging with customers, and a bigger focus on customer experience. This has made securing the business, its assets, people and customers a multifaceted challenge. Are there security solutions that can keep pace with transformation in this sector?

Physical, logical and virtual systems converge

For many financial organisations, operational efficiency, securing cost efficiency and risk management remain a high priority. As physical, logical and virtual systems converge, assets, information and people are under threat. To achieve greater control and lower risk, the consolidation of systems and efforts to achieve standardisation across these organisations have become increasingly important.

The IT environment is far from stable as technology continues to leapfrog ahead. CCTV systems, for example, have evolved from using local storage for footage to using network storage, from running analytics on the server to enabling analytics on the network device, and from providing a single camera view to providing multiple simultaneous views. At the same time, legacy systems must be incorporated. With multiple protocols and formats to accommodate, a standardised environment where, for example, end-to-end encryption is enabled, is vital.

How does consolidation and standardisation drive tighter security? Consider this: whether in a backwater town or major city centre, every branch of a bank presents the same level of risk, in that each provides access to the bank’s core systems. Security thus must be applied in a consistent manner across geographies and facilities, regardless of relative perceptions of risk.

Similarly, banking organisations often have personnel moving between branches and banking divisions. With larger banks employing more than 100 000 staff across hundreds of branches, this can be a security nightmare, especially as banking halls become more ‘open’ to customers and it becomes more difficult to identify staff and manage access to restricted areas. With increased threats to data, assets and people, it is critical that the security systems in place be able to work together to manage identity and access, placing a single consistent layer of protection across the organisation, regardless of facility type or geography.

Such a system would, for example, ensure each employee only needed a single security card (rather than multiple cards for multiple sites) that would grant them access to specific areas based on their security level, for example, to restricted areas but not to strongboxes. It would also work at a logical level, denying network access to someone who tries to sign in from one location while being logged in at another.

It’s clear why leading control and security solutions that have a large research and development component, clear roadmaps, a proven track record and global recognition are gaining favour among financial organisations.

Security smooths the way

Financial institutions function in a highly competitive environment where customer service and the customer experience is a differentiator. This has seen facilities introduce couches and ticketing systems in banking halls. With security systems sharing the banking network with these systems, it’s not hard to see the synergies. For example, to improve floor operations, CCTV camera footage feeds logistics systems, alerting managers to where service bottlenecks may be forming and driving allocation of more consultants to particular areas.

As physical, logical and virtual systems continue to converge, ensuring a single consistent risk and security policy will be very important. Any new security systems or features will require forethought. Ensuring that their security systems are open, integrate easily with other systems, and constantly evolve, enabling the organisation to make use of new and emerging technologies, will position banks well to secure their people, customers and assets in physical and virtual environments.

As businesses continue to evolve with the help of technology, the goal is to build even smarter, more secure and more sustainable environments. Smart solutions that harness new technologies and emerging approaches will create a firm foundation for growth and competitiveness.

For more information contact Johnson Controls, +27 (0)11 921 7141, neil.cameron@jci.com, www.johnsoncontrols.com
Co-operation and data delivers returns for SAICB

By Andrew Seldon.

Data analysis and information sharing among insurance companies is producing sterling results in the fight against fraud.

Fraud is nothing new to most industries in South Africa and around the world. In the insurance industry, however, fraud ranges from individuals ‘trying their luck’ to sophisticated criminal syndicates focused on stealing as much as they can from insurance companies.

A common refrain among those who are criminally inclined is that this fraud is not really a crime because people are stealing from insurance companies, which have plenty of money. The reality, however, is that these companies make their money from premiums their customers pay, meaning the more fraud they suffer, the higher the premiums will climb in order to meet the needs of legitimate clients.

According to Garth De Klerk, CEO of the SAICB, the tough economic conditions in South Africa have resulted in a higher number of false claims over recent years as many people try to alleviate their financial predicaments by making fraudulent, low-value insurance claims for, among other things, lost cellphones, TVs, tyres and so on. These claims traditionally go unnoticed unless the claimant makes a mistake because they are common and for smaller amounts of money.

This is changing, however, as insurance companies increase their use of technology to validate claims (although the traditional human anti-fraud element is still in use). Today, technology is a must for these organisations as they strive to provide a better and faster service to customers. At the same time, technology is used to provide risk profile modelling, which is able to flag suspicious claims or claimants.

It’s not only individuals at work in committing fraud. Crime syndicates are just as active in designing fraudulent schemes for higher claim amounts. These schemes involve multiple people and sophisticated strategies to defraud insurance companies, especially in areas such as car, life and funeral coverage, although they are not limited to these areas.

Here again, the combination of technology and people, as well as co-operation between organisations within the industry and authorities makes an enormous difference in curbing fraud.

Garth De Klerk, CEO of the SAICB.

Intelligence gathering, analysis and sharing

The South African Insurance Crime Bureau (SAICB) was launched in 2008 after a four-year investigation by the South African Insurance Association (SAIA) on how to best address crime and fraud committed across companies in the short-term insurance industry. De Klerk explains that the organisation is a non-profit, non-commercial enterprise focused on fighting insurance crime across the industry.

There are currently 21 organisations that are members of the SAICB, mostly in the short-term insurance industry, but with other companies slowly realising the real benefits of membership.

De Klerk describes the organisation as a fusion centre in the middle of the insurance landscape where data is collected from its various members, analysed and the results shared with members and/or authorities which act against fraudsters. The organisation brings the industry and related parties, from SAPS to the Department of Home Affairs, the Hawks and the NPA together to discuss ways and means of eliminating fraud.

The SAICB does not only deal with information, however, it also has feet on the ground as it works with various authorities to address the fraud issue and go after perpetrators. De Klerk notes that the use of intelligence has had a remarkable impact on the fraud committed in member companies.

“Our members have seen an average return on investment (ROI) to the various companies of 230%,” he states. This makes a significant difference to the amount lost to fraud each year, and consequently to the bottom line.

Advice to individuals and companies

As noted above, insurance fraud affects everyone, the insurance companies as well as individual and business customers. It is therefore imperative that everyone plays their part in ensuring that legitimate clients receive good service and fast resolution to their claims.

Companies need to understand that fraud is real and does impact their bottom line, from paying higher premiums to longer resolution times. If corporate clients make the effort to ensure their activities are in accordance with their insurance policies and focus on preventing fraud, everyone wins in the long run.

De Klerk says individuals can also assist in helping themselves in this endeavour by not ignoring the fraud their insurers deal with on a daily basis. Being open, honest and transparent with your insurance company is key to stress-free dealings in this regard. Companies and individuals should not try to hide things from their insurers and must read and understand their policies. Even unintentional false claims cause problems for both sides and can result in delayed payments or unnecessary investigations.

Insurance companies are professional organisations that are run according to strict governance rules. Clients should treat them as such and also adhere to professional and ethical conduct in their own businesses, as well as any claims they have, thereby improving the industry and service levels for everyone – except the criminals.

For more information on the SAICB, go to www.saicb.co.za

www.securitysa.com May 2017 29
Can you screen integrity?
Increased screening solutions incorporate a variety of methods and processes.

Screening or vetting employees before employment, and in some cases during their employment at a company, is nothing new in the fight against fraud and poor placements. There are a variety of companies offering these services, which include checking that people are who they say they are and so on.

In some instances, companies are looking for more than simply verification, however. This is where other screening methods, such as social media or behavioural screening come into the picture, as well as the increasing requirement for integrity testing.

Jennifer Barkhuizen from Managed Integrity Evaluation (MIE) explains that research done on top performing companies over many years shows that these companies have one thing in common: integrity. More specifically, the benefits they achieve include:

- **Improved reputation:** Companies viewed as having integrity are seen as more credible to investors, clients and employees. Credibility means more trust, productivity, sales, market share and promotional opportunities. Companies with a firm commitment to a code of ethical standards build trust with their shareholders and public.

- **Enhanced customer loyalty:** In 1999, DePaul University studied three hundred large companies. The study found that companies that made an explicit commitment to an ethics code provided more than twice the value to shareholders over companies that did not.

- **Higher profitability:** Companies that operated with serious codes of conduct performed better than those without, in a variety of financial measures (The Institute of Business Ethics Report 2003).

- **Loyal and committed employees:** Many studies indicate that employees will have greater loyalty when they work for a company they view as having good values and ethical practices.

"Given the importance of integrity to companies, it then becomes important to have people with integrity," Barkhuizen says. "Psychometric integrity tests measure integrity levels and propensity toward counterproductive behaviour in the workplace."

There are various tools available to measure integrity, which are selected depending on the position and level of the candidate. She says integrity tests incorporate measures such as honesty, trustworthiness, credibility, violation of policies, rules and regulations, reliability, 
“With regards to MIE’s findings, our statistics for 2016 show that out of over 561 000 qualifications checked, 15.37% of the qualifications were found to be either misrepresented, fraudulent or cancelled.”

-Jennifer Barkhuizen, Managed Integrity Evaluation (MIE)

dependability, lying, denial, projection, justification, manipulation, attitudes, values, aggression, emotional stability, impulse control and work ethic amongst others.

**When is vetting required?**
Organisations should take the level and type of positions into consideration when doing background checks. Basic background checks include qualification checks (matric and/or tertiary qualification), credit record (whether the person will be working with cash or finances) and a criminal check.

A more comprehensive check can include employment reference, identity verification, driver’s license verification and competency assessments.

"With regards to MIE’s findings, our statistics for 2016 show that out of over 561 000 qualifications checked, 15.37% of the qualifications were found to be either misrepresented, fraudulent or cancelled," adds Barkhuizen. "We also found that Africa and International qualifications checked in 2016 carried a higher risk of being fraudulent, as candidates believe their qualifications cannot or will not be checked.

Our criminal statistics show that out of 741 560 criminal checks conducted, 10 % of candidates were found to have a criminal record.”

Organisations often face the risk of fraud and corruption when it comes to their procurement processes. Fraud scenarios can include:

- Conflicts of interest between employees and vendors,
- Collusion between vendors,
- Vendors or employees defrauding the company,
- Tender collusion and irregularities,
- Quid-pro-quo corruption,
- Vendor kick-backs and bribery,
- Bid-rigging,
- Financial mismanagement, and
- Price fixing and defective pricing.

**Take ownership to reduce fraud**
With widespread reports of corruption in South Africa, the onus lies with companies to make sure they follow the correct procedures to rid their companies of corruption. Barkhuizen says the first step is to conduct comprehensive background screening checks when taking on new staff or entering into new partnerships.

Vetting the procurement process within supply chains of organisations is very important. This is possible by using solutions to combat procurement fraud. One such solution is the use of technology to assist in identifying potentially corrupt relationships between vendors and employees.

“More companies are becoming aware of solutions available in the market to assist with identifying fraud and corruption," notes Barkhuizen. "It is up to companies to ensure they have the necessary tools available to combat fraud as criminals will continue to find new and ‘innovative’ ways to commit fraud.”

MIE has found the demand for background screening has continued to grow the last year, showing a 14 % increase in the uptake of vetting solutions by businesses. Conducting background checks gives companies peace of mind when taking on new staff members as well as assisting companies to break the cycle of corruption.

“Background screening provides a reasonable level of certainty to companies that the candidates they employ are who they say they are. Pro-active background screening also helps companies avoid increased recruitment costs and potential negative reputational and financial implications,” Barkhuizen adds.

"With ongoing development of various vetting solutions available to organisations, it is important to include candidate and supplier screening into your organisational strategic planning and partner with a reputable background screening company to assist with combating insider fraud.”

For more information contact Managed Integrity Evaluation (MIE), +27 (0)12 644 4000, info@mie.co.za, www.mie.co.za
THE FUTURE OF INTEGRATED SECURITY

It’s not uncommon to face the double dilemma of:
• Tight budget.
• Inefficient security system operations and maintenance.

You cannot compromise on the integrity of your security systems. In addition they should be integrated, but budgets do not allow for this. The answer is easy as Naxian Systems’ IoT (Internet of Things) XaaS (Everything as a Service) solution.

Naxian’s IoT XaaS provides you with:
• Predictive and preventative maintenance across all your security systems
• All your security services centrally and remotely managed
• Tax benefits as you move your system from CAPEX to OPEX
• Time to concentrate on your core business
• Reduced security labour costs
• Maximum uptime, resulting in reduced risk and enhanced efficiency.

To find out how Naxian Systems can save you time and money CALL +27 87 820 0620
Virtual access is real, but not an easy decision.

Biometrics in its many forms has become standard in many organisations, especially for access control and time and attendance (T&A) functionality. But biometrics can be used for much more.

In a few companies, fingerprint biometrics is also being used to control which employees have access to sensitive areas and sensitive functions where rogue employees are able to fiddle with a company’s finances. Yet, most companies still rely on passwords and ‘traditional’ virtual access control methods to protect bank accounts and accounting packages (and for virtual access on the whole) – most of them without managing the passwords people use or how they go about remembering them.

A few companies have taken the plunge and now use fingerprint biometrics to control access to their premises as well as their virtual premises. Instead of logging on with a password, a swipe of the finger is all it takes. Perhaps the growth of fingerprint access on smartphones has made people more aware of the possibilities.

Yet, despite the obvious security benefits of biometrics, many companies have no plans to change their operational systems to incorporate them, even in sensitive positions. Hi-Tech Security Solutions asked ViRDI SA’s Deon Janse van Rensburg for his take on why this is happening despite the growing global awareness of fingerprint biometrics.

Janse van Rensburg says that he is finding more companies enquiring about the convergence between physical and virtual access control systems. However, the enquiries seldom turn into a rollout. He says there are two main issues preventing virtual biometric access from becoming mainstream: cost and an understanding of how these systems work.

“Any converged system becomes an expensive capex exercise due to the complexity of the system, resulting in many man-hours in configuration and training,” Janse van Rensburg explains. “Users rarely have an idea of this complexity and rarely understand the impact that the deployment of such a solution will have on their businesses from a capex, administration, maintenance, infrastructure layout and IT infrastructure point of view.

“I call it the ‘Hollywood Effect’ and many other disciplines are experiencing the same where expectation rarely meets reality.”

More secure access?

Janse van Rensburg is clear that biometrics does add to the level of security. “As any IT security specialist will tell you, passwords to access computer systems are predictable due to users using passwords that they can remember and that are familiar to them. I recently read an article that provided examples of such predictable passwords which include names of pets, family members, birthdays etc.

“Another issue is that passwords are shared with other people, rendering the security features virtually useless. With fingerprint biometrics and the way the extraction technologies work, this becomes exponentially more difficult as fingerprint templates are extremely complex and should be encrypted to an AES standard.”

Additionally, he notes that since the same optics and algorithms are used for both physical and virtual access control, the virtual systems are as secure as the systems being used for access control and T&A. “The challenge is that physical access control systems, i.e. the biometric terminals, are very rarely the object of targeted malicious software and hacking attacks. This is where the difference lies, virtual systems are under constant hacking attacks and the safeguarding thereof cannot be handled by the biometric devices. If the network security can be breached then the system is vulnerable.”

ViRDI’s virtual access devices

When it comes to the options customers have from ViRDI for virtual access, Janse van Rensburg says the company supplies various PIV/iAFIS types of devices – dependent on the application. “Normally we would supply our FOH02 USB reader, but if the client has the requirement for FBI approved PIV/iAFIS devices they would be looking at the FOH04 and V-ScanFB series of devices.

“Our off-the-shelf software is actually a combination of packages. V-Bioguard interacts with Active Directory and replaces the password functionality with fingerprints. It provides a GUI for rights assignment, monitoring and reporting functionality. The second portion of the software solution is the MASS-Server, which allows the identification of a 1:1 000 000 (1:N) fingerprints in under 1 second.”

For more information contact ViRDI Distribution, +27 (0)11 454 6006, deon@virditech.co.za, www.virditech.co.za

Secure your solution using Suprema’s SFM6000 fingerprint modules that provide optimal fingerprint biometric authentication for various applications, e.g. access control terminals, time and attendance devices, door locks, alarm panels, safes, vending machines, automotive, ATMs and fast-growing IoT applications.

Loaded with a 1 GHz CPU and the latest Suprema algorithm, SFM6000 achieves exceptional matching speeds of up to 5 000 matches per second and has a massive user capacity of up to 25 000 templates.

The new optical sensor structure offers IP65-rated ingress protection as well as an operating temperature that has been extended to -15 to 60°C.

The series supports open source hardware platforms, including Arduino and Raspberry Pi, making integration easier for developers. The SFM6000 Series is backward compatible by maintaining SFM5000 & 3000’s form factor and sensor types, allowing existing customers to easily adopt the improved benefits of the series.

For more information contact Suprema: +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za
Management, risk management and assurance

By Colin Hill (PMP), business solutions manager: Risk Management Solutions, SAS.

A three-level risk management approach to fraud prevention.

Ever wondered why we can’t get a handle on fraud and why it keeps occurring? It’s actually simple to understand, but it’s also one of the largest issues many companies face.

Consider this scenario. A thief manages to get through a business’s security door while the guard is on a break. He dodges the surveillance cameras, sidesteps an unlocked security gate, forces open the safe and makes his getaway with thousands in cash. Or imagine a hacker breaks into your valuable private database and obtains access to all your customers’ account information. Criminals are experts; if they fail during the first hacking attempt, they will keep changing their attack methods until they are successful.

There are two ways to prevent fraud. One is to have a proactive fraud prevention system in place that uses a hybrid of analytical methods; the second is to make your fraud prevention strategy part of your risk management strategy.

Consider the fraud or hacker scenario
Fraud or hacking occurs when someone evades a security control or when a control is not working effectively. In the above example, an unlocked security gate made it easier for the robber to reach the money. In the online world, security controls include firewalls, anti-virus systems and network security programs, among others. A weakness in one control affects all other controls and opens a business up to possible fraud and other crime. Ensuring all controls are implemented correctly and are working effectively through continuous monitoring, forms part of risk management.

An effective risk management approach incorporates three levels, collectively known as combined assurance. This model ensures risk management processes are working effectively and that risks are being managed acceptably by incorporating three lines of defence – management, risk management and assurance – which can be a control department or internal audit. Crucially, the three layers must be coordinated effectively with clearly defined roles and responsibilities for all stakeholders.

Management
Managers are responsible for defining a business’s goals and implementing strategies to achieve them. Along with this comes the responsibility to outline and enforce policies and processes to overcome risks that stand in the way of achieving those goals.

Management must be informed on and understand the risks to their business. They should ask the right questions to get the right information that will empower them to react quickly and make effective decisions on risk responses. Ultimately, management forms the first line of defence against business risk and should take accountability for risk management. They should establish a culture of risk management, in which staff understand the risks and are trained on how to respond to threats. To assist them with this process, management should be updated daily on the level of risk for the organisation. They should have a daily view of the risk profile of their business and act on failing controls.

Risk management
A risk department, appointed by management, will develop, implement and oversee risk management methodology, policies and processes to ensure that risk is managed at acceptable levels. The team is responsible for identifying and monitoring risks and must proactively respond to any changes in the threat landscape.

The compliance department is tasked with ensuring the business meets all compliance requirements with applicable laws and regulations. The risk department consolidates the compliance effort and impact of non-compliance with the risk management efforts. They support and report back to senior management on risk, governance and compliance issues and ensure management is kept up to date, while staying on top of staff training and championing the risk management culture within the business.

Assurance
This is mostly provided by an internal audit and serves as an independent, objective assurance of the management of all risk management and compliance requirements. It provides assurance on risk management processes, the management of key risks and the effectiveness of controls in place, and delivers a reliable assessment of risks and reporting of risks.

Auditors evaluate whether management has identified key risks and has developed and implemented techniques and controls to address these. They provide assurance that risks are being managed and that processes and controls are in place and working efficiently. Auditors also oversee the implementation of risk management processes and advise on new developments.

Not only does combined assurance integrate the lines of defence to provide management with a complete view of governance and the risk management process, but it also assists with the making of strategic decisions based on a complete view of how risk and compliance is being managed throughout the organisation.

A business that does not adopt this three-line defence model is immediately at risk of breaching regulations such as the Protection of Personal Information (PoPI) Act.

Risk is an unavoidable part of doing business today. More processes are driven by technology, business is increasingly conducted online and the trading landscape changes at breakneck speeds. All this presents new risks while existing threats evolve and take on new forms. What we have learnt from the past is that companies that foster cultures of combined assurance, understand risk and take the necessary steps to address and prevent them, are more likely to weather a tough business climate.
Hi-Tech Security Solutions looks at a few of the companies and products you can expect to see at Securex 2017 from 30 May to 1 June at Gallagher Convention Centre in Midrand.

It's time for the 2017 edition of Securex and Hi-Tech Security Solutions has collected information from many of the exhibitors to provide our readers with a small sampling of what you can expect at the event. This year's Securex will be held from 30 May to 1 June at Gallagher Convention Centre in Midrand.

Apart from the various companies exhibiting, a few of which are highlighted below, other attractions include the New Products Display, the Securex Seminar Theatre brought to you with Hi-Tech Security Solutions, the FPASA InFireS Seminar, the ESDA breakfast and the SAIDSA Techman Competition.

New to Securex 2017 is the launch of a technical training component. Two morning and two afternoon sessions covering various topics such as surveillance for the entrepreneur (targeting end users and installers), IP surveillance and remote deployment (targeting entrepreneurs), storage know-how (targeting installers), and IP convergence possibilities and solutions in industry (targeting installers and end users), have been scheduled. See more at www.securitysa.com/56686n.

To provide a glimpse into what you can expect at the show from the various exhibitors, Hi-Tech Security Solutions asked them for an insight into their plans. Below is a brief overview. There will be far more at the show than we can fit in this article, so be sure to grab a copy of the Visitor's Guide at the entrance to the exhibition.

Top CCTV

Top CCTV is a CCTV superstore and wholesale supplier in South Africa for a full range of CCTV cameras, DVRs and surveillance products. It has been providing solutions to customers for more than 10 years and decided to showcase its solutions at Securex this year. Top CCTV will be showcasing solutions for vehicle mobile DVR solutions, solar powered long range beams, farm protection solutions, thermal solution, dash cameras single and dual view (Eagleye), home and business CCTV systems (Dahua & Hikvision), intelligent security and video analytics, and automatic license plate recognition system. Sales, marketing and technical teams will be available at the stand to discuss any questions you may have.

See more in Hall 2 Stand D22

Softcon

The core modules of Softcon’s solution is building management, with the main focus on access control, input/output monitoring, biometric solutions, smart card solutions, wireless communication, GSM communication, vending control, fuel control, solutions for visitor control, asset management, ID card production, cashless Point of Sale (POS) at canteens and Parking Point of Sale (PPOS).

Softcon has integrated key technology partner’s solutions as Morpho from Safran and contactless Smartcard Technology from HID Global amongst others, to provide secure identity and access solutions to our customer base.

See more in Hall 2 Stand B11

Hi-Tech Security Solutions will be at Securex once again with our range of security publications on the stand, from the monthly publications to the annual handbooks, including the CCTV Handbook 2017 which was published in April 2017, The Access & Identity Management Handbook 2017, the Residential Estate Security Handbook 2016 and the Hi-Tech Business Directory 2017. All Hi-Tech Security Solutions publications are published in print and online.

At a time when everyone is inundated with information and pressed for time, Hi-Tech Security Solutions provides relevant, credible information addressing Africa’s security challenges. We sift through the morass of information available and provide relevant insight into the various aspects of the industry to keep our readers informed. We also break down the articles published into electronic newsletters published twice each week that provide a quick read of the relevant news and opinions.

Visit the Hi-Tech Security Solutions stand and complete a subscription form while you enjoy freshly popped popcorn.

See more in Hall 2 Stand F63
BEST OF THE BEST

In a world of choices why not choose the best.
Suprema’s latest range of biometric readers provide exceptional matching performance, uncompromised security and accuracy along with top-notch usability.

Suprema
Leader in Biometrics and ID Solutions

SECUREX SA 2017 - HALL 2 - STAND A02B
enquiry@suprema.co.za | +27 11 784 3952 | neaMetrics (Pty) Ltd - Distribution Africa www.suprema.co.za
Trackforce

Trackforce’s GuardTek Suite of physical security management software provides simple, configurable solutions that increase productivity, create transparency and support growth. For more than a decade, Trackforce has been giving companies the ability to track, manage and streamline operations with intelligent innovation.

The suite, known as GuardTek, is fully customisable and easy to adopt, providing endless features for all operational needs. Ideal for posted officers, web-based GuardTek Post is designed for officer-manned checkpoints and lobbies. Features include post orders, incident reporting, digital OB book, time and attendance, training and certification, visitor registration, asset management and more. For mobile officers, GuardTek m-Post is an Android app that provides intelligent guard tours, photo and video enhanced reports, electronic OB book and activity reports, dispatch, lone worker protection, GPS tracking, visitor registration and more. All products come with live on-boarding and continued support at no additional cost.

See more in Hall 2 Stand D20

ESDA member breakfast

The Electronic Security Distributors’ Association (ESDA) will again be hosting a breakfast event at Securex, to be held at the Gallagher Convention Centre in Midrand at 7am on 30 May 2017. The guest speaker at the event will be Emma Sadlier, a media law consultant based in Johannesburg. The talk will focus on the legal and reputational risks of social media.

Social media is very much part of our lives and is used extensively by companies and their employees. While there are benefits in using social media, incorrect usage can have serious implications for both the company and the employee. Claiming ignorance is no defence or protection. Join us to gain a better understanding of the legal and reputational risks of social media within the business environment.

Emma’s areas of expertise include all aspects of print and electronic media law, with a particular focus on defamation, privacy and social media law. Her presentation will cover the social media landscape in South Africa as well as the legal considerations of using social media, including defamation, privacy, hate speech and intellectual property. She will also touch on common social media disclaimers (such as “tweets are not endorsements”; “I tweet in my personal capacity” etc.).

After the breakfast, guests are invited to visit the exhibition and stop by the ESDA stand.

The breakfast is free of charge and exclusively for ESDA members. To book, contact shirley@esda.org.za.

See more in Hall 2 Stand F42

Suprema

Suprema will be showcasing a handful of new products and solutions at Securex SA alongside its extensive range of IP access control devices, PC fingerprint solutions, mobile biometric platforms and integrated software solutions.

This year sees the launch of Suprema’s brand new flagship terminal, FaceStation 2. It offers uninterrupted face recognition regardless of indoor lighting conditions and boasts fast matching speeds and massive memory capacity. FaceStation 2, powered by Suprema’s 1.4GHz quad-core CPU, provides fast matching speeds of up to 3 000 matches/sec. Its massive memory capacity accommodates up to 30 000 users, 50 000 face image logs and 5 000 000 text logs.

The company will again have a wide array of new value-added integrations, including Cathexis Vision, NX Witness and Arteco on the VMS front and Impro portal, Avigilon Access Centre and Isona’s on the access control front, now all supporting Suprema’s new range. NX-Witness Hive VMS is developed by NetworkOptix, one of the top 10 fastest growing Software Companies in the USA by Inc.5000. Offering powerful VMS features and resilience in failover, it is considered one of the most advanced rapid search and user-friendly video management platforms in the world.

Arteco make the interoperability between systems, devices and different types of applications more intuitive and easy than ever imagined. From video security, access control, intrusion and fire detection to building automation, traffic control, parking management and beyond, this focus has opened up new and interesting opportunities in logistics, healthcare, critical infrastructure, transportation and large retail environments. Each of these operations may care about different information, but in the end, they are all focused on what is important to their environment: the event.

More specialised products on show include Live Scanners, ePassport Readers and Embedded Fingerprint Modules including the new SPM6000 series that provides record-breaking biometric authentication for OEM’s.

BioRugged, which has integrated Suprema’s high-precision fingerprint sensors into its mobile solutions, will show off a new age of integrated biometrics for mobile and rugged platforms ideal for KYC, biometric ID management and any application requiring state-of-the-art biometrics built for Africa.

See more in Hall 2 Stand A02b

Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences – whether making purchases, crossing borders, accessing e-government services or logging onto corporate networks. They also expect the ecosystems that allow this flexibility to be entirely reliable and secure. Entrust Datacard offers trusted identity and secure transaction technologies that make these ecosystems possible.

See more in Hall 2 Stand C06
Active Track

Active Track is a workforce management and reduction of payroll specialist. Its products put an end to your guards falling asleep, and ensure that patrols are carried out correctly. The products also guarantee control over your workforce, and ensure that you only pay for real hours worked.

Active Track’s success stems from reliance on cutting-edge technology, as well as cost-effective, all-inclusive monthly rental fees. The Active Track device offers real-time monitoring and two-way communication with your personnel. Designed as a user-friendly, tamper-proof and waterproof device, the Active Track can withstand the harsh conditions of your labour-intensive industry.

The device ensures that your guard or employee is awake, carrying out all patrols or duties correctly, and assisted in emergencies, by relying on its GPS, GSM and RFID capabilities, panic and duress functions and 24-hour support centre.

The FPX10 is a GPS and GSM-enabled system engineered to monitor time and attendance, and the location of assets. The FPX10 has improved and extended biometric capabilities, evidenced by its portable nature, extended battery life, accurate 21-point fingerprint and RFID reader, easy configuration to site requirements, and tamper-proof design. Functionality and captured data can be controlled remotely, via an online platform, and integrated into almost any payroll management system.

See more in Hall 2 Stand B15

Frank Street

Frank Street will be exhibiting the latest Milesight and Luxriot EVO product ranges as well as its own spy camera range. Milesight will introduce the Milesight PTZ bullet camera, a first of its kind, and the all-new 9/16/32CH PoE NVRs, as well as a high-speed dome camera. Luxriot Evo Global surveillance ecosystem solution not only offers 64-bit speed and all the necessary tools for setting up an absolute situational alertness system rapid response to events, but also introduces a central server governance hierarchy of all the components.

Frank Street will give away a 16ch Luxriot EVO licence each day at Securex. Clients simply need to register for the company’s weekly emails to be entered into the draw.

See more in Hall 2 Stand F06b

Procore Trading

Procore Trading’s Intimus 9000 Degausser uses most modern APT technology to erase information from hard drives. The Intimus 9000 produces an erasing field many times stronger than those produced by the read/write heads in hard drives and tape drives. The field strength, along with the encompassing magnetic field, ensures the data is no longer recoverable by computer or laboratory attacks. In addition, the INTIMUS 60 CC6 is a Level 6/NSA, high-security shredder with advanced i-control technology, automated lighting/reverse and forward functions.

See more in Hall 3 Stand J10
FLIR

FLIR announced four new security products recently. The new products include FLIR United VMS 8.0, the latest version of the company’s flagship video management solution (VMS), and three high-performance security cameras, including the FLIR PT-Series HD (High-Definition) thermal and visible camera system, the FLIR Quasar 4K fixed box camera, and the FLIR Ariel 3MP (3-megapixel) corner camera. All three cameras integrate with FLIR United VMS 8.0 and expand the company’s end-to-end line of security solutions.

The FLIR PT-Series HD is a dual-sensor camera system that provides superior, long-range perimeter intrusion detection regardless of lighting and environmental conditions. The high-speed, pan-tilt camera provides quick and accurate threat verification. The FLIR PT-Series HD offers either a cooled or uncooled 640x480 resolution thermal camera with a 1080p HD visible camera. Multiple high-performance thermal lenses are available, including optical zoom lenses up to 14X. The HD visible camera also features a 30X optical zoom lens with autofocus and low light capabilities. The FLIR PT-Series HD integrates with FLIR United VMS 8.0 and other major VMS software providers.

See more in Hall 2 Stand D09

Duxbury Networking

Duxbury Networking will highlight future-ready security solutions for physical and virtual networks at Securex. Under the spotlight will be a range of offerings designed to promote proactive security capable of adding significantly to the strength and viability of the corporate network infrastructure.

Underlining the need for more all-encompassing security protection to counter insider risks, vanishing trust boundaries and a lack of compliance management – as well as rising incidents of hacking, spam and spyware – Duxbury Networking will unveil new additions to its security armoury. These include network access control, security information management, and other leading-edge offerings that provide a holistic view of enterprise security.

According to Andy Robb, chief technology officer at Duxbury Networking, these solutions offer many benefits outside of the traditional security envelope.

See more in Hall 2 Stand D02

Powell Tronics

Powell Tronics is celebrating its sixth consecutive year as an exhibitor at Securex. The company’s stand will feature the new Morpho Extreme, the Morpho V2 Tablet (with Powell Tronics’ ATOM and PT-ROLLCALL) and Impro’s Portal Range. The company will also have a surprise offering in its IP intercom range. Business card draws and prizes will run regularly on the stand and the sales team will be on hand to demonstrate all of the products and discuss solutions.

See more in Hall 2 Stand B07

GeoVision SA

GeoVision SA will again be participating in this important annual security event and numerous new products will be on display, in particular its IP range.

A new high-tech, but very affordable mini dome and bullet range will be on display for the visitors to view and play with. Other products making a debut include the following: a facial recognition reader, long range tag reader (RU9003), IP covert fish eye and the PPTZ.

The face recognition reader can work with GV-AS Manager to create a complete access control system. Two types of operation modes are supported: face recognition or card.

GV-RU9003 is a Radio Frequency Identification (RFID) reader of ISO 18000-6C (EPC GEN2) standard. Designed for parking lot management, the reader can read a RFID tag within 10 m range.

The IR Fisheye Camera is an outdoor fisheye camera that allows you to monitor all angles of a location. The camera is equipped with an IR LED ring that provides infrared illumination under low-light situations.

The PPTZ is a two-in-one fish eye and PTZ camera. The camera offers 7 megapixels and allows for the zooming in to enhance picture quality.

At the end of the event, a visitor, by way of a lucky draw, will win a GeoVision IP camera valued at R 5000.

See more in Hall 2 Stand C04
JOIN MIRO AT AFRICA’S LARGEST SECURITY SHOW

As experts in the wireless IP convergence industry, MIRO’s major focus at this year’s Securex will be on the technology available to support your IP surveillance solution.

As the security industry trend is towards more IP based technology for its many benefits, MIRO’s 15 years’ experience in IP convergence makes them the obvious partner.

Uniview’s scalable portfolio consists not only of IP cameras, but up to 128ch NVRs and video management software; providing high-end capabilities and specialised features at an extremely competitive price.
**Desert Wolf Consulting**

Desert Wolf supplies rugged mobile solutions. With more than two decades’ experience, Desert Wolf strives to produce only the best logistical support trailers and complete military and commercial mobile surveillance solutions. The trailers include luxury camping and off-road trailers, search-and-rescue trailers, support trailers, disaster recovery trailers and advanced diesel-fired field kitchens. Desert Wolf also produces tactical unmanned aerial and ground vehicles to support surveillance outside line of sight. The Black Hornet surveillance drone system will be launched in South Africa during Securex 2017.

See more in Hall 3 Stand GG01

**Hitek Security Distributors**

The house of ProvisionISR, INIM Electronics & DUEVI, presents expert solutions to all your security requirements. Offering you the latest in advanced technology from CCTV and alarm systems to home automation.

Visit Hitek to view the quality of the upcoming 4 MP (4K) AHD cameras and also the latest (H.265) technology in its 4 and 5 MP IP camera and NVR range. Not only does this technology enhance your video quality, even with increased compression rate, you use up to 50% less storage space, 50% less bandwidth and 50% lower bitrate.

ProvisionISR also offers reliable analytics and POS solutions allowing easy integration with IP and AHD technology. The new powerful operating system OSSIA offers an easy interface, a new web interface and app which is user friendly and simplifies your workflow, setting you free from labour intensive operations.

See more in Hall 2 Stand A02c

**Keystone Electronic Solutions**

Keystone Electronic Solutions is an electronics research and development company. During Securex 2017 the company will be showcasing Project V, a ‘stream on trigger’ solution that provides centrally managed video surveillance, triggered either through security events or alarms, or via a video-on-demand interface. The platform provides digital video recording (DVR) which archives either on the central Project V server or at the remote site. Integration with customer systems, such as network management systems, access management systems, trouble ticket management and reporting tools, can all be provided through an open integration Application Program Interface (API).

See more in Hall 2 Stand E48

**Graphic Image Technologies**

Graphic Image Technologies (GIT), specialists in both remote and enterprise CCTV and control room technologies, will be showcasing its latest range of SerVision and FLIR products and solutions that feature innovative features, functionality and integration capabilities, bolstering security for businesses of all sizes.

The SerVision range, that will be displayed by GIT, includes applications and fleet management solutions that enable companies to keep an eye on both the driver and the surrounding area, allowing the control room to proactively monitor situations. For example, reckless driving can be monitored in real-time or potential highjackings thwarted. A new addition to the SerVision mobile range is the introduction of a new IP mobile NVR with the ability to record and stream video up to 1080p as well as integrate with telematics products such as Mobileye. This new model (IVG400N) will be on show.

In addition, GIT will also be showcasing a number of FLIR solutions including its thermal cameras and video analytics solutions for perimeters such as housing estates, solar farms, industrial or large warehousing environments and more. The advantages of these solutions include investment in fewer cameras to monitor a larger area more effectively as well as intelligence that alerts the control room to real threats proactively.

FLIR’s enterprise Latitude IP-based Video Management Systems (VMS) allows users to monitor and detect threats from any mobile device or platform across a number of sites and cities.

See more in Hall 2 Stand F05

**Linkqage**

Linkqage specialises in integrated connectivity solutions covering information technology, security, and the audio-visual solutions market. Connectivity goes far beyond the physical plug and sockets. Linkqage offers the expertise and the understanding that covers all the protocols and communication standards in today’s challenging interconnected world. From items as small as the Internet of Things (IoT) for your smart-home or office, to large data centres and hotel buildings, we know we have the right solution for you.

See more in Hall 2 Stand A10
SAIDSA will be hosting its third Techman Competition at Securex on Tuesday 30 May 2017, commencing at 10am. 24 SAIDSA-Certified Technicians will compete in the wiring and installation of an intruder alarm system consisting of 10 products on a display board, with strict judging criteria.

The technicians will be required to plan, wire, terminate, glue, harness and mark each product to a control panel according to SAIDSA minimum installation standards and within a specific time limit.

See more in Hall 2 Stand F43

Econz Wireless

Econz Wireless, a leader in the time & attendance, employee tracking, and mobile workforce management, will be demonstrating its timecard features on its stand:

- Time card collection.
- GPS tracking.
- Daily job journal forms.
- Reports.
- API and third-party systems.
- Administration viewing, and
- Custom support.

Stop by the stand for a free demo.

See more in Hall 3 Stand H03

Mitsubishi Electric

From the control rooms that keep traffic flowing, the utilities that light and heat our homes, to the emergency services that watch over our safety, Mitsubishi Electric builds the video wall systems that touch our daily lives.

Mitsubishi LED, DLP Video Wall Cube & LED, LCD Displays are designed and built to meet the most demanding requirements of the end user. Its Seventy Series LED Cube Displays offer the highest performance with the lowest power consumption figures in command and control room applications. Unique, fully redundant LED air-cooled projection engines and long-life fans deliver up to a remarkable 100 000 hours of maintenance-free operations, without expensive replacement lamps and with excellent environmental credentials.

As one of the first manufacturers to introduce display wall cubes using DLP technology in 1997, Mitsubishi Electric has a long history and extensive experience in the production of display wall systems.

See more in Hall 2 Stand C15

The legal and reputational risks of social media

Presented by Emma Sadleir

Date and time: 30th May at 7.00 am
Venue: Gallagher Convention Centre, Johannesburg
RSVP: shirley@esda.org.za

This prestigious, free-of-charge event is exclusively for ESDA members. ESDA members can enjoy a delicious hot breakfast and gain a better understanding of the legal and reputational risks of social media within the business environment before moving onto the Securex exhibition.

Book now as space is limited and seats are reserved on a first come basis.

Invitation to ESDA members
Jablotron will be launching its J150R wireless one-way repeater, extending communication range up to 300 metres in open areas, making it particularly useful where obstacles are apparent. A back-up booster box will increase the efficiency of wired installations and allows an increase from the original 500 up to 1 000 metres on the smaller system and an increase from 1 000 metres up to 2 000 metres on the larger system. A multifunction thermometer can be used as a standalone version or integrated into a Jablotron system. New passive wired and wireless cameras with a 90° angle are also being launched, together with a new wireless receiver – the J111R.

See more in Hall 2 Stand E32

PSS Distributors

PSS Distributors is a distributor of uninterruptable power supplies (UPS), inverters, batteries, solar panels, surge protection and generators. Full support is given throughout South Africa in all major areas: Johannesburg, Pretoria, Cape Town, Durban, Port Elizabeth and East London.

PSS Distributors will be showcasing its new SHC Series solar inverter at Securex 2017. The SHC Series solar inverter comes with features such as LCD display, battery input, AC input, solar panel input, build-in charge controller and AC battery charger. Monitoring the unit from the front LCD display allows you to view AC voltage, frequency, battery voltage and solar panel voltage. Units are easy to install and excellent for the security industry and remote sites. Setting up is straightforward, you simply connect your batteries, solar panel and mains or generator if available.

The SHC Series will use the solar panel to charge the batteries and supply the load, and if the panel voltage is not enough it will use the mains to assist. Three models are available: 1000 VA, 2000 VA and 3000 VA. Inductive loads such as fridges, small motors and fluorescent lights may be used on the units, keeping in mind that you have to size the units properly.

See more in Hall 2 Stand C08

Zonke Monitoring Systems

Key Systems offers several methods to store, audit and manage your keys and assets. Its personalised cabinets are used to secure a variety of sensitive items, however, keys still remain customers’ main focus for asset retention. The two most widely utilised methods for storing keys are through direct entrapment and/or Tamper-Proof Key Rings. Assets are assigned to one or more users based on pre-determined rules. PIN user access comes standard and many other access options are available.

See more in Hall 2 Stand E12
Everybody.

Everywhere.

Every day.

Ordinary days require extraordinary protection.

Find out more about the software behind the everyday at Securex South Africa, Hall 2, Stand D05 or at genetec.com/protectingeveryday

genetec.com

© 2017 Genetec Inc. GENETEC and the GENETEC LOGO are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.
Nemtek

The Nemtek Group manufactures a full range of energisers and fencing hardware and is a globally known and well respected company. With its pioneering products it has become the benchmark for the security electric fencing industry.

This year at Securex, Nemtek will be showcasing the Druid FG7 system, which has a seven-inch LCD touch screen that can be used to control up to 32 Druid two-zone energisers providing up to 64 zones. All energisers and their zones can be controlled via the FG7 controller. A further 31 Nemtek network IO relay cards can be controlled from the FG7. A graphic image of the site with its zones and the energiser and fence conditions which includes battery voltages and fence voltages can be displayed on the LCD screen.

Additionally, the Nemtek taut wire system measures tension changes on the fence wire in a particular direction and will set off an alarm if there is a threat of intrusion. The taut wire controller FG7 is a seven-inch LCD display screen can be used to control up to 31 taut wire sensors and network IO cards.

The combination of taut wires and a monitored electric fencing system creates a formidable detection and deterring barrier.

See more in Link Node Stand LN06

Integrity Control Systems

Integrity Control Systems specialises in security packaging & IME’s (integrity monitoring enablers) including tamper evident bags, specialised security tapes and labels, secure containers and totes, asset labels and uniquely serialised seals. All of these products help to identify point of liability and preserve the chain of custody where they are deployed. Unique standard number formats or intricate barcode structures are vital in the traceability cycle.

See more in Hall 3 Stand GG02

Rik Rhino

Rik Rhino Surveillance specialises in technical security and surveillance solutions. We aim to improve the safety and security of our clients with wireless technology and smart applications to meet our customers’ needs for technology-based surveillance systems. We provide solutions which are efficient, reliable, and durable, while still maintaining ease-of-use and practicality.

The first of the Rik Rhino products we will be exhibiting is a 14-megapixel camera with a waterproof design and a highly sensitive InfraRed motion sensor. This camera is conveniently compatible with the new Rik Rhino app (available both on Google Play and the App Store) which allows you to monitor review all images captured from your phone.

Our funky pocket-sized V16 Tracker will also be part of the show. It’s controlled by a master phone and comes with a fitted SIM card, making it perfect for emergency contact in any sticky situation.

Need something more hardcore? Then the waterproof GPS will be right up your alley. It has real-time tracking, an SOS alarm and caters to both business and personal purposes.

See more in Hall 3 Stand H09

TecSec

TecSec is partnering with IndigoVision at Securex this year. The company will demonstrate Control Center Version 14 which now provides for Light, Pro and Ultra offerings. Brand new to the IndigoVision stable, TecSec will showcase the BX thermal bullet camera. It includes all the reliable analytics that users have come to expect from the BX range, whilst also including temperature monitoring.

One IndigoVision Ultra 5K camera has the power of 10 virtual cameras, each with individually configured resolution and frame rate, meaning you can monitor large areas that require higher levels of scrutiny without the inconvenience, and cost, of physical camera redeployment. The Ultra 5K delivers outstanding image detail and performance in all lighting conditions.

IndigoVision’s Frontline 2 Bodyworn cameras will also be on show, ensuring every incident is seen, heard and recorded thanks to its incredible 28 hours encrypted on-board recording, 130° lens, HD video and high fidelity audio.

See more in Hall 2 Stand F23
The journal for decision makers who solve today’s security challenges

Covering:

- Access control
- Perimeter security
- System integration
- Identity management
- Integrated solutions
- Security services
- Surveillance
- Alarm and intrusion detection
- IT infrastructure for security
- Fire technology
- Risk management
- Cybersecurity

Available in the following formats

**The Print Magazines**

**Monthly issues:** 10 issues from February to November


**Annual Directory:** The Hi-Tech Security Business Directory

**Email News Briefs**

Twice a week our News Briefs cover the latest news and views. Fast, to the point and direct to your inbox, they are the ideal way for professionals to stay in touch with what matters to them.

**The Hi-Tech Security Solutions website**

www.securitysa.com

The place where professionals search for products, services and suppliers. With access to every article we have published since 2002, this is the ultimate security reference site.

Visit us in Hall 2, Stand F63 to apply for a free* subscription

*The publisher has the right to refuse a free application if the respondant does not qualify in terms of our target audience.
**Morse Systems Africa**

In an earlier era, business decisions were often made based on gut instinct, golf games, politics, and very occasionally market research. Since that time, organisations have moved away from this type of marketing and adopted a more research-backed, results-driven approach to business.

Take for example the use of key management systems. These systems are designed to store and control access to mechanical and other keys used throughout a facility. Keys can only be accessed by pre-authorised individuals with a proper code, badge and/or biometric identification. All access activity is automatically recorded and from this data, management has a complete history of who removed and returned which key and when. The data gathered from the automatic recording of access activity can be used to analyse trends to generate valuable, actionable intelligence for both physical security and business practices.

See more in Hall 2 Stand F11

---

**Tagtron Solutions**

Tagtron Solutions is a 100% South African company with a young, innovative research and development team bringing together the latest European technology and Proudly South African manufacturing expertise. In addition to offering locally produced products, Tagtron Solutions will showcase the following systems at Securex:

- **Tagtron AM EAS System**: The first and only AM (Acousto-Magnetic) EAS system to be fully designed and manufactured in South Africa.
- **Tagtron EM Retailor System**: Electro-Magnetic (EM) EAS system specifically designed for retail environments.
- **Tagtron Library SelfCheck Unit**: The attractive, lightweight Tagtron Compact is the only South African manufactured RFID Library SelfCheck Unit.
- **RFID Vehicle Access Control**: Coded RFID windscreen tags enable effortless (hands free), safe and secure access to and exit from facilities.

See more in Hall 2 Stand F30

---

**ProGroup**

ProGroup’s solutions include ergonomically centric design, as well as production at our fully equipped workshop, and installation on site, from a standard single person monitoring desk through to fitting out fully contained control and surveillance operations, complete with video walls, multi-level surveillance rooms, access portals and central command centres. The company custom designs to clients’ requirements.

See more in Hall 2 Stand B05

---

**SALTO**

SALTO is launching a new version of its JustIN Mobile solution combining BLE and NFC capabilities in a single app at Securex. With just a single app, depending on the type of mobile phone used, it will activate its BLE or NFC element, enabling users to open doors just by presenting the smart phone to the BLE or Mifare equipped handle set, cylinder, wall reader, etc.

Its secure encrypted technology is compatible with iOS (BLE) and Android (BLE and NFC), and users can receive their access rights instantly and remotely. All that’s needed is a 3G connection to the smart phone.

It automatically detects if a door is Bluetooth or NFC equipped and then uses its secure encrypted technology to open the door – even if the user has multiple access rights to several doors across different sites in the app.

The app also provides a powerful online system wherever the user is, converting any SALTO handle set to an online handle set as its bi-directional communication transmits audit trail and handle set battery status back to the operating system. It even sends the blacklist to the handle set, eliminating any cancelled cards or smart phones if they are used, even if the door is off-line.

See more in Hall 2 Stand C03

---

**Genetec**

Genetec is set to throw the spotlight on Mission Control, a unique Decision Support System (DSS) that will provide security professionals in Africa with new levels of situational intelligence, system visualisation, and incident management. Designed to work seamlessly with Security Center, the company’s unified security platform that combines video surveillance, access control, automatic licence plate recognition (ALPR) and communications management, Mission Control aims to simplify the operator’s tasks and decision-making process when handling routine activities and undesirable situations.

Ideally suited to meet the operational needs of larger, multi-site deployments in markets such as higher education and transportation, Mission Control will give operators a holistic, unified, and map-centric view of their entire security infrastructure. Mission Control will also move beyond the capabilities of traditional security platforms, enabling organisations to manage the entire lifecycle of incidents and situations, from monitoring incoming sensor data and detecting incidents, all the way through to resolution and auditing.

See more in Hall 2 Stand D05
PRODUCTS AND SERVICES

Biometric enrolment and verification
Rugged long lasting mobile terminals
evoting, KYC, Mobile POS and PTT solutions
GIS and business analytic systems

AI010
BIOMETRIC PAYMENT TERMINAL

Ruggbo 20
RUGGED BIOMETRIC HANDHELD

Visit us at the Suprema stand
Securex SA: Hall 2 Stand A02b
Cathexis Technologies will launch the latest features from its IP video management software, CathexisVision, when it joins the line-up of exhibitors at Securex South Africa 2017.

Cathexis will demonstrate some of the outstanding CathexisVision features that current Cathexis customers are already familiar with and reveal the latest enhancements that come with CathexisVision 2018.

Cathexis has added several enhancements to its Automatic Number Plate Recognition (ANPR) solution, including vastly improved recognition times and additional licence plate libraries, which will not only add value to global customers, but also comply with stringent global legislation.

The CathexisVision Advanced Video Analytics feature significantly boosts the value of any CCTV surveillance installation with the ability to configure analytics on both pre-recorded and live footage. In addition to its current capabilities, CathexisVision 2018 now includes: Snap Search, Smart Search and Activity Trails.

CathexisVision has launched a series of new Advanced VMD Algorithms that easily adapt to changing environmental conditions. This feature now includes: improved noise suppression and flare detection as well as advanced tamper detection. Additionally, CathexisVision 2018 comes with tailored solutions for all security requirements and significant advances to licensing requirements that will provide for a seamless user experience.

The CathexisVision design tools already allow users to design the best solution for each unique application. CathexisVision 2018 now features an updated and fully integrated design tool for system hardware and licensing as well as analytics loading on CPU in server selection.

See more in Hall 2 Stand B01

Amax Electronics offers security and communications installation and maintenance services to estates in Gauteng. It customises software solutions for clients and sets up command and control centres, as well as boom gates, turnstiles and access control compliant with SA legislation. Amax Electronics has 15 years’ experience in gated community security systems, integrating multiple systems.

Amax is launching its Estate Management System (EMS) at Securex. The EMS platform integrates all Amax systems and although it communicates with each system, each remains independent from the other.

See more in Hall 2 Stand B03

Dahua Technology brings high-value, full-service, video surveillance and comprehensive security solutions to professionals globally. It was ranked 4th in “Security Top 50” by A&S magazine in 2016 and ranked 2nd in terms of video surveillance equipment market share according to the 2016 IHS report. Dahua provides clients with comprehensive solutions in focus verticals such as intelligent traffic, safe city and smart building. Featuring customised technical innovations and end-to-end services, Dahua intelligent traffic solutions and others earn customers’ trust by best solving their problems. Dahua has a R&D team of more than 5 000 professionals to develop cutting edge technology solutions with high quality and performance.

See more in Hall 2 Stand C10

Hisasco supplies the entire spectrum of ‘detection’ including security X-ray machines with single and multi-view capabilities, advanced CT systems for automatic explosive detection, hand-held and walk-through metal detectors, radiation-free body scanners and explosive trace detectors. All its security detection equipment is provided with the applicable technology and in varying sizes depending upon individual requirements and applications.

See more in Link Node Stand LN04

ZKTeco South Africa is all about solutions. What can our products do for you? Not only will you get to experience the solutions first-hand, be certain that you will find the best solution at our booth. The ZKTeco Experience Booth, an integrated showroom for demonstrations of our security products and total security solutions offers you and your company the ultimate experience in security solutions. With demonstrations done by our experienced sales team and technical specialists, be certain that you will enjoy personal and comprehensive experience of the total solutions and functions.

With ZkBioSecurity, your ‘All-In-One solution’ upgraded systems are much more user-friendly and our Green Label range changes to more sophisticated products. You can expect to find new releases, like the new Biometric Full Height Turnstile within our launch of Entrance Control Products. We will also be launching new products for inspection control solutions and smart locks. Intelligent concepts within ZKBioSolutions, like our ZKBioFleet, ZKBioSchool and ZKBioGym are designed to showcase how each solution works.

Exciting competitions on the hour and three big prizes up to the value of R10 000 will be the order of our 2017 Securex exhibition.

See more in Hall 2 Stand A03
TRY THE SKYHAWK SURVEILLANCE EVALUATION DRIVES TODAY!

Get a 50% Discount on 2 SkyHawk Drives

To know more, visit us at Stand E22 at Securex
30 May to 1 June @ Gallagher Convention Centre
Experience the latest from Bosch’s integrated security and safety portfolios. AVOTEC video-based fire detection solution offers reliable early fire detection in critical and industrial indoor applications. It is suited as an addition in cases where common systems show its limits – identifying flames and smoke directly at the source and much quicker than common fire detectors, providing faster response times.

Bosch’s fixed dome, bullet and box cameras from the new IP 4000i, 5000i and 6000 series offer resolutions up to 5 megapixel and low-light solutions. With Essential Video Analytics as standard, captured video data can be repurposed for uses beyond security, such as gathering business statistics, making these cameras perfect for small and medium businesses.

The G and B Series intrusion control panels offer an integrated use of different physical security and safety domains (intrusion, fire, access, video systems) along with mobile access combined in one system and out of one box. At the same time, they are highly flexible in regards to customisation and integration capabilities.

See more in Hall 2 Stand C01.

New Teltron

New Teltron, supplier of the HID Fargo brand since 1995, offers years of experience in all aspects of this niche market. We stock the entire range of Fargo printers and consumables, from the current entry-level model to the industrial model, as well as consumables for all – even consumables for discontinued and legacy models. With our sales team boasting full technical knowledge and our technical section for servicing/repairs, the company is the Accredited Service Centre for Africa.

See more in Hall 2 Stand F21.

Gurtam

Looking for solutions to secure your fleet or assets? Visit the Gurtam booth at Securex 2017 and opt for Wialon GPS tracking system allowing to advance your fleet and asset security, improve driver safety and get a complete overview of the events taking place in a designated route or area.

Also at Securex, Gurtam is going showcase its newest solution flespi – an innovative backend platform specially designed to work with telematics data and make it generally available.

See more in Hall 2 Stand E50.

Sasstec Group

Sasstec has earned its reputation as one of South Africa’s turnkey solutions in the South African integrated security services market. Among the companies operating under the Sasstec Group the company will be showcased is SA Fence and Gate. Some of the products being exhibited include their highly-rated security solution bow fence and the best quality manufactured gates.

Also on exhibit, will be products and solutions from Integritron Integrated Solutions, a company that will be showcasing its unique blend of integrated electronic security systems and turnkey solutions in surveillance, access control, intrusion detection and automation.

Xtreme Intelligence Systems will also be exhibiting their software and technology solutions. Come and view an extensive library of software components, and a framework which has been developed and used to successfully foster rapid software development, integration and deployment in various industries.

Silverline Wire Products will be showcasing its steel and wire fencing related material such as a wide variety of diamond mesh, welded mesh, field fences and flatwrap, amongst other security related products.

See more in Hall 2 Stand D01.

MiRO

MiRO’s major focus at this year’s Securex will be on the technology available to support your IP surveillance solution, from high capacity microwave backhaul links right down to the last mile wireless connectivity needed for your security solution – regardless of size or complexity.

With the addition of Axcess-E into its portfolio of security brands, MiRO provides clients with an opportunity to expand their security portfolio. MiRO’s first wireless access control product considerably reduces installation time and costs by eliminating hardwiring. And because Axcess-E is locally developed, the turnaround time for delivery to clients is fast and efficient.

Complementing the company’s existing range of security solutions is the Uniview IP surveillance product range. Uniview’s scalable portfolio consists not only of IP cameras, but up to 128ch NVRs and video management software; providing high-end capabilities and specialised features at an extremely competitive price.

See more in Hall 2 Stand A02.

Quantum Design and Engineering

Quantum Design and Engineering (QDE) will exhibit its locally designed and manufactured Pepper Gas Alarm System, Protecto. This alarm system comes with optional GSM and Modbus capabilities, as well as a good track record for the last four years. This Pepper Gas Alarm protects your assets and buys time needed for armed response to respond.

As the intruder will not be able to enter the premises after the gas has sprayed, your assets will be protected against theft and vandalism, and you can rest assured that your belongings will still be in tack when you need them. This unit is ideal for warehouses, storage units, holiday homes, factories, containers, high sites and even your garage. It is easy to programme and you can set it up according to your needs using PIRs, sensors, beams or magnets or connect it to your current alarm system.

QDE will Launch their GSM PROTECTO Commander at the show, a 2-input, 2-output unit that will put control in your hands.

See more in Hall 2 Stand A14.
AFRICA’S LEADING SECURITY & FIRE TRADE EXHIBITION

DOES SECURING YOUR BUSINESS FEEL LIKE...

MISSION: IMPOSSIBLE?

ARE YOU READY TO ACCEPT YOUR SECURITY-READY MISSION?

You will gain access to:

160+ EXHIBITORS FROM OVER 10 COUNTRIES
FREE-TO-ATTEND SEMINARS
NEW TECHNICAL TRAINING COURSES
LIVE DEMONSTRATIONS

REGISTER ONLINE!

www.securex.co.za

For more information, contact:
Leigh Miller, Marketing Manager
Tel: +27 010 003 3060
Email: leighm@specialised.com

Brought to you by:
SPECIALISED EXHIBITIONS
MONTGOMERY
At this year’s show, Paxton will unveil the latest addition to their Net2 Entry range, the Net2 Entry Touch panel. This new door entry panel comes with a host of premium features, including a quality 7-inch colour touch-screen and personalisation options, making it suitable for more sites than ever before.

Visitors to the stand can also receive demonstrations of Paxton’s Net2 access control range, showing first-hand how straightforward Paxton products are to install and use. Comprising smart, simple door hardware and advanced, yet easy to use software, Net2 is an advanced PC based access control solution offering centralised administration and control of sites from one to thousands of doors and with up to 50 000 users. Paxton offers free, hands-on, training for installers across its Net2 access control and door entry range. Each session is designed to educate installers on fitting Paxton products, including fault finding, problem solving, and useful information regarding the administration and use of the systems. Paxton will also shortly be commencing Net2 Advanced training in South Africa. This course is designed for installers who have already completed their Net2 Essential training and wish to expand their knowledge of the more specialised applications for Net2. It will provide the opportunity for installers to expand their knowledge of Net2 and gain extra opportunity to upsell access control benefits to their customers.

See more in Hall 2 Stand C11

Axis Communications will have a strong focus on solutions tailor made for the retail and critical infrastructure verticals at Securex. One such product ideal for a retail environment is the AXIS FA series. The modular AXIS FA Series consists of separate units that comprise the AXIS FA54 Main Unit, AXIS FA1105 Sensor Unit with a standard lens, AXIS FA1125 Sensor Unit with a pinhole lens and AXIS FA4115 Dome Sensor Unit with a varifocal lens. The series enables cost-effective and highly discreet indoor surveillance of four closely situated areas using one camera system.

A highlight on the stand will be the Axis Q1659, its first to combine professional-calibre photographic imaging technologies from Canon with its proven surveillance technology. The camera brings a new level of ultra-high image quality.

The integrated solutions wall will showcase the Network Horn speaker used in collaboration with the AXIS A8105-E Network Video Door Station. The device doesn’t just let you identify and control who enters your premises, it connects to your system just like any other surveillance camera and records what’s happening outside your door.

As always, Axis has chosen two valuable Axis partners to collaborate with the company on its stand. These are Ngaro Intelligent Solutions, a company specialising in developing surveillance and control systems based on infrared imaging as well as Vaxtor, which develops high performance products and solutions for licence plate recognition.

See more in Hall 2 Stand A01
Abelard Underwriting Agency

Abelard Underwriting Agency has been providing specialist liability and motor insurance products to the security industry since 1998. Its recent partnership with underwriting managers Leppard and Associates and Lombard Insurance Company has led to new and exciting opportunities with regard to product enhancement.
See more in Hall 2 Stand F08

WMS

WMS provides offsite CCTV monitoring services as well as rental finance to system installer and integrators. By partnering with WMS you can now offer offsite CCTV monitoring services to your new and existing clients and enjoy monthly revenue share for as long as that contract runs without any additional overheads to your business.

The solution utilises a self-learning behavioural analytics software which learns the environment and flags abnormalities to the WMS control room. This allows our control room to pick up on suspicious activities and action them making our solution truly proactive as well as effectively identifying and managing incidents when they occur.

Our detection technology integrates into most existing CCTV cameras for minimal hardware requirements and capital outlay for maximum return on investment. WMS offers rental finance so that our partners are now able to offer their customers rental options whereby the customer avoids a large once-off payment and the installer get paid upfront.
See more in Hall 2 Stand D24
Dallmeier, Gallagher and AcoustAlert integrated

Local and International IT specialists meet in PE to dust down recently announced integration between Dallmeier and Gallagher.

Six project-orientated IT and software specialist met in PE this month to work through and implement the Dallmeier and Gallagher new concept integration from Dallmeier to Gallagher, and Gallagher to Dallmeier in what is dubbed as “source to third party and third party to source integration”.

This new model of integration or ‘mixture’ is known simply as ‘CASi’ or Complex Adaptive Systems integration. This is where individual subsystems work together to produce a result equal to more than the square of the individual sub-systems without losing their (the individual subsystems’) unique features, performance and identity.

The group of six took this a step further to mix in the unique features of Modular’s AcoustAlert perimeter detection system to further enhance the CASi and value modelling of Dallmeier’s SeMSy video management systems and Gallagher’s Command Centre access and alarm management platforms.

This new model of integration is unlike previous concepts of PSIM (Physical Security Information Management) integration where one software suite provides a platform created by middleware developers to manage multiple unconnected security subsystems and devices in a partial manner.

Cliff Rose from Modular says this is groundbreaking concept engineering designed to deal more conclusively with emerging complex security problems which includes perimeter detection, alarm management and video verification, and tying this up with advanced situational awareness (ASA) options. The interoperability of primary systems like Dallmeier’s SeMSy and Gallagher’s Command Centre ensures that the reliability of these platforms and the years of development are fully optimised, more than if they operated on their own.

E.P Smit from Dallmeier Germany says that because all Gallagher events are logged and can be expertly linked to video footage, this enhances the search and reconstruction of video evidence to produce a conclusive video archive of Gallagher event-driven activities. Within SeMSy footage is bookmarked and linked through Pguard which is Dallmeier’s event and incident logger. All Gallagher event conditions are available within SeMSy though an OPC bridge and interface server giving the client the ability to link any access or intrusion alarm within Gallagher to any video footage or sequence in Dallmeier.

Technical manager David Massop from Gallagher says that the New Zealand office implemented the Dallmeier ActiveX integration options which provides video verification for any alarm or activity event within Command Centre. On its own, the Gallagher Command Centre is a powerful software solution designed to help manage access control and intrusion detection on your site. This is now further enhanced with the corresponding video verification footage which allows for an intuitive operator response.

Dallmeier’s local representative from Johannesburg, Riaan Kruger, was also part of the six-man CASI team along with Nic van der Walt, Modular’s operations director, and Sidney Paton, Modular’s software engineer responsible for the AcoustAlert software development and integration. Modular has been a Dallmeier international partner for more than 20 years and is also certified in the Dallmeier SeMSy VMS support programme run from Germany.

“The AcoustAlert (PIDS) interfaces directly into SeMSy through a common point user-interface or directly into Gallagher I/O control to give the user application flexibility of the whole integration process,” says Rose. “We see this integration of world leading products as positioning Modular to compete for larger integrated projects in the justice and correctional services sectors as well as the renewable energy, rail, and private sector industrial and commercial markets.”

“The joint integration work we completed here once again highlights a key feature found in all Dallmeier technology: its easy connectivity with and interoperability across different platforms. In an increasingly networked world, this is a decisive factor as customers often demand cost-efficient but nonetheless highly reliable solutions for existing systems to integrate with technology upgrades,” says Smit.

Modular’s offsite control room activities remain a key business area and is also under constant development as technologies evolve and user requirements become more specific with measurable results.

For more information contact Modular Communications SA, +27 (0)83 456 9542, cliff@modular.co.za, www.modular.co.za
System Integrators

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

BT-SA
BT-SA offers end-to-end security solutions that include design, installation and maintenance of high-tech integrated products. Its in-house team of experts can integrate all fire and security systems into a single platform with one-user interface capabilities. These products include a variety of fire detection and suppression, evacuation systems, access control, CCTV and all intruder detection types.

Tel: 0860 105 183
sales@bt-sa.co.za
www.bt-sa.co.za

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

G4S Technology
G4S Technology designs, installs and maintains fully integrated surveillance security and Life Safety systems, protecting customers with various requirements. We secure and protect a range of facilities including small stand-alone offices, schools, large multinational organisations and even high security government facilities. Our sector approach allows us to tailor and integrate solutions for customers.

Tel: +27 (0)10 001 4500
tim.timmins@za.g4s.com
www.g4s.co.za

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

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

To list your company here, contact Vivienne at vivienne@technews.co.za or +27 (0)11 543 5800.
Integration enhances mining security and operations

Developing a security management system for the mining sector is not a simple task. Still considered a critical contributor to the local economy, the South African mining sector boasts a total annual income of R550 billion and is one of the country’s biggest employers. With South Africa’s economy built on gold and diamond mining, the sector is an important foreign exchange earner, with gold accounting for more than one-third of exports. Gold mining in South Africa also accounts for over 10% of the world’s gold production.

Headquartered in Johannesburg, South Africa, AngloGold Ashanti is the second largest global mining company with 19 gold mining operations based in nine countries, as well as several exploration programmes in both the established and new gold-producing regions of the world.

Developing a security management system for the mining sector is not a simple task. Mining operations are typically characterised by multiple sites in remote locations, often in hostile environments with limited infrastructure.

In addition to preventing incidents that involve security breaches and theft, the security or risk management plan must take a number of other factors into consideration, including occupational health and safety and the threat of labour unrest by hundreds of workers on site.

A typical mining security management system would combine various aspects of security features, including: manned guarding, CCTV surveillance, access control, perimeter security, fire protection, alarms, X-Ray systems and plant management systems. AngloGold Ashanti with its operations based throughout various countries in Africa is no exception.

Surveillance solution from Cathexis

AngloGold Ashanti’s African CCTV solution includes some 2 500 cameras distributed across about 12 geographical locations, including mines and plants in South Africa, Ghana, Tanzania and Guinea. Cathexis Technologies has provided AngloGold Ashanti with its flagship video management surveillance system for the past 15 years, ensuring that all of these sites are accessible remotely for support and centralised monitoring capability using the CathexisVision. While security is certainly a high priority for the mining sector, risk management has to work closely with other departments to streamline operational costs effectively and increase return on investment. Therefore AngloGold Ashanti was recommended a solution which, through its integration capabilities with third-party systems and powerful analytics functionality, could generate actionable information, not only for security management, but all mining operations.

CathexisVision provides a management tool that enables operators and managers to function in a multi-tiered control environment with multiple CCTV cameras installed on different sites and locations. The system manages these sites from a central command centre.

“During our 15-year working relationship with AngloGold Ashanti, we have seen the company demonstrate an exceptional willingness to embrace the power of a fully integrated security solution,” says Gus Brecher, MD of Cathexis Africa and business development and marketing director for Cathexis Technologies. “This leading-edge thinking has provided us with the ability to create a sophisticated and fully integrated infrastructure and security management system throughout the organisation’s African mining operations.”

Video management software features

Some of the main features of the CathexisVision installation include:

- Video analytics that provide triggers based on certain events or actions to the system and enable user-defined action.
- Integration that enhances the effectiveness of the system by enabling predetermined actions based on information received from integrated third-party systems, including access control, fire panels, alarm panels, X-Ray systems and plant management systems.
- The interactive graphical interface provides a visual representation of one mining site or multiple sites. Users can also navigate multiple sites throughout the enterprise with the map facility.
- Health monitoring provides continuous monitoring of all the components, including hardware and software integrity, and provides automated warnings of any possible impending failure. This allows maintenance engineers to perform corrective maintenance before the system fails.

Feature migration

One of the major requirements of the CathexisVision installation at the AngloGold Ashanti mining sites has been the need to upgrade the CathexisVision software on an annual basis to ensure that the installation is always kept up-to-date with the latest international trends and developments, and that the surveillance system is reaping the full benefits of the latest CathexisVision features.

Given that Cathexis has worked with AngloGold Ashanti for over 15 years, this has necessitated the need to migrate an analogue CCTV system into a digital, networked solution, as per global market trends. However, given the significant investment in surveillance systems, Cathexis is able to apply its technology and integrate with existing analogue systems, bringing them up to speed with the latest IP technology. In addition, CathexisVision supports the most popular brands of IP cameras, using both ONVIF or proprietary protocols.

“Working with the security management team from AngloGold Ashanti has been a significantly rewarding experience,” says Brecher. “AngloGold Ashanti is one of the most forward-thinking and innovative organisations operating in the mining sector today, and with a willingness to embrace the features and competencies provided by the CathexisVision Technology, we’ve had an exceptional opportunity to demonstrate the effectiveness, efficiency and true capabilities that CathexisVision provides.”

For more information contact Cathexis Africa, +27(0)11 240 0800, sales@catfrica.co.za, www.cathexisvideo.com
Bosch expands MAP 5000 range

Bosch has expanded its range of intrusion alarm systems with two new solutions made for small to medium-sized applications such as schools, small offices, smaller retail stores or art galleries. The new Modular Alarm Platform (MAP) 5000 S and 5000 SC complement the two already available MAP 5000 systems for larger applications such as airports or shopping malls.

The two new systems are compatible with the full range of peripherals for the Modular Alarm Platform such as keypads, modules and sensors, and are scalable up to 600 addresses and 127 addressable Local Security Network (LSN) devices. Thanks to their modularity, they can grow to cover as many as 500 areas and 1000 users. The MAP 5000 S and the MAP 5000 SC are controlled via up to two touch screen keypads.

Both new intrusion alarm systems are designed to be easy to install and integrate into the building’s management systems while providing robust and reliable security. Thanks to the self-learning mode of the LSN bus, the system can be put into operation quickly – a short circuit or interruption on the LSN loop does not lead to system failures. Using the Open Intrusion Interface (OII), the new systems can be integrated into the Building Integration System (BIS) from Bosch, or others.

The MAP 5000 S and MAP 5000 SC comply with international security standards and are certified in accordance with EN 50131 Grade 3, VdS class C and SES. AFNOR 3 shields are in preparation.

For more information contact Bosch Security Systems – South Africa & sub-Saharan Africa, +27 (0)11 651 9600, security.systems@za.bosch.com, http://africa.boschsecurity.com

Glass break detector

Tyco Security Products introduced the Visonic GB-502 PG2 Glass Break Detector with proprietary microphone technology that provides reliable identification of broken windows or glass doors.

Ideal for the home or business, the detector is designed to identify only true breaking glass by analysing patterns of sounds using a three-stage, multi-level classification process, essentially eliminating the issue of false alarms. Early and accurate detection ensures users that their property is not only more secure, but also gives them notice to act quickly so they can protect against damage, added costs and potential insurance liabilities from temperature extremes, water infiltration or other harmful environmental factors.

The Visonic Glass Break Detector can also help to reduce costly energy consumption with its ability to monitor environmental conditions. A single detector, which can be wall or ceiling mounted, is able to protect rooms up to 120 square metres, eliminating the need for individual glass break detectors on each door or window. Low-power operation extends the battery life for up to five years, reducing maintenance costs.

For more information contact Tyco Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com

High-Definition Ground Radar

The AdvanceGuard high definition radar security surveillance solution is an innovative alternative to high-cost manned guarding and provides a reliable, low cost solution that delivers continuous automatic perimeter surveillance. From small sites to large complex compounds, AdvanceGuard provides the most comprehensive security surveillance system available.

- Unrivalled detection performance & low false alarms
- Operates in all weather and light conditions
- Automatic perimeter & wide area security
- Complete situational awareness

CALL 012 142 0000 NOW!
or e-mail info@mass-solutions.co.za
www.mass-solutions.co.za
From the inside out

By Andrew Seldon.

Spotter defends long perimeters from the inside out.

In the traditional layered approach to security, securing the perimeter is a critical aspect of the full security solution. When it comes to large areas that need to be secured, however, such as one finds on mines, ports, game reserves, borders and large industrial plots, protecting your perimeter is a complex task.

Charles Harrison, MD of local system integrator Secu-Systems explains that while there are many products that can detect a perimeter breach and raise the alarm, there are few which can then track the suspect once inside the perimeter of large environments. Due to the large open spaces of these environments, by the time security personnel get to the breach location, the suspects will have moved off and can be anywhere on the site.

Secu-Systems’ Spotter is a solution to this problem that uses thermal and visual surveillance cameras, as well as Panoptes MTI software to set up a perimeter protection solution from well within the perimeter.

The system needs to be set up on a high site where it can view the area to be monitored, and from where it provides 360-degree protection.

Due to the combination of visual and thermal cameras, the system works 24-hours per day, irrespective of light or weather conditions. Moreover, the Panoptes software, developed for the Australian military, will identify intruders from kilometres away and then track them as they breach the perimeter and move into the area. Security personnel can therefore be sent to their exact location.

Security and safety

Spotter can also be used to monitor specific sites to prevent theft of anything from fuel to pipes and cabling, as well as malicious damage to property. Keeping an eye on the movement around vehicles and diesel pumps will quickly identify unauthorised movement after hours, for example, preventing theft and damage.

From a safety perspective, the Secu-Systems solution also provides an additional layer of security in dangerous environments. In the mining field, for example, illegal miners are a problem throughout Africa and are often injured or killed during normal mining operations – such as dumping. With the solution in place, Harrison says it is easy to identify where people are and ensure there are no injuries and therefore that the mine will not have to lose money from being forced to shut down while an investigation is conducted.

Harrison provides an example of a solution installed at a mine with a perimeter of well over 50 km. Ten Spotter systems (in other words, 10 camera installations at high points) were installed and they cover the whole mine, and area of about 150 square kilometres.

---

Image 1

Image 2

Image 3

Image 4
Another example he offers is from a West African mine in Guinea. This mine is plagued by over 100,000 illegal miners. Six Spotter systems were installed to cover an area of about 63 square kilometres. Image 1 shows an illegal mining camp on the mine, while Image 2 shows a few of these miners at work.

In all cases, Harrison says the savings customers have experienced as a result of installing the Secu-Systems’ solution has been substantial. In fact, he says that not only is the solution the cheapest per square metre in the industry, it delivers the best in terms of measurable reduction in losses in the mining environment – not to mention the life safety aspect.

Self-sufficient
Spotter solutions are housed in self-sufficient containers fitted with their own power reticulation, which includes solar panels mounted to the roof of the container and battery banks installed within the container. Security systems are integrated with the camera solution and include wall-top and/or additional freestanding electric fencing with energisers operating off the internal power reticulation. All sides of the container are equipped with nozzles and high-pressure hydraulic piping. It also includes wireless communication back to a centralised control room (as long as line of sight can be attained).

The cameras can detect movement in as little as four pixels. Therefore, with high-powered, PTZ thermal cameras placed on high sites, intruders cannot hide and are followed throughout the location until removed, thus giving management complete 360-degree situational awareness and peace of mind.

For more information, contact Secu-Systems, +27 (0)11 794 7834, charles@secusystems.co.za, www.secusystems.co.za
Reduce false alarms with verification

By Allyson Koekhoven.

False alarms mean that valuable resources, which should be available to tackle real crimes, are tied up in unnecessary and futile time-wasting exercises. The result is increased frustration levels, a possible delay in reacting to actual events and increased operational expenses. Hi-Tech Security Solutions chats to two video verification vendors about how this technology addresses these issues in a seamless and intelligent manner.

Rory Webber of Videofied explains that the company first pioneered video verification technology in 2001 and has continued to refine its product offering to cater for both indoor and outdoor applications. When a standard PIR activates an alarm, it automatically triggers a surveillance camera which records a 10-second video clip and sends it to a central monitoring station for action.

Webber points out that the company operates 150 control rooms countrywide, with each of the operational personnel trained to make an informed decision based on the video clip. The outcome of the video clip survey is that false alarms can be readily and quickly identified, thereby ensuring that appropriate armed response resources are allocated to an event when an alarm is verified as being genuine, or are instructed to stand down in the case of false alarms.

According to Webber, the popularity of video verification has not only grown at a rapid rate in South Africa, but more recently, cross-border clients are seeing the benefits attached to this technology. Video can be transmitted through a number of common avenues, including IP network routers and GPRS.

More than security

In addition to reducing the number of normal false alarm alerts, video verification is being increasingly used as a tool for fault finding in the manufacturing sector. By moving cameras and PIRs to areas where they are most functional in terms of determining issues, operators can uncover event trends and programme the system to activate a PIR each time a pre-selected event occurs. This results in decreased operational costs.

By integrating video verification into other technologies, controllers are equipped to make educated decisions. An example Webber cites is that of a perimeter fence equipped with a vibration sensor. When a person climbs onto the fence, an alert is sent to the control room. Traditionally, a security officer then has to walk along the fence line until he determines what has activated the sensor.

Integrating an outdoor video surveillance camera with the vibration sensor means that the camera can be automatically activated to run a video clip and send it immediately to the control room when the sensor is activated. The operational personnel can then decide if the alarm is genuine or not and in instances where there is a breach in security, it will allow the controllers to determine the appropriate number of security personnel and the correct level of response, suitable in that scenario.

Once received and actioned in the control centre, the 10 second video clip can be sent to any valid email address. Webber adds that the low cost of data usage in the Videofied product range has always been the company’s strategic advantage.

Videofied is fully secure with bi-directional communication and requires both a username and password.

Various solutions

Ruan Fourie from Elvey says that the company’s Risco IP cameras are integrated with alarm systems in various types of systems. Firstly, there is PIR/camera integration, with a snapshot relayed to the control room, while another system allows the end user to view the camera images on a mobile or desktop device, with replication of the image occurring in a control room.

Fourie says that typically, video verification via the cameras entails the placement of the majority of the cameras on the perimeter of property, together with one or two cameras on the interior of buildings. The Risco IP cameras feature two-way audio. This is useful for control room personnel to audibly notify a perpetrator that, for example, an armed response unit is en route. Similarly, parents can communicate with their domestic workers or children from a remote workplace.

In all instances, permissions are set up in advance to allow control room personnel to access the camera feed when an alarm is triggered during an active armed phase, or by pressing a panic button on the premises. By limiting remote control room viewing to permissible events, homeowner privacy is ensured.

In addition, the homeowner can set up the system to allow the authorisation of specific parameters in terms of areas of coverage. For instance, any viewing of bedrooms and pool areas could be disallowed. “End users need to understand that there is the risk of privacy invasion and conversely, where zones are disallowed, there is the risk of a valid event not being adequately covered. It is therefore important to reach agreement on areas of compromise in terms of privacy versus and personal safety and security,” says Fourie.

Because all data is sent through a secure server hosted in the Cloud and then on to the control room, data security is ensured and is only accessible via end user permissions. The Risco cameras are integrated with building management systems and live viewing is firstly provided via Risco IP cameras using VUpoint, a Cloud-based platform that uses IP cameras to provide real-time video streaming in response to alarm triggers or on demand.

Video verification not only reduces costly false alarms, but provides for faster emergency response, enhances personal safety levels, provides more accurate confirmation of emergency status and has been proven to increase the apprehension of suspects.

For more information contact
- Videofied: www.videofied.com
- Elvey Security/Technologies: www.elvey.co.za
Wireless PIRcam alarm verification

Evidence in full colour
Securing just one aspect of your home or business is no longer an option in a market where criminals are seemingly always one step ahead. As a result of this, local infrastructure supplier BT-SA notes that the popularity of integrated security systems is on the increase, particularly as a smart home or office solution.

“Just to secure the perimeter of your home or business, but neglecting to monitor access control is not an option these days,” states Erik Jordaan, MD at BT-SA. “Security needs to be viewed as an onion concept, where multiple layers make up the whole, and only one layer does not make for an entire solution.

“By applying these layers of security, management challenges do arise, particularly when it involves various security products and devices. Which is where an integrated security line of action to smart homes really comes into play,” adds Jordaan.

Security for home and business

Take back control of your home and business by investing in integrated security solutions.

There is no doubt that applying a layered approach to your security environment, and then linking these components into a centrally managed environment, is the way to go. By linking your CCTV cameras, electric fence, access control and then your intruder detection systems to a single management unit that you can review remotely from your mobile device, enables you to respond to threats more effectively.

Let’s take this a step further and integrate it into your smart home solution to have a birds-eye view of your home, all from a mobile platform of your choice, accessible at any time and from anywhere.

“Security solutions shouldn’t baffle you. They should empower you. If your alarm goes off at home and your armed response calls, how many times have you rushed home to find that a window was open or a pet has triggered one of the sensors? With a mobile integrated solution, you can make a calculated and informed decision on how to react to each incident,” he says.

Smarter technologies

According to Jordaan, the technology exists today to ensure that your smart home also boasts smart security. Alerts can be tailored to advise you of a perimeter breach, a gas leak, a power outage or even a fire. By linking these systems to a central management unit that sends notifications via the Internet is where the real magic happens.

For commercial businesses, CCTV cameras are nothing new. But now, linking cameras to video analytics, facial or licence plate recognition, adds real value to the business. Traditional fire alarms are great, if you have someone on the premises at all times. By adding thermal sensors and integrate it to your overall security management system, you can react to a fire before it takes hold of your premises and cause costly damages.

“Connect your fire detection and suppression devices onto a power management system and be alerted of anomalies in the environment. This also allows you to remotely switch off the power to avoid potential problems,” urges Jordaan.

Security has for many years been a grudge purchase – you acquire systems purely for insurance purposes. However, with integrated smart security solutions you take back control and you can make smart decisions for your home, small office or business.

For more information contact BT-SA, 0860 105 183, sales@bt-sa.co.za, www.bt-sa.co.za.
A ‘lawful’ approach to Wi-Fi

How connectivity can benefit law enforcement.

The Internet of Things (IoT) is challenging the way people live and work, and how government and businesses interact. In fact, this new ecosystem is creating the foundational building blocks for smart cities where traditional models of service delivery are being challenged.

Says Riaan Graham, sales director for Ruckus Wireless sub-Saharan Africa: “While the move towards ‘smart’ is slow as infrastructure and connectivity needs to be deployed to truly drive an interconnected eco-system, for those that are moving towards a more mature model, the benefits are undeniable across all services – including law enforcement.”

“If we look at today’s judiciary system, often, judges have to rely on alternative links as GSM connectivity is not always possible due to various technical challenges. Use of a Wi-Fi hotspot could result in easy, quicker access to legal and other information that could be critical in a trial. This could have a significant impact on the productivity of the court.”

This fast and reliable Wi-Fi has the added benefit of providing journalists with the means to file stories sooner and get breaking news out more efficiently. Consider also the potential of providing legal teams who might not have the resources of larger firms with online access to research that can assist in their preparations.

“Suddenly, technology becomes an equaliser with those legal professionals coming from underprivileged communities having Internet connectivity they might not have otherwise had to refine their case work. But these benefits extend beyond the parameters of the court,” adds Graham.

Police stations often have to rely on expensive satellite access to file reports and stay updated on various legal and security matters. Creating a network of Wi-Fi hotspots that not only cover the police station, but key areas of the community, could provide a much-needed boost to reducing crime. Additionally police officers in the field can be fitted with hidden cameras on their uniform as well as a dashboard camera in the police car – providing accurate evidence of incidents that can be helpful in a trial.

“Such a Wi-Fi network gives community members an opportunity to engage more directly with local police and send out alerts on any criminal activity they might witness or even call for medical services when seconds matter. Extending this Wi-Fi access to a community centre provides additional opportunities for education, employment, and even the enhancement of existing crime watch programmes.”

Wi-Fi will give police in these communities the capability to check on suspect IDs and vehicle licence plates more effectively and cheaper than before. This also means that police officers who roam the neighbourhoods can leverage VoIP services to create community-wide alerts should the need arise.

Streamlining the processing of information, filing of reports, responding to community queries, and engaging with officers in the field are all valuable enhancements brought about with the availability of Wi-Fi.

“As we have seen from consumer and business perspectives, Wi-Fi access empowers users to find different ways of doing things. Having access to the Internet and all the related information it provides leads to a smart way of doing things and helps government embrace the concept of smart cities. Even in sectors of the market where Wi-Fi has not been typically seen as necessary, it is incredible what innovation this connectivity can unlock,” concludes Graham.
Locally made server cabinets and racks

By Brett van den Bosch.

Local manufacturers offer various cabinets and related equipment made for the South African and international IT markets.

The modern security industry is continually coming up with high-tech solutions tailor-made for solving very particular challenges. As the adoption of networking technologies became more widespread, at least it wasn’t necessary for the security industry to reinvent the wheel as far as networking equipment goes. The servers, routers, switches and cables already widely used in the IT sector were fit for purpose, and were gratefully adopted. The same goes for server cabinets and related equipment essential for any IT infrastructure.

Buying a server cabinet is a lot like buying new clothes. First you need a clear idea of the form and function you’re after, before you even start shopping around. Brand names are more important to some than they are to others, and as with clothes, there are several globally renowned cabinet manufacturers that you really can’t go wrong with. Next you find something in a colour that catches your eye – in the case of a cabinet that is typically a simple choice between grey, black, beige or grey. Accessorising is a must, so trays, power supplies, fans, plug points and the like must all be catered for.

The question of cost is a common thread running through all these decisions, and for the civic-minded there’s also the desire to support locally made products. Local manufacturers are addressing both these concerns by offering ranges of cabinets and related parts made for the South African market. Hi-Tech Security Solutions profiled two of them to learn what they have to offer.

ModRac

Located in Midrand, ModRac (a division of Datanet) is built around making and designing all metal products for the African market. It offers a full range of wall boxes, cabinets and accessories for the ICT market, including IP-rated units for harsher conditions. Its fully-fledged design team is able to take on most engineering jobs, including security-specific, specialised brackets for cameras and kiosks.

According to divisional director Craig Luck, ModRac came up with the ‘DC in a box’ concept which allows smaller or remote companies and branches a cheaper, more effective option to building an entire data centre. Today this concept has been adopted by all cabinet manufacturers locally and internationally, he says.

In exploring some of the bigger issues and challenges facing local manufacturers of this type, Luck points out that the Chinese market offers products at very cost effective prices, while the American and European markets offer top quality, high-end products which are seen as superior.

“Both these perceptions are incorrect though,” he insists, “as ModRac offers a good quality, cheap product that competes well on price and a high quality, top end product that competes with anything out of Europe or America.”

Luck stresses that there are definite advantages to dealing with a local cabinet manufacturer: “Locally made racks offer design tweaks and quick alterations that cannot be done by the imported solutions. These are often overlooked when the initial tenders are being awarded. The ability to talk to the designers face to face, and the fact that the Rand-Dollar exchange rate does not affect our costs as much as that of imported units, gives many of our regular customers peace of mind when tendering on large projects.”

CPS Technologies

CPS Technologies was founded as a sheet metal fabrication company in 2005, and has manufactured premium quality server enclosures and accessories for the likes of Mustek, Rectron and Eurobyte Technology. It has a modern manufacturing plant situated in Midrand which houses up-to-date machinery including CNC punching presses, laser, bending and welding machines, plus a fully automated cleaning and powder coating plant.

The company’s Ryan Arild explains that its focus is entirely on the design and manufacture of high-end 19-inch equipment enclosures. “We cater for special projects and we guarantee continuity and availability of stock items, in addition to providing quick delivery of all our products,” he says. “We pride ourselves on manufacturing cabinets of the highest quality, constantly improving and innovating our existing range of products to be able to satisfy the installers’ requirements and they are comparable with imports from the EU and USA. Our cabinets are favoured by blue chip organisations not only for their quality and features but also for their very competitive pricing. Companies are recognising the importance of good quality server cabinets that comply to all laid down international standards.”

The spectrum of server cabinets and accessories offered by CPS includes the Apollo range of wall and swing box enclosures and free standing cabinets, the Atlas range of free standing cabinets for heavy loads, the Polar range of air conditioned cabinets, and the Aries range of IP55 enclosures in various form factors and sizes.

For more information contact:
• ModRac, +27 (0)11 990 6120, brentl@modrac.co.za, www.datanet.co.za
• CPS Technologies, +27 (0)11 312 9310, sales@cps-africa.com, www.cps-africa.com.
modrac
a proudly local manufacturer of steel enclosure and racking products

From audio/video and multimedia equipment, complex monitoring systems, rack-mount and tower servers, to extensive cabling operations solutions.

Contact us

t: +27 11 990 6120
e: brentl@modrac.co.za
a: 704 16th Road, Randjespark, Midrand, South Africa
w: www.datanet.co.za
Why hardware acceleration will save you

Milestone Systems is the first VMS vendor to introduce hardware accelerated video decoding using Intel's built-in Graphics Processing Unit.

Servers are traditionally designed to handle huge data streams and a little number crunching. Alternatively, they are number crunching wonders with little capacity for databases. But the handling of video in VMS is all about huge data streams and a lot of specialised number crunching.

Milestone solves this by using the processor on the graphics card in Intel CPUs to do all the video calculations. A graphics card is specialised to handle the display, but it can also be used for other tasks. By doing this, we can use less hardware in VMS installations. This lowers the hardware cost, simplifies the installation and produces less heat and power.

Slash hardware costs by 50% or more

As the number of cameras added to surveillance systems continues to rise, the resulting increase in video streams is putting the VMS systems under increasing ‘processing pressure’, which can only be as fast as its computing power (CPU) allows. When the processing tipping point is reached, one solution is to add more hardware to increase computing power. But is this the only option?

Milestone Systems is the first VMS vendor to introduce hardware accelerated video decoding using Intel's built-in Graphics Processing Unit (GPU) component in the CPU and the Intel Media SDK. This unleashes more processing power, using less hardware.

Christian Ringler, director Middle East, Africa & DACH at Milestone, says, “By adopting this technology, the IT department can cut hardware costs by 50% or more, simplify the installation, as well as produce less heat and consume less power, adding to its green credentials.”

Greater processing power

The ability to process video has traditionally been dependent on the CPU of the surveillance system. In this scenario, to increase a system’s ability to process video, it has been necessary to add bigger servers, which not only cost more, but also add to the complexity of the system. This leads to higher administration costs and power consumption.

By harnessing the video processing capabilities in the GPU, the processor-intensive task of decoding (rendering) video is offloaded to the dedicated graphics system, leaving the processor free to perform other tasks. Computers with compatible Intel processors, firmware, drivers and a Microsoft operating system can run the latest version of XProtect Smart Client and benefit from more than 80 percent reduction in processor load.

Ringler comments: "Intel has very cleverly taken the graphics adaptor that you would associate with ‘gaming technology’ and shrunk it down to a size which means it can be incorporated into the processor. This means that the computing power, or graphics processing power, is dramatically increased while the physical space it takes up is significantly decreased. We are taking the designing principles of cell phones and applying them to our surveillance systems.

“It's important to understand the computing power we are talking about here: Intel and Milestone’s solution is purposely separate from the data center server, as this is not designed to handle the huge data streams and specialised number-crunching involved in video processing.”

The key challenges

Hardware acceleration resolves two fundamental surveillance issues. The first is the sheer volume of video that is being captured by an increasing number of cameras on systems in all sorts of environments and industry sectors. This ranges from capturing human behavior in retail stores, to sophisticated security systems monitoring in real time, to monitoring endangered species in zoos.

There is no doubt that the value of the video analysis is creating a greater demand for larger surveillance systems. Hardware acceleration overcomes the bottleneck this creates at the CPU.

The second challenge is software decoding of video. Each compressed video stream that the operator views on their monitor is being decoded by the CPU. As if this wasn’t putting enough strain on the processing power of the system, the demand for clearer, higher definition images that result in admissible evidence when needed, means the adoption of large scale HD and UHD systems is growing and adding to the incredible loads put on processing power.

Ringler explains: “To avoid poor video quality, end-users believe that they must purchase extra processing power at huge expense, both to buy the asset and maintain the subsequent running costs this involves (e.g. high power consumption). However, by using Intel Quick Sync Video, Milestone is able to dramatically reduce processor utilisation and display more video streams while eliminating those jerky video streams and grainy images that are all too common when the CPU cannot cope.”

Hardware acceleration revolution

Hardware acceleration is set to transform the surveillance industry, as by taking this approach we ultimately use less resources while increasing video capabilities.

“Our partners are winning tenders thanks to this technology, as we are typically able to reduce the number of recording servers by a factor of three or more. Taking the hardware acceleration approach offers the same, if not better performance, than adding more hardware to a system,” Ringler concludes.

For more information contact Milestone Systems, +27 (0)82 377 0415, arms@milestonesys.com, www.milestonesys.com
Extinguish fire without destroying assets

Firetrace is self-activating and reliably suppresses fires in seconds.

Micro-environments such as electrical control panels, data storage cabinets, speciality vehicles and bank depositories are notoriously difficult to protect against fire. Challenges such as space for fitting fire protection equipment and a lack of power sources on moving assets result in a very limited choice of equipment that will still perform up to standard in case of a fire.

Sperosens provides specialised safety solutions to counter these challenges and enables customers to focus on their core businesses.

Firetrace systems can be installed in virtually any enclosed space where high-value assets are located or where an increased risk of fire could be mitigated by an automatic fire suppression system.

Firetrace is self-activating and reliably suppresses fires in seconds, providing low maintenance, cost-effective fire detection and suppression all in one. Due to the speed of suppression in case of a fire the damage and downtime to equipment is minimal to none. The fire protection system can be re-armed in a matter of minutes.

The effectiveness of a Firetrace system comes from the proprietary, polymer tubing that will rupture when exposed to a flame. This specialised detection tubing combines leak resistance, flexibility, durability and precise temperature sensitivity, allowing it to react quickly when the heat from a fire is present. The detection tubing connects to a Firetrace cylinder that contains the best fire suppression agent for a particular hazard.

Configuration options vary to offer customers a solutions best designed for their specific need and level of risk.

Firetrace systems operate without the need for any power source – either external or battery – and requires no releasing panel to operate. The system is available in a standalone (no power source or control panels) and conventional network option, or a combination of both.

Depending on the type of enclosure or fire hazard, Firetrace systems can be arranged as either direct or indirect release. One of the extinguishing agents that can be used with Firetrace is Novec 1230 fluid as a great alternative to water sprinkler systems, foam and dry chemicals. The advantages of using a clean gas include:

- **Low toxicity to ensure the safety of personnel**
- **Extinguishes fires in less than half the time of CO₂ and inert gases**
- **No damage to sensitive equipment**

**Firetrace direct release systems**

Firetrace’s direct low pressure (DLP) release systems use the Firetrace tube as both the detection device and suppressant delivery. As the fire begins, the portion of the tube nearest the point where the heat is detected ruptures, forming an effective spray nozzle. The pressure will then drop as the Firetrace tube releases the entire contents of the cylinder through the distribution nozzle to effectively suppress the fire. More than one Firetrace tube can be used enabling the system to cover more area.

In a significant development for the electrical industry, Firetrace has recently been granted the prestigious LPCB (Loss Prevention Certification Board) approval for both its 3M Novec 1230 and FM-200 DLP systems. The approval is the first of its type for a tubing system and is important to the electrical sector as it covers 1 kg, 2 kg and 5 kg systems for electrical panels up to 2 m³ in volume.

**Firetrace indirect release systems**

If you have a larger area that requires a high volume of extinguishing agent in order to effectively suppress a fire, you might look for a Firetrace indirect low pressure (ILP) release system. This uses the Firetrace tube as a fire detection and system activation device, not as the discharge tube.

Firetrace’s indirect low pressure (ILP) release system. This uses the Firetrace tube as a fire detection and system activation device, not as the discharge tube.

Once the tubing senses the fire, it ruptures; resulting in a drop of pressure that causes the indirect valve to activate. This diverts flow from the detection tube to the larger outlet ports.

Then the fire suppression system kicks in. The extinguishing agent is discharged from the cylinder through the diffuser nozzles, flooding the area in a proprietary mix of fire extinguishing chemicals, effectively suppressing the fire quickly and thoroughly.

Multiple diffuser nozzles can be added to meet the specific application requirements. The indirect release system can be used with Novec 1230, FM-200, dry chemical powders, CO₂ and foam.

Applications of the Firetrace DLP and ILP systems include in-cabinet protection for typically CNC machines, electrical cabinets and controls, plant equipment, fume cabinets and on-road vehicles and mass transit, as well as industrial environments such as ports, mines and quarries, oil and gas refineries and airports.

**Firetrace total flooding systems**

Firetrace E4 engineered clean agent systems are the newest evolution in total flooding fire suppression solutions. They feature a selection of cylinder sizes, including the biggest available in the industry, so even the largest of facilities can now be effectively protected.

Featuring 3M Novec 1230 fire suppression fluid, UL and FM listed Firetrace E4 systems are shattering traditional design limitations by using 500 psi/35 bar pressure in low-cost, low pressure equipment. They offer significant improvements compared with more traditional clean agent total flooding systems for large spaces, providing superior performance, greater flexibility, improved value, speedier installation and a measurable competitive edge for system installers.

Applications of Firetrace E4 include facilities housing computers, telephone equipment, radio and TV communications, and cellular telecommunications. It is also suitable for the protection of document storage, hospitals, control rooms, libraries, test facilities, museums, flammable material storage and wind turbines.

For more information contact Marihette Hattingh, Sperosens, 086 177 3767, marihette.hattingh@spero.co.za, www.spero.co.za.
Who maintains your fire detection system?

By Charles Thiong’o, FDIA.

Installing a fire alarm is just the first step to fire safety.

A fire alarm system that is not regularly serviced and maintained will eventually cease to function. This could result in loss of life or huge fire damage costs for your company. Who is responsible?

The building owner/end user

The building owner or end user is responsible and liable for maintaining his fire detection and alarm system.

SANS 10400:2010 T1 General Requirement:

(1) Any building shall be so designed, constructed and equipped that in case of fire… (e) adequate means of access, and equipment for detecting, fighting, controlling and extinguishing such fire, is provided.

T2 Offences states:

(1) Any owner of any building who fails to… (b) maintain any other provision made to satisfy the requirements of sub-regulation (T)1(1) (e), shall be guilty of an offence. The business, or building owner, has the responsibility to designate persons with knowledge of how the fire alarm operates. The designated persons should at least know when there is a problem with the system, how to test alarms, how to reset the system and who to call for service when there is a fault on the system or if it is due for service.

SANS 10139:2012 Part 12 is about maintenance, servicing and routine testing of fire alarm systems.

Daily inspections of the fire system must be done to ensure the panel is not displaying any alarms.

Weekly tests conducted by the user of the system ensures he tests one manual call point to check that the panel performs its functions correctly and ensure all relevant warning alarms operate.

This routine testing of the system provides an opportunity for occupants of the building to become, and remain, familiar with the fire alarm signal that the system produces. The weekly test should be carried out at approximately the same time each week. Instructions to occupants should then be that they should report any instance of poor audibility of the fire alarm signal.

Servicing visits

Service visits should not exceed six months. If a risk assessment shows a need for more frequent inspection and service visits due to environmental conditions or operational use of the building, then all interested parties should agree on more frequent inspection and servicing routine.

If this recommendation is not implemented, it should be considered that the system is no longer compliant with the SANS 10139:2012.

Log book

The responsible person should ensure that the system log book is kept up to date and is available for inspection by any authorised person (e.g. representatives of enforcing authorities and property insurers). All alarms, tests and services shall be recorded in the log book.

If there is no proof of regular maintenance of the fire alarm system or the system log is not maintained, insurance companies may refuse to settle a claim after a fire incident.

The contractor

The onus is on the business or building owner to appoint a competent contractor who is duly registered and certified to carry out the maintenance and servicing of the fire alarm system in accordance with SANS 10139:2012.

Maintenance by a competent person ensures that the system will continue to function as originally intended.

The service technician shall conduct a visual inspection to check whether structural or occupancy changes have affected the compliance of the system with the recommendations of SANS 10139:2012 for the siting of manual call points, automatic fire detectors and fire alarm devices.

The log book should be examined to ensure that all faults and incidences have been recorded and appropriate action has been taken. SANS 10139:2012 sets out procedures that are to be followed by the service technician during his service visit.

All devices on the system shall be tested at least once a year to ensure their continued functionality. The standard stipulates how various devices should be tested and serviced and this should be carried out with reference to the manufacture recommendations.

The fire alarm system is also likely to require non-routine attention, including special maintenance. Non-routine maintenance includes:

- A special inspection of an existing fire alarm system when a new servicing organisation takes over servicing the system.
- Repair of faults or damage.
- Modification to take account of extensions, alterations, changes in occupancy or false alarms.

Continued on page 70
DO YOU KNOW THE OPERATIONAL STATUS OF YOUR CRITICAL FIRE SYSTEMS?

Use the internet to VERIFI your Fire Risk Exposure.

The Sperosens VERIFI system provides an encompassing, accurate, always-available status of various critical systems such as fire protection equipment. VERIFI Monitors and reports the real time status and fault conditions to users. In accordance with SANS requirements the user can obtain electronic records of inspections and events. Real time computer displays present a detailed overview of the entire facility including event logging, alarming and reports. The VERIFI system provides the user with peace of mind that the investment in fire protection or other critical systems is worthwhile. Early warning is given to report faulty equipment or overdue inspections to prevent loss of property and prevent costly downtime. VERIFI measures parameters and communicates the data using the Internet of Things (IoT) communication technology.

BENEFITS
- Easily obtainable fire audit information, where legal responsibility applies
- Early fault detection to plan preventative maintenance
- Ensure the safety of people, inventory and infrastructure
- Early warning prevents damage
- Possible reduction of insurance costs
- 24/7, 365 Dashboard Information of threats, events and failures

Do not hesitate to contact us for additional product information and re-seller opportunities.

www.spero.co.za • info@spero.co.za • +27 12 665 0317
SAQA training as a requirement for PSiRA registration

Terry Henderson casts light on the training and certification debate in the fire industry.

Recently the media has been flooded by articles relating to PSiRA and SETA certified training. SANS regulations dictate how installations of fire detection systems should be carried out. Preservation of life is governed by the OSH Act. These two criteria dictate that fire detection installers must be competent and therefore it is important to have certified courses available which are aligned with the requirements of the National Qualifications Framework (NQF).

In terms of section 23(3) of the PSiRA Act, all natural persons applying for registration must meet minimum training requirements in order to register for these courses. PSiRA comments that the new updated standards will better the industry.

Terry Henderson from White Rose Training and Development Institute says the company is the only accredited company that has SASSETA approved training, recognised by the QCTO, offering specific unit standards within which recognition for fire detection is given. The company is therefore the only one able to give a NQF-based training which can lead to a certificate of achievement being awarded by SASSETA. The SASSETA learner achievement certificate or statement of results, were gazette by PSiRA as a requirement before an individual can be registered as a security (fire) service provider.

All other companies that carry out fire detection training can only give a certificate of attendance or of competence on their products or training. This does not meet the requirements of PSiRA.

Henderson adds that no-one will be excluded from joining the fire detection industry as long as they get certified. Additionally, because the training is SAQA/SASSETA/QCTO accredited, companies can claim back a large majority of the training fees as determined by the skills levies act.

According to the Department of Labour, anybody installing or maintaining fire detection systems have to be registered. All these ‘technicians’ also have to prove competency. In addition to fire detection installation and maintenance training, White Rose can offer SASSETA certified RPL testing (Recognition of Prior Learning) for the existing fire detection industry participants which will prove competency against the relevant Fire Unit Standards. Once completed, the SASSETA learner achievement certificate or statement of results will be accepted by PSiRA as a requirement before an individual can be registered as a security (fire) service provider. All of this training will go a long way to ensuring the uplifting of the industry and compliance to National Regulations.

According to Henderson, White Rose opens up a whole new world for the learner by not only providing them with NQF-based training but also providing them with updates on regulations and new products which ensure they are kept abreast of skills and latest technologies.

He says that White Rose has the sole objective of ensuring competent and professional fire detection technicians are put into the industry with the correct national qualifications. This will uplift the industry and be in the interest of preservation of life and property thereby adding value to all South African citizens and visitors to our country.

Leaders who attend and complete the White Rose courses are able to carry a National Certification which stands them in good stead for their working life anywhere in South Africa.

For more information contact Terry Henderson, White Rose Training and Development Institute, +27 (0)83 402 4002, terry@whiteroseinstitute.co.za.

---

Continued from page 68

- Action to address an unacceptable rate of false alarms.
- Inspection and test of the system following a fire.

Who should I trust?

Ensure your maintenance contractor can prove a track record for servicing and ask to check his service sheets to ensure he has a full working knowledge of fire detection and alarm systems, as in all industries there are good and bad service companies. Based upon the above guidelines end users are strongly advised to enter into a service agreement upon the completion of any new installation works on their premises with the contract installer involved.

The FDIA has in the past concentrated only on how installations are carried out but are now in the process of investigating the feasibility of registering service/maintenance companies involved in the industry in an attempt to ensure quality service to all end users.

We encourage all end users to only use FDIA registered contractors as they have the capability and mandate to ensure that not only is your fire detection system installed correctly, but it is serviced and maintained as per the required standards and regulations.

For more information contact the FDIA at fdia@fdia.co.za or www.fdia.co.za.
As security systems have transitioned into network devices over the last few decades, system vulnerabilities have transitioned as well. This shift in network utilisation brings with it far more vulnerabilities than compared to older analogue systems, and due to the very nature of networking the outer boundary of the surveillance system can be vulnerable to attack.

The ‘arteries’ of an IP system, the physical network connections, need to reach the edge components, namely the cameras, which are often mounted in exposed locations. Thus, these arteries and edge components need intensified protection.

Trusted Platform Module
In this document we focus on the ‘key vault’ inside a device which stores, amongst other private data, the most secret data for authentication and authenticity of a device: the Trusted Platform Module.

For years, Bosch IP cameras, encoders and selected storage systems have come with an onboard security chip – actually a system-on-a-chip which we call our Trusted Platform Module (TPM) – that provides functionality similar to crypto smart cards, like credit or debit cards. Such a Trusted Platform Module secures authenticity and acts like a safe for critical data, protecting certificates, keys, licences, etc. against unauthorised access even when the device is physically opened to gain access.

We consider it a necessity and expect state-of-the art technology to take care of security when referring to our financial transactions in everyday life. Why then should video surveillance equipment and assets be secured less?

The following description applies to all devices equipped with a Trusted Platform Module. For simplicity and according to the highest vulnerability level, we will refer to the device as being a camera.

What a Trusted Platform Module is
A Trusted Platform Module is a self-contained system that acts as a cryptographic co-processor to the camera system, connected to it via a serial interface. The Trusted Platform Module runs its own firmware which is continuously maintained to provide optimal protection against possible threats known from the market. Its firmware is only loaded in a secure production environment, not remotely like firmware for cameras. New Trusted Platform Module versions thus are only deployed with new produced cameras.

Communication between the camera firmware and the Trusted Platform Module chip happens via ‘Secure Apps’ inside the Trusted Platform Module. These provide the interfaces and commands for certain functionalities. There is no possibility for the firmware or operating system to modify anything inside the Trusted Platform Module directly.

The Certificate Store as a functional block in the camera stores less critical data, like certificate bodies and public keys, in a dedicated memory, but outside the Trusted Platform Module. All critical cryptographic activities are handled by specific functions,
Talk everywhere

Combining conventional 2-way radios with modern smartphone technology.

Halo Technology’s Smart PTT radios allow you to talk everywhere. These communication devices combine conventional 2-way radios with modern smartphone technology.

Smart radios look and feel like conventional 2-way radios but that’s where the similarities stop. Smart PTT radios take advantage of existing cellular mobile networks for coverage across Africa to offer 2-way communication between your office in Pretoria and your suppliers in Namibia or anywhere else in Africa (SIM card required).

Smart radios therefore have virtually limitless range. As long as there is a mobile signal or Wi-Fi coverage, you can communicate. Conventional 2-way radios are mostly limited to line-of-sight range without the use of expensive repeaters, even then the range will be limited to a geographical area.

Smart radios do not suffer from interference. We’ve all experienced bad reception when using crackly walkie-talkies. This can even be the same with professional 2-way radios. Because smart radios are digital and they harness the power of cellular or Wi-Fi networks, they provide high-quality audio with no crackles.

Our radios are offered with dispatch software that allows the dispatcher to trace and track all radios. They also contain a facility that promotes group and individual communication within the network of the organisation, and all communications are safe and secure. Battery time is extended and the radios can easily be charged as one would do with a normal two-way radio.

The benefits are similar to those of cell-phones: they do not lose signal, they are cheaper to use and facilitate better communication across the network. They also enable messages to be sent by the operator to one or many radios on the network to make communication more efficient.

If the radio is stolen or lost, the operator can put it out of action until it is retrieved, at which point it can be reactivated again. For private calls, a setting can be selected that links two specific radios, and after the call is completed the radio automatically reverts back to the original group. All calls are also recorded and available for playback when needed. Some of these radios even offer GPS tracking that displays time, distance travelled, and speed.

Because they are effective at wide-area communication in many different environments, they are the perfect replacement for cellphones and they provide additional functionality. Other features of Smart PTT radios include noise reduction, weather channels and safety features. In addition, they are water- and heat-resistant.

For more information contact Deon Swanepoel, Halo Technology, +27 (0)12 997 7107, deon@halotechnology.co.za, www.halotechnology.co.za

called Secure Apps, which make use of the Trusted Platform Module’s internal resources.

What a Trusted Platform Module does

As mentioned before, a Trusted Platform Module acts like a co-processor to the camera system. The key vault resembles some volatile and non-volatile memory to store keys and other relevant data during runtime or over power cycles, according to operational requirements.

Private keys, if loaded with a certificate, are stored inside the Trusted Platform Module and then are no longer retrievable. They can then only be used through cryptographic operations provided by the Trusted Platform Module, respectively its Secure Apps. It is recommended to password-protect the private key to keep it a secret until safe storage within the Trusted Platform Module, e.g. using PKCS #12 file format.

Private keys that result from certificate signing requests (CSR) are created internally, kept secret and never revealed to outside the Trusted Platform Module, making certificate enrolment via certificate signing requests the highest level of security.

Its encryption engine provides key handling support for symmetrical encryption like Triple DES or AES with up to 256 bits key length by calculating and producing the encryption key. Once the key is delivered, the Triple DES or AES encryption or decryption itself for video or other payload is then done by the encryption engine (hardware accelerator) in the main CPU.

The PKI engine supports in certificate validation and authentication, handling key lengths of up to 2048 bits, while the Secure CPU helps with any other cryptographic functionality like creating signed hashes for e.g. video authentication.

What a Trusted Platform Module’s benefits are

A camera as the most exposed component of an IP video surveillance system faces the most threats. Besides the many cyber threats, it can also be stolen and hacked. Such might happen as the ultimate attempt by an attacker to retrieve certificate and key to later-on simulate a camera by his/her own equipment, trying to hack deeper into the surveillance system, maybe even beyond.

A device, be it a camera or any other system, without a Trusted Platform Module must store private keys in its file system, where it might reside in an especially encrypted file, but the key to this must also be stored somewhere in the file system.

If hacking into a camera’s certificate store does not reveal what is being looked for, a side-channel attack may do. Such an attack uses analytic hardware equipment to listen to the data bus of the system while this is performing its tasks. When triggering the authentication process, at some point, the key will appear unencrypted.

With sufficient criminal energy, time and appropriate equipment, the attacker will eventually succeed. A compromised private key can cripple the whole Public Key Infrastructure.

Having a Trusted Platform Module integrated, no such attempt will become successful as any activities involving a private key occur only inside the Trusted Platform Module. The Trusted Platform Module’s chip technology is even protected against light and laser attacks if someone would afford to grind off the chip’s housing.

For more information contact Bosch Security Systems – South Africa & Sub-Saharan Africa, +27 (0)11 651 9600, security.systems@za.bosch.com, http://afrika.boschsecurity.com

CYBER SECURITY

Private keys that result from certificate signing requests (CSR) are created internally, kept secret and never revealed to outside the Trusted Platform Module, making certificate enrolment via certificate signing requests the highest level of security.

Its encryption engine provides key handling support for symmetrical encryption like Triple DES or AES with up to 256 bits key length by calculating and producing the encryption key. Once the key is delivered, the Triple DES or AES encryption or decryption itself for video or other payload is then done by the encryption engine (hardware accelerator) in the main CPU.

The PKI engine supports in certificate validation and authentication, handling key lengths of up to 2048 bits, while the Secure CPU helps with any other cryptographic functionality like creating signed hashes for e.g. video authentication.

What a Trusted Platform Module’s benefits are

A camera as the most exposed component of an IP video surveillance system faces the most threats. Besides the many cyber threats, it can also be stolen and hacked. Such might happen as the ultimate attempt by an attacker to retrieve certificate and key to later-on simulate a camera by his/her own equipment, trying to hack deeper into the surveillance system, maybe even beyond.

A device, be it a camera or any other system, without a Trusted Platform Module must store private keys in its file system, where it might reside in an especially encrypted file, but the key to this must also be stored somewhere in the file system.

If hacking into a camera’s certificate store does not reveal what is being looked for, a side-channel attack may do. Such an attack uses analytic hardware equipment to listen to the data bus of the system while this is performing its tasks. When triggering the authentication process, at some point, the key will appear unencrypted.

With sufficient criminal energy, time and appropriate equipment, the attacker will eventually succeed. A compromised private key can cripple the whole Public Key Infrastructure.

Having a Trusted Platform Module integrated, no such attempt will become successful as any activities involving a private key occur only inside the Trusted Platform Module. The Trusted Platform Module’s chip technology is even protected against light and laser attacks if someone would afford to grind off the chip’s housing.

For more information contact Bosch Security Systems – South Africa & Sub-Saharan Africa, +27 (0)11 651 9600, security.systems@za.bosch.com, http://afrika.boschsecurity.com

CYBER SECURITY

Private keys that result from certificate signing requests (CSR) are created internally, kept secret and never revealed to outside the Trusted Platform Module, making certificate enrolment via certificate signing requests the highest level of security.

Its encryption engine provides key handling support for symmetrical encryption like Triple DES or AES with up to 256 bits key length by calculating and producing the encryption key. Once the key is delivered, the Triple DES or AES encryption or decryption itself for video or other payload is then done by the encryption engine (hardware accelerator) in the main CPU.

The PKI engine supports in certificate validation and authentication, handling key lengths of up to 2048 bits, while the Secure CPU helps with any other cryptographic functionality like creating signed hashes for e.g. video authentication.

What a Trusted Platform Module’s benefits are

A camera as the most exposed component of an IP video surveillance system faces the most threats. Besides the many cyber threats, it can also be stolen and hacked. Such might happen as the ultimate attempt by an attacker to retrieve certificate and key to later-on simulate a camera by his/her own equipment, trying to hack deeper into the surveillance system, maybe even beyond.

A device, be it a camera or any other system, without a Trusted Platform Module must store private keys in its file system, where it might reside in an especially encrypted file, but the key to this must also be stored somewhere in the file system.

If hacking into a camera’s certificate store does not reveal what is being looked for, a side-channel attack may do. Such an attack uses analytic hardware equipment to listen to the data bus of the system while this is performing its tasks. When triggering the authentication process, at some point, the key will appear unencrypted.

With sufficient criminal energy, time and appropriate equipment, the attacker will eventually succeed. A compromised private key can cripple the whole Public Key Infrastructure.

Having a Trusted Platform Module integrated, no such attempt will become successful as any activities involving a private key occur only inside the Trusted Platform Module. The Trusted Platform Module’s chip technology is even protected against light and laser attacks if someone would afford to grind off the chip’s housing.

For more information contact Bosch Security Systems – South Africa & Sub-Saharan Africa, +27 (0)11 651 9600, security.systems@za.bosch.com, http://afrika.boschsecurity.com

CYBER SECURITY

Private keys that result from certificate signing requests (CSR) are created internally, kept secret and never revealed to outside the Trusted Platform Module, making certificate enrolment via certificate signing requests the highest level of security.

Its encryption engine provides key handling support for symmetrical encryption like Triple DES or AES with up to 256 bits key length by calculating and producing the encryption key. Once the key is delivered, the Triple DES or AES encryption or decryption itself for video or other payload is then done by the encryption engine (hardware accelerator) in the main CPU.

The PKI engine supports in certificate validation and authentication, handling key lengths of up to 2048 bits, while the Secure CPU helps with any other cryptographic functionality like creating signed hashes for e.g. video authentication.

What a Trusted Platform Module’s benefits are

A camera as the most exposed component of an IP video surveillance system faces the most threats. Besides the many cyber threats, it can also be stolen and hacked. Such might happen as the ultimate attempt by an attacker to retrieve certificate and key to later-on simulate a camera by his/her own equipment, trying to hack deeper into the surveillance system, maybe even beyond.

A device, be it a camera or any other system, without a Trusted Platform Module must store private keys in its file system, where it might reside in an especially encrypted file, but the key to this must also be stored somewhere in the file system.

If hacking into a camera’s certificate store does not reveal what is being looked for, a side-channel attack may do. Such an attack uses analytic hardware equipment to listen to the data bus of the system while this is performing its tasks. When triggering the authentication process, at some point, the key will appear unencrypted.

With sufficient criminal energy, time and appropriate equipment, the attacker will eventually succeed. A compromised private key can cripple the whole Public Key Infrastructure.

Having a Trusted Platform Module integrated, no such attempt will become successful as any activities involving a private key occur only inside the Trusted Platform Module. The Trusted Platform Module’s chip technology is even protected against light and laser attacks if someone would afford to grind off the chip’s housing.

For more information contact Bosch Security Systems – South Africa & Sub-Saharan Africa, +27 (0)11 651 9600, security.systems@za.bosch.com, http://afrika.boschsecurity.com
All-in-One iSTAR Ultra Video

The small iSTAR Ultra Video appliance combines access control with embedded video recording and remote management.

Tyco Security Products, part of Johnson Controls, has launched iSTAR Ultra Video that offers distributed, small site security with enterprise performance.

This small appliance combines the access control features of iSTAR Ultra with embedded video recording and management that is remotely managed by an integrated C-CURE 9000/victor application to meet the security needs of small remote sites. Each iSTAR Ultra Video is factory-imaged with the latest firmware and camera licences.

Each iSTAR Ultra Video appliance supports up to 8 readers and 8 IP cameras. Used with IP-ACM Ethernet door modules, iSTAR Ultra Video is aimed at large corporations whose footprints include smaller remote networking facilities, fibre huts and other small but critical facilities that need constant monitoring and control. The distributed security architecture can scale to thousands of sites, making it an option for enterprise customers with multiple remote locations.

Each appliance manages up to 500 000 cardholders in a local database and can buffer up to 500 000 transactions locally when offline. It includes the full functionality of a VideoEdge NVR and its built-in intelligence allows users to receive multiple video streams for live, record, alarm, and meta-data collection.

The system provides full configuration and viewing functionality at the remote location while providing bandwidth-managed movement of the data distributed locally from where the video is securely stored. Users can easily back up video to any network location to increase storage capacity and system reliability.

Smart Streaming technology tailors video streams based on viewing conditions, which significantly reduces network bandwidth, CPU resources, and memory usage. VideoEdge dynamically scales and transcodes multiple live streams to all clients, further reducing bandwidth.

For the most critical areas, iSTAR Ultra Video features built-in intrusion zone functionality allowing you to monitor and respond to intrusion alarms quickly, without relying on a third-party intrusion panel. Any door or input wired to the IP-ACM Ethernet door modules can be configured as part of an intrusion zone, either as a 24/7 monitored input such as a glass break detector, or as a controlled input such as a motion sensor or door. Zones can be armed and disarmed using a combination of card and/or PIN, and/or remotely from C-CURE 9000 or victor clients. In response to zone alarms, specific cameras may be configured to present a live view and/or recorded video to the operator.

The onboard analytics transform video into business intelligence to better analyse operations, maximise revenue potential, and increase situational awareness.

For more information contact Tyco Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com.
Automated key control improves manual systems

By Fernando Pires, VP sales and marketing, Morse Watchmans.

Keeping operational costs down and improving efficiency.

Everyone makes mistakes and, in many cases, they can be good learning opportunities. However, some mistakes have more far-reaching and even potentially dangerous ramifications than others. The importance of securing people, places and assets, mistakes can lead to losses and potentially cost lives.

In the event of a lost key or mismanaged keys for instance, locks may have to be re-keyed, inventories will have to be taken or audits performed, lost or damaged items replaced and there will have to be a follow up investigation to determine who may have been responsible or who last had the keys. Not only are these disruptive exercises but they can also be quite expensive depending on the number of doors that must be re-fitted and the types of locks required. A policy review may even be initiated to help ensure that keys are better managed and controlled and that measures are put in place so that the situation does not re-occur.

Without question, physical keys still play a vital role in the security process but key management is one of the most overlooked areas within security. Company policies regarding key control and usage are fine in theory but are too often ignored in practice. Keys are passed around and/or duplicated, manual logging is not reliable and so on. When it comes to tracking and controlling access to keys, lessening or even eliminating human errors is a primary motivation for an organisation to make the decision to move from a manual system to an automated key management system.

Here are five areas where the implementation of an automated key management system can make a difference.

Key control
Not knowing if an employee attempts to get possession of a key they are not authorised to use, or when a key is returned by an employee other than the one who took it out, can quickly become a liability. Key control and management systems are designed to secure keys in a tamper-proof cabinet and access to the cabinets and to individual keys is controlled at all times, with every key accounted for.

Admins can access, program and monitor the system over a network from anywhere. This convenience allows facility managers to see reports, change users, establish permission levels for each user code, monitor data or configure the systems from virtually any location, all providing added control.

Policies and procedures
Policies and procedures are established for a reason but they may not always be followed. One of the ways in which organisations can help ensure that employees follow company policy regarding key usage is to make sure that it is easy or convenient to do so. Key management systems with automated tracking relieve the responsibility of an employee having to manually sign out a key or log returns into the book.

Other time-saving features may include the option to return a key to any key cabinet in the system rather than having to return the key to the cabinet from which it was removed. Users can see which keys they have out, if any of their keys are overdue and when their keys will become overdue. Biometric identification, large, easy to read touch screens, voice cues and status bar guides help to ensure a fast and easy procedure when accessing or returning keys to the cabinet.

Improved security
Hardware and software technologies are not the only measures available to improve security; information often is just as valuable. Key management systems allow keys to be managed according to requirements (i.e. time/day available, personnel, etc.) and management can quickly query what keys have not been returned and when a key will become overdue. And if a key is not returned to the key cabinet as scheduled an alert is sent via email or SMS text to appropriate personnel so that immediate action may be taken. Mobile apps let authorised users to see a wide range of live information and interact remotely with the system.

In the event of an incident, management can query the system for specific details such as listing all transactions between certain times and when doing a follow up investigation, request a report for the hour preceding the incident. Or, immediately following an incident such as the discovery of a damaged or missing piece of equipment, a report can be generated showing who last accessed the particular key.

Key usage information
In addition to key tracking, the recorded data from a key management system provides a wide range of business intelligence that can be analysed for identifying policy and procedure infractions and/or improvements. Trends that could take weeks or months to detect manually can be seen almost instantly when relevant queries are programmed into the reporting software. This highly specific intelligence allows root causes of problems to be identified rather than symptoms, and enables management to enact countermeasures that will help prevent new incidents before they occur.

Integrated systems
Today’s advanced key management systems feature open protocols and partner certifications that let them integrate into broader security systems, including identity management, access control, and visitor control. Managed separately, they create unnecessary extra work for staff and leave open the potential for security vulnerabilities. When integrated though, processes can be streamlined and redundancies eliminated across common points. Employees can be entered into the access control system, for example, with their credentials’ profile information, access group, etc. instantly transferred to other systems. The system can also pass data about transactions and alarms back to the access control system.

To help ensure system integrity and protection from breaches, data can be encrypted with AES-256 technology. Other new features are continually being added to help protect the system from security breaches via the network.

Finally, all of these improvements made possible by implementing a key control and asset management system in place of a manual system can help to keep operational costs down: there are no lost keys to be replaced, easy use encourages adherence to organisational policies and procedures, control of keys makes facilities less vulnerable to break-ins and theft, analysed data can point out weaknesses and improved operational efficiencies in an integrated system save time and money.

For more information, contact Morse Watchmans, +1 203 264 4949, morse@morsewatchman.com, www.morsewatchmans.com
Tyco Security Products, part of Johnson Controls, announced the release of AC2000 v8, which offers new features that increase the performance, simplicity and scope of the AC2000 access control system suite from CEM Systems. These include AC2000 Data Partitioning and enhancements to AC2000 Security Hub command and control application. CEM Systems has also released enhancements to the emerald Intelligent Access Terminal range with the emerald TS100f and TS200f fingerprint terminals.

“The latest release of AC2000, which include data partitioning, offers enhancements for multi-site and multi-tenanted customers,” said Richard Fletcher, product manager, CEM Systems. “AC2000 Database Partitioning is a powerful feature for scenarios where multiple companies utilise a single security management system. It empowers each company by giving them control over their own private access areas while still allowing them access to common areas within the building or campus.”

Enhancements within AC2000 Security Hub, centralised command and control application include, map zones, reports and a seamless video integration interface which enables live video footage for specific configured alarms to be displayed.

This release also offers enhanced functionality of emerald, CEM Systems’ intelligent access terminal. Designed for use with the CEM Systems AC2000 security management system, emerald terminals not only control access to restricted areas but also open up a world of infinite possibilities by bringing AC2000 intelligence directly to the edge. emerald now supports a configurable ‘Boarding and Deplaning Route Management’ (BDRM) mode which provides a sophisticated touch screen-based passenger routing system for airports. emerald BDRM can be pre-programmed to activate a variety of functions from a single selection on the device including enabling relevant signage, interlocking a series of doors to form a route, enabling air bridges, fixed ground power units and much more.

Building on the existing range of video, perimeter, fire and intrusion integrations, AC2000 now offers new integrations including interfaces to DSC PowerSeries Neo intrusion panel and Milestone XProtect Professional Video Management System.

For more information contact Tyco Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com.
Blok Developments is an urban property developer operating in Cape Town’s Atlantic Seaboard and CBD. Its thoughtfully designed and detail orientated apartments are built to make a lasting contribution to the neighbourhoods they develop in.

Security is a priority for Blok and its residents. It required a system that would allow it to control who could access the developments, and had the functionality to easily assign, update and bar access tokens, from a simple, reliable user interface. Blok also needed residents to have the option to visually identify visitors via video intercom.

Solid Systems, a managed IT service provider based in Cape Town was approached by Blok to install a security solution that met the requirements on their four new developments.

Solid Systems recommended Net2, Paxton’s flagship access control system, to control the access on site. It also included a Net2 Entry monitor, Paxton’s intuitive, colour touchscreen internal monitor, in every property for visual authentication and a direct line of communication to the security desk.

Net2 is a user friendly and flexible networked access control system, designed to make the management of any site straightforward. Net2 Entry, combined with Paxton’s plug-and-play door entry solution, Net2 Entry, has provided Blok Developments and its residents with a simple security system that is managed remotely by Solid Systems.

Solid Systems will manage and maintain the system on behalf of Blok, programming access control tokens and monitoring the system remotely. Michael Claxton, MD at Solid Systems says: “Our network management solution pro-actively detects issues within the Blok ICT environment, and attempts to resolve the issue automatically. If unsuccessful, a certified IT professional is notified and assigned to the issue for a speedy resolution.”

In place of traditional locks and keys, the residents now use tokens to access the site. If a token is lost, it can easily be barred from the Net2 system. New tokens can be added, and access permissions can be updated with ease. The use of individual tokens also provides Blok’s security personnel with a full audit log of who has entered and exited the developments, further enforcing the level of security for their residents.

The penthouse residents present their token upon entering the lift, which will then take them directly into their property.

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

**Site statistics**

**Type of site:** Residential  
**Location:** Cape Town, South Africa  
**Number of doors:** 12 doors. Four developments.  
**Solution required:**  
- Video intercom for visual visitor authentication  
- Full audit log of those entering and exiting the site  
- Simple token management system  

**Result:**  
- Increased security solution across all developments  
- Flexible management enabling property owners to control site access  
- Remote management via network connection

**Paxton products used:**  
- Net2 plus controller  
- Net2 Entry monitor  
- Net2 Entry vandal resistant panel  
- Proximity metal keypad, MIFARE - KP75  
- Proximity metal reader  
- Proximity marine reader

**Integration:** Lift integration for penthouse access
Pursuant to a financial audit, a restaurant with outlets across the Western Cape, was advised that it was losing profits due to excessive overtime pay. After a brief investigation, it appeared that staff were manipulating hours worked, by recording inflated clocking in and out times in the manual entry book.

In an effort to combat the fraud, the business owner turned to fellow restaurateurs in search of a solution. It transpired that many restaurateurs had faced similar problems, prior to installing and utilising the mobile FPX10 biometric clocking system, supplied by Active Track.

After a discussion regarding the payment structure, and installation, the owner chose to run an FPX10 pilot project in his restaurant situated in the Cape Town city bowl.

As part of the package, Active Track provided training to the managers on how to install the FPX10 device, how to upload the fingerprints of staff; how the data is captured on the device and automatically integrated into the restaurant’s payroll system, how to view the captured data in real time via Active View – Active Track’s online portal. Further training covered how to grant various employees access to certain areas and how to amend this access remotely, and how to optimally use the various panic activation functions.

At the end of the first month of installation, the restaurant’s payroll for its city bowl restaurant had decreased dramatically. This was due to the staff’s inability to manipulate the data captured by the FPX10 and the payroll system only processing payment for real-hours captured, and therefore worked.

For more information contact Active Track, +27 (0)11 551 1687, info@activetrack.co.za, www.activetrack.co.za
Panoramic camera with its combined 4 fixed 2 PanoVu DS-2DP0818Z-D Series 180-degree consultation exercise, Hikvision proposed the city, Seo-gu Office turned to Hikvision. After a separate PTZ imaging over the entire imaging solution for the project that would enable the capture of high-quality panoramic, a bad odour monitoring and tracking system at atmospheric information project, to establish dyeing stakeholders. From that meeting, it economic, environmental and industrial was conducted within South Korea's largest industrial area, in Busan Metropolitan City, the country's second largest city next to Seoul. The Hikvision PanoVu camera demonstration was not only deemed a success, but also regarded as 'a perfect fit' for the monitoring system's requirement. Installed in November 2016, the new atmospheric information system is capable of measuring in real-time, complex odours composed of hydrogen sulphide, ammonia and volatile organic compounds in and around the surrounding industrial area. The main control point, located at the Lifelong Learning Hall in Seo-gu, monitors system equipment consisting of 2 sets of 4 PanoVu DS-2DP0818Z-D cameras, 11 malodour measuring instruments (serving as a neural network in the monitoring complex), and two weather measurement instruments, which collect weather data such as wind speed, humidity and temperature. Monitoring the entire city area, the Hikvision cameras are integrated into the system's atmospheric pollution sensors and capable of visually pinpointing the source of any atmospheric bad odour release.

The result
"The Seo-gu Office Atmosphere Monitoring Centre is extremely pleased with the high-resolution picture quality they can now display on their large format video wall, and in combination with the PanoVu cameras’ Panoramic Mode + PTZ tracking function, are able to display wide-area coverage and close-up visual tracking via integration with the system's atmosphere sensors," says Joey Kim, SI Team, Hikvision Korea. "The atmospheric information system's pollution monitoring sensors and integrated PanoVu cameras can define the precise location of each sensor's triggered event and with the PanoVu PTZ camera, automatically track and target the precise location of the event actuation."

For more information contact Hikvision South Africa, Evan Liu, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com

---

Hikvision launches Blazer Pro

Blazer is an all-in-one, high-end server solution.

Hikvision has launched Blazer Pro, an all-in-one high-end server solution designed to meet the needs of medium to large camera count, mission-critical surveillance network projects.

Combining Hikvision's Video Management System software and data storage into one physical server solution, Blazer Pro is capable of handling up to 128 or 256-channels. Catering for any large to mid-size surveillance application, the all-in-one server not only performs basic functions like recording, live view, playback, and alarm management, but also optional advanced functionality such as ANPR, business intelligence, and people counting.

Using a dual-boards design, the solution ensures a fail-proof backup system with the server board and storage board working independently so that in the advent of VMS server failure, normal recording, preview and playback functionality remain unaffected. The system uses Linux, providing more dependable operation.

In a project with several local NVRs performing local recording and using Blazer Pro as the central platform managing those NVRs, if a local problem occurs with an NVR or it is removed (stolen), all is not lost, as the unit will retain the key IP channel's data from that local site. This fail-safe solution is facilitated by key IP channel streams being simultaneously transmitted in real-time, from the local NVR, to the central server.

Blazer Pro boasts many advanced video footage and system safety technologies, including flexible user management, which allows users to prioritise access for management and personnel – to ensure that staff members can be allocated an appropriate system access authority.

Providing effective system awareness and identification, Blazer Pro’s alarm management interface is a simple and friendly interface that displays real-time performance and alarm notification, making it easier to identify an alarm, locate relevant video and associated information in a single window.

For more information contact Hikvision South Africa, Evan Liu, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com
Dahua takes HDCVI into the 4K era

Dahua's 4K analogue offering delivers 3840(H) x 2160(V) ultra-high resolution images, equivalent to 4X 1080 HD cameras.

HD analogue technology is gaining traction. By 2018, over 90% of analogue cameras will be HD analogue (according to a 2016 IHS report). Dahua introduced HDCVI technology in 2012 and continues to enhance the technology by delivering improvements in terms of resolution, light sensitivity, intelligence and usability.

The emergence of multi-mode DVRs, which records video from HDCVI, TVI, AHD, CVBS and IP cameras, makes it easy to upgrade a site incrementally. Future development of HD analogue will fill the needs of IoT and big data applications, which will drive value to security systems in the next few years. AI (artificial intelligence) deep learning will be a key technology component to enable this.

Dahua's 4K offering delivers 3840(H) x 2160(V) ultra-high resolution images, equivalent to 4X 1080 HD cameras, to achieve wide angle coverage and clear video evidence at the same time.

HDCVI 4.0

Dahua has now introduced its HDCVI 4.0 technology framework, with three key components: 4K video capture, IoT for multi-dimensional sensing and AI to transform HDCVI video into searchable Boolean data. New products will be introduced throughout 2017 to enhance the user experience of HDCVI customers. The HDCVI community can expect more opportunities to use HDCVI technology to expand the security application space.

Dahua 4K-HDCVI adopts 4K Ultra HD image acquisition and back end DVR storage. The technology architecture overcame the common bottleneck of transmission bandwidth to achieve high resolution video previously only available on IP. This is a major breakthrough to extend the potential of HDCVI.

Dahua IoT-HDCVI technology combines IoT sensing technology and enables cameras to surpass basic function of providing video information. Using IoT sensors, coaxial cables are capable of transmitting not only video signal, but also information such as alarm, temperature and humidity. The HDCVI technology architecture supports complex data transmission between camera and DVR, and makes it possible for multi-dimensional sensing cameras and DVRs to form an IoT solution. The near real-time transmission of HDCVI also improves the responsiveness of IoT applications.

Dahua AI-HDCVI technology integrates HDCVI video and audio with AI (artificial intelligence) deep learning. AI performs near-human level accuracy in image classification and voice recognition to transform HDCVI video and audio into searchable Boolean data. The output of this analysis could solve resource allocation problems, for example, in the retail industry with customers and/or in the management of city transportation with vehicle traffic analysis.

The scalable and expandable architecture of HDCVI enables future-proof products and solutions to be developed. It protects customers' investment by allowing seamless upgrading to new technologies as they emerge.

The 4K era

While the industry is trying to break through the bandwidth constraints of coaxial cable transmission, Dahua's signal modulation mechanism and noise reduction technique has also increased the distances video signals can be transmitted. The use cases are:

- RG6 coaxial cables for 700 m video and audio lossless transmission
- RG59 coaxial cables for 500 m video and audio lossless transmission
- UTP Cat 6 network cable for 300 m video and audio lossless transmission
- The Dahua offering includes 4K box cameras, 4K IR bullet and dome cameras, 4K fish-eye panoramic cameras, 4K multi-sensor 180-degree panoramic cameras, and a series of 4K supported XVR (multi-mode DVRs).

The new 4K XVR recorder is compatible with all existing HDCVI/HDTVI/AHD cameras, and also supports CVBS and IP cameras. This makes upgrading to 4K much more convenient and cost effective. The installation, configuration, operation and maintenance of 4K HDCVI are the same as before, preserving the plug & play convenience of analogue video system. Once your existing DVR is replaced by a new 4K XVR, you can simply replace the existing camera with a 4K camera or add a 4K camera as you go.

One new product is the DH-HAC-PFW3601, which is the first HD analogue multi-lens infrared camera with a 4K 180 degree panoramic view. This product makes use of Dahua’s advanced image stitch algorithm to perform 180-degree panoramic seamless stitching. It can be controlled by the OSD menu and easily operated. By using three SONY STARVIS sensors and F1.4 large aperture lens, this infrared camera delivers high quality images even under low light. In addition, the camera has IP67 and IK10 protection, making it a good choice for important entrances and exits area, city transportation junctions, and parks.

For more information, contact Dahua Technology South Africa, fritz.wang@global.dahuatech.com, www.dahuasecurity.com
Kedakom entered the South African market this year with a series of road shows highlighting the company’s products. These included a range of surveillance and body-worn cameras, as well as a range of solutions for command and control centres and its own NVRs with advanced analytical capabilities.

Kedacom provides carrier-class video surveillance core devices and supplementary software systems, helping users establish command and control centres based on IP video applications with more than 100 000 channels. Highlights include powerful networking systems, high reliability, abundant professional functions and a track record of high profile clients in the public and private sector.

Recognitive NVRs

In a traditional video surveillance system, cameras capture video streams or snapshots which are transmitted to a backend storage device. Access to the data means logging into the storage systems and searching for the relevant information.

The next level of technological advancement was all about ‘smart’ video surveillance systems that allow features such as tripwire drawing and warning area masking that tracked breaches of virtual lines. The above has limitations though, for example, managing multiple targets, change of target sizes, light intensity and the time it takes to interrogate the data etc.

This is where Recognitive technology closes the gap. The Kedacom range of Recognitive solutions use sophisticated image recognition algorithms and high-performance chipsets to identify and classify objects, including human faces, human bodies and multiple moving targets. The technology has a huge range of functions including the ability to trace target movement, determine speed, direction and characteristics like size, colour and type.

The backbone of the technology is the Kedacom Recognitive NVR. It combines Smart Video Synopsis and Recognitive analytic algorithm features. Smart Video Synopsis compresses video data into brief video clips and automatically extracts photos of moving objects with reference to their colour, size, direction, speed and other characteristics that can be individually or collectively set up.

Users can browse video clips of moving targets and use snapshots and defined characteristics to narrow down their search and quickly find relevant data for quick decisions. The intelligent NVRs revolutionise traditional video retrieval using numerous target characteristic metrics, style filtering and recording timeframes. This is just one of the analytic features that help streamline surveillance and organisational efficiency.

The Recognitive NVRs support any standard ONVIF camera and thus are interoperable with other major camera brands as well. The NVR’s modular architecture allows for up to 64 channels.

“The intelligent NVRs revolutionise traditional video retrieval using numerous target characteristic metrics, style filtering and recording timeframes.”

Success stories

In Europe Kedacom has a vibrant client base that has implemented the intelligent tracking systems to simultaneously track and capture critical live video streams and snapshots that make it possible to pre-empt malicious or dangerous activities. Another success story is the Turkey border. The technologies on this project include industrial grade NVRs with RAID storage and laser PTZ cameras for full HD surveillance. Other projects include, the Safe City Project in Suzhou China where up to 60 000 cameras are managed under one system.

For more information, contact Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co.
Video enhances security and performance

Observing large areas with multi-focal technology.

Success for both the airport and mining industry hinges on cost-efficiency. Driven by cost pressures, airport operators have been on the topic for years: the need to lower ground handling costs, notably through the optimisation of aircraft turnaround times. High-performance video systems, such as Panomera and intelligent management software from Dallmeier are increasingly being used to achieve just that at airports worldwide – in addition to ground and airspace security.

The mining industry is dealing with comparable challenges, albeit in a different environment. Mines are still prone to theft by employees or intruders along the perimeter. That so-called 'green area' requires a general surveillance coverage whereby faces must be clearly identifiable. Panomera guarantees just that by providing a pixel density which is high enough for identification.

Since mines are dangerous surroundings due to the operation of heavy equipment and large-scale earth movement, work safety is another top priority for mining companies. While Dallmeier technology is ideally suited to enhance both safety and security across mining sites, the industry has been moving towards also using video systems for analysing and optimising business operations.

Mining is a complex multi-stage process, whose profitable execution depends heavily on operators' ability to avoid operational disturbances. Coupled with intelligent video analysis tools, Panomera offers unique capabilities for ensuring smooth workflows.

The multifocal sensor system Panomera was specially developed for the all-encompassing video surveillance of expansive areas, such as strip mines. A huge area can be surveyed from a single location and resolution can be scaled as needed.

From the beginning of the mining process, when a new area is developed, through every stage of the raw materials extraction offers potential applications for video technology.

During construction, Panomera – together with other primary and secondary measures – helps secure and control access to the site. The system's unique resolution and overview also assist management in ensuring that the often wide-ranging activities comply with permits by providing a comprehensive visual status report at all times. Once production begins, Dallmeier's multifocal sensor technology proves its suitability for collecting and implementing business intelligence data.

Analogous to aircraft parked at terminals for deboarding and refuelling, dump trucks arriving at crushers are monitored in minute detail during unloading. Meanwhile, dedicated software analyses the video images, immediately notifying security staff of incidents such as a collision between the load bed and the crusher chute. The software correlates the real-time images with a stored schedule and informs staff of any delays so that the overall flow of truck traffic can be adjusted accordingly.

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

New cameras from FLIR

Multiple new thermal and visible security cameras and a major update to VMS.

FLIR Systems has announced its United VMS 8.0, the latest version of the company’s flagship video management solution (VMS), and three high-performance security cameras, including the FLIR PT-Series HD (high-definition) thermal and visible camera system, the FLIR Quasar 4K fixed box camera, and the FLIR Ariel 3MP (3-megapixel) corner camera. All three cameras integrate with FLIR United VMS 8.0 and expand the company’s end-to-end line of security solutions.

FLIR United VMS 8.0 is an enterprise-level video management solution for managing video security operations. United VMS 8.0 manages large and multi-location video operations, and includes FLIR Latitude software, as well as FLIR Horizon and FLIR Meridian network video recorders.

The United VMS 8.0 delivers a more secure system through stronger online security credential requirements. A simplified system installation process and streamlined camera discovery make integration with FLIR products easy. Also, FLIR United VMS 8.0's open platform design allows for integration with third-party technologies and is customisable and scalable for any size deployment, from small retailers to large enterprises to critical infrastructure.

The FLIR PT-Series HD is a dual-sensor camera system that provides superior, long-range perimeter intrusion detection regardless of lighting and environmental conditions. The high-speed, pan-tilt camera provides quick and accurate threat verification. The FLIR PT-Series HD offers either a cooled or uncooled 640x480 resolution thermal camera with a 1080p HD visible camera. Multiple high-performance thermal lenses are available, including optical zoom lenses up to 14X. The HD visible camera also features a 30X optical zoom lens with autofocus and low light capabilities.

The FLIR Quasar 4K fixed box multiple-resolution camera can be programmed to switch from 4K daytime mode to 1080p lowlight-nighttime mode to provide optimum, continuous performance. Its compact design allows for the use of specialised camera housings, ranging from explosion to extreme weatherproof, and can accommodate a range of lenses from super-wide to telephoto.

The FLIR Ariel 3MP corner camera features a 3-megapixel visible camera that provides ceiling-to-floor and wall-to-wall viewing. The corner camera also includes a built-in microphone for audio monitoring and discrete night vision illumination for monitoring low light to totally dark locations. FLIR Ariel 3 MP also features an impact-resistant, vandal-proof, flush-mount housing, making it ideal for locations such as medical facilities and prisons where the safety of at-risk occupants is essential.

For more information contact FLIR Systems www.flir.com or refer to the www.hsbd.co.za for SA distributors.
New SerVision mobile DVR/NVR

In-vehicle HD digital video recording and live transmission for remote monitoring.

Graphic Image Technologies is pleased to announce that the new SerVision IVG 400-N DVR/NVR is now available locally, offering both in-vehicle HD digital video recording and live transmission for remote monitoring.

“The dilemma most surveillance operators are faced with involves having to choose between high-resolution recording quality and the ability to view real-time transmission, when it comes to being able to keep eyes on vehicles while mobile,” says Laurence Smith, executive at Graphic Image Technologies, “It’s now possible to have dual streaming of both HD-quality recording from IP cameras running at either 720p or 1080p, and lower-quality transmission of footage at the same time.”

With support for IP cameras, high definition recording and the SerVision-optimised H.264-based codec for live streaming at low bit rates, the IVG400-N is ideal for installation on any type of moving vehicle. “The IVG400-N enables fleet operators to remotely monitor their moving assets, drivers and vehicles in real-time, from either one central remote location or multiple sites or smartphones. While the compression is not as high as is possible with analogue set-ups, this product is still a market leader in compression ratios. Fleet managers can now expect outstanding quality HD recording with IP cameras, as well as live video transmission over IP, wireless and cellular networks,” says Smith.

Seamless integration with fleet management

Ideal for installation on buses, trains, police cars, delivery trucks, armoured vans, emergency response vehicles and more, the SerVision IVG400-N system promises effortless integration into other fleet management products, such as Telematics. “The ability to integrate with other products is a huge opportunity, given Intel’s recent acquisition of Mobileye – a company that develops vision-based advanced driver assistance systems to provide warnings for collision prevention and mitigation. The IVG400-N has already been integrated with Mobileye and will work in conjunction with the in-vehicle CCTV setup,” Smith adds.

Additional advanced features that will appeal to fleet managers include geo-fencing, route deviation and speed alerts. The system has a built-in Wi-Fi interface that can be used to create a mobile hotspot to offer Internet connectivity to passengers or to wirelessly backup video to the SVControlCenter’s storage server.

“Thanks to innovative video compression techniques, SerVision has found a way to transmit high-quality video over all network types, which means that narrow bandwidth constraints experienced by most security sites are now a thing of the past. With the IVG 400-N, we no longer have to choose between image resolution and real-time monitoring,” Smith concludes.

For more information contact Graphic Image Technologies, +27 (0)11 483 0333, laurence@git.co.za, www.git.co.za

Interactive home automation

ZeroWire is a self-contained, wireless security and interactive home automation system. With ZeroWire, users will gain the support through the Z-Wave protocol, which ensures secure communications of the different systems and software applications with other devices, such as thermostats and lighting controls, offering one single system for both home automation and security.

An added benefit is the integrated support for IP cameras, for live video and replaying of recorded footage based on alarms or action triggered events, reducing the risk of false alarms and increasing the information available in case of an event. The UltraSync interactive services ensure the advanced cloud features can be accessed anytime and anywhere. With an iOS and Android app, and an online portal, the installed system can be efficiently monitored and managed remotely. It allows the user to view the system status, offer system controls such as bypass zones, arming and disarming, reading the event history and much more. Whether using the UltraSync platform for remote servicing and monitoring or for remote programming, a secure connection is guaranteed between the device and the ZeroWire system.

For more information contact Elvey, +27 (0)11 401 6700, info@elvey.co.za, www.elvey.co.za.
ViRDI has extended its range to include two new, cost effective models. ViRDI optics come with a 10-year warranty. Internationally and independently recognised by FVC-onGoing as having one of the most reliable algorithms, which ensures system integrity and an exceptionally high enrolment rate. Built with the same stringent quality controls and practices that have made ViRDI products synonymous with terms like “reliable” and phrases like “it just works”.

**Key Features**
- Networkable
- PUSH communication
- Bluetooth®
- OSDP
- IP65
- Patented live and fake finger detection
- Embedded digital camera
- Built-in card reader
- Up to 10 000 fingerprints
- 100 000 offline logs
- KC, CE, FCC and RoHS certified
- FBI PIV certified sensor

For more information contact Regal Distributors, +27 (0)11 553 3300, info@regalsecurity.co.za, www.regalsecurity.co.za

---

Kedacom has launched the IPCS21-H210-W PTZ IR camera. This PTZ can be mounted on the top of vehicles with five powerful magnets at its base. The high capacity built-in battery delivers 8-hour long operation time while its embedded Wi-Fi module requires no cables. A conventional vehicle can be transformed for surveillance with high quality video acquisition and transmission capability by integrating it with the IPCS21-H120-W PTZ camera. With four embedded IR light units and a super low illumination sensor, up to 60 m distances can be monitored after dark.

The image quality of the PTZ is enhanced as follows:
- 2.0 megapixel 1/2.8-inch Progressive Scan CMOS sensor
- 20x optical zoom
- 1080p@60fps
- H.265 video codec, saves up to 50% in bandwidth and storage
- Ultra-low illumination, 0.003 lux with colour picture
- IR automatically adjusts
- 120 dB Ultra WDR
- 3D noise reduction / HLC / BLC

The camera is designed to work in all conditions and withstands operation temperatures of -40°C to 70°C. It is rated IP66, and sports TVS 6000V lightning protection, surge protection and voltage transient protection.

For more information, contact Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co

---

TeleEye released an addition to the MQ2200 Series Starlight IR cameras to its camera product line. Adopting Sony Starlight CMOS Sensor, the new MQ2200 Series from TeleEye enables a much higher sensitivity to various lighting environments compared to the MQ200 Series. With the advancement of MQ2200’s camera lens and the image signal processor, the performance of this powerful Starlight sensor can even be maximised.

The upgraded camera lens enables higher image clarity of the images and improved the black-edged problem of the video. In addition to the use of an advanced image signal processor, a higher processing power is also performed. The video quality is therefore greatly improved with higher image clarity, image recovery and digital noise reduction. With the above enhanced combination, the new MQ2200 Series is capable of delivering detailed and coloured images even in extreme low light and backlight conditions, enabling every object and colour to be recognisable in the above lighting conditions, whereas the MQ200 Series can only show the black shadow and indistinct contours of the objects.

For more information contact TeleEye (South Africa), +27 (0)11 557 9200, www.teleeye.com
Fit-for-purpose solar cables

Specialist cable manufacturer, Helukabel, has invested considerable resources in the development of a comprehensive range of cables and accessories exclusively for solar energy applications. Having supplied cabling solutions for some of South Africa’s main solar projects, the company has also cemented its status as a local solutions provider.

The list of local solar plants is an impressive one and includes the latest plants in Kalkbult, Droogfontein and De Aar, among others. The company is also gearing to supply several other new projects throughout southern Africa.

According to Helukabel South Africa sales manager, Hardus van Dyk, Helukabel’s foresight saw the company already developed appropriate solutions for photovoltaic applications in the early ‘90s with the development of its first photovoltaic (PV) cables which are still marketed under the Solarflex trademark. These carry global approvals from TÜV and VDE. In combination with its state-of-the-art PV-connectors, the company can offer users in the photovoltaic industry with pre-assembled PV-cables and wires for quick plug-and-play on-site installation.

Solar solutions

These pre-assembled solutions include chains, PV wiring fuse/diode, pre-assembled potential equalisation cables, adaptors and other fit-for-purpose photovoltaic cables. Components in the solar range include panel boxes, male and female connectors and branches with a host of accessories that include cable glands, protection tubes, shrink-on sleeves and cable ties.

“An example of the Solarflex solutions is Helukabel’s Solarflex-X PV1-F solution specifically for the solar industry which is able to withstand the harsh environments of solar plants exceeds TÜV, CE, RoHS and VDE quality certifications to ensure the longevity of installation where it is used – which generally has an anticipated life of 25 years’ service,” van Dyk says.

All Solarflex cables are ozone, UV and weather resistant and are highly resistant to chemical interference, as well as fire and abrasion. In addition, the cables can be made in rodent resistant versions or to customers’ exact requirements for specific sites. The bare copper, tinned and finely stranded cable is double insulated with cross linked Polyolefin while the outer sheath comprises the same material in a black, red or blue. The nominal voltage of this particular cable is rated at 600/1000 V AC and 1800 V DC. Other requirements unique to solar energy applications have also been researched and Solarflex-X PV1-F cables have been developed to enhance the operational efficiency of these sites.

For more information contact Helukabel SA, +27 (11) 462 8752, doug.gunnewegh@helukabel.co.za, www.helukabel.co.za.

Pan and tilt unit

FLIR announced the newest member of its motion control systems pan and tilt units (PTU), the new FLIR PTU-5. Standing only 15.24 cm tall when fully integrated, the new FLIR PTU-5 can hold up to 2.267 kg on its top bracket, packing performance into a compact package. Fully sealed and weather-proof rated to IP67, the PTU-5 is a low-cost unit that is easily integrated in- and outdoors.

Features
• Class-leading speed and accuracy
• Turn on and track moving targets in seconds
• Extra small, rugged, portable design
• Lightweight, Mil-spec system for harsh environments
• Easy integration
• Flexibility for a wide range of applications and sensors

For more information contact FLIR Systems www.flir.com or refer to the www.hsbd.co.za for SA distributors.
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<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>52*,77</td>
</tr>
<tr>
<td>Akhanani Distributors</td>
<td>+27 (0)11 613 7299</td>
<td><a href="mailto:sales@akhanani.com">sales@akhanani.com</a></td>
<td><a href="http://www.akhanani.com">www.akhanani.com</a></td>
<td>8</td>
</tr>
<tr>
<td>Axis Communications</td>
<td>+27 (0)11 548 6780</td>
<td><a href="mailto:sasha.bonheim@axis.com">sasha.bonheim@axis.com</a></td>
<td><a href="http://www.axis.com">www.axis.com</a></td>
<td>10,26</td>
</tr>
<tr>
<td>Bosch Security Systems - South Africa &amp; sub-Saharan Africa</td>
<td>+27 (0)11 651 9600</td>
<td><a href="mailto:security.systems@za.bosch.com">security.systems@za.bosch.com</a></td>
<td><a href="http://africa.boschsecurity.com">http://africa.boschsecurity.com</a></td>
<td>57,71,72</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>62</td>
</tr>
<tr>
<td>CAMROSA</td>
<td>*27 (0)72 580 7318</td>
<td><a href="mailto:fdia@fdia.co.za">fdia@fdia.co.za</a></td>
<td><a href="http://www.fdia.co.za">www.fdia.co.za</a></td>
<td>68,70</td>
</tr>
<tr>
<td>Catexhis Africa</td>
<td>+27 (0)31 240 0800</td>
<td><a href="mailto:sales@catexhisvideo.co.za">sales@catexhisvideo.co.za</a></td>
<td><a href="http://www.catexhisvideo.com">www.catexhisvideo.com</a></td>
<td>56</td>
</tr>
<tr>
<td>Crest Advisory Africa</td>
<td>+27 (0)11 534 8454</td>
<td><a href="mailto:training@crestadvisoryafrica.com">training@crestadvisoryafrica.com</a></td>
<td><a href="http://www.crestadvisoryafrica.com/">www.crestadvisoryafrica.com/</a></td>
<td>9</td>
</tr>
<tr>
<td>Dahua Technology South Africa</td>
<td>+27 (0)11 462 8752</td>
<td><a href="mailto:doug.gunniewegh@dahual.co.za">doug.gunniewegh@dahual.co.za</a></td>
<td><a href="http://www.dahua.co.za">www.dahua.co.za</a></td>
<td>3*,79</td>
</tr>
<tr>
<td>Dallmeier Technology Southern Africa</td>
<td>+27 (0)11 510 0505</td>
<td><a href="mailto:dallmeiersa@dallmeier.com">dallmeiersa@dallmeier.com</a></td>
<td><a href="http://www.dallmeier.com">www.dallmeier.com</a></td>
<td>81</td>
</tr>
<tr>
<td>Electronic Security Distributors' Association</td>
<td>+27 (0)11 401 6700</td>
<td><a href="mailto:info@eley.co.za">info@eley.co.za</a></td>
<td><a href="http://www.eley.co.za">www.eley.co.za</a></td>
<td>63*,82</td>
</tr>
<tr>
<td>Elvey</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>63*,82</td>
</tr>
<tr>
<td>FLIR Systems</td>
<td>+44 780 151 4810</td>
<td><a href="mailto:david.montague@flir.com">david.montague@flir.com</a></td>
<td><a href="http://www.flir.com">www.flir.com</a></td>
<td>25*,81,84</td>
</tr>
<tr>
<td>Forbes SA</td>
<td>+27 (0)11 469 3598</td>
<td><a href="mailto:sales@forbb.co">sales@forbb.co</a></td>
<td><a href="http://www.forb.co">www.forb.co</a></td>
<td>80,83,83</td>
</tr>
<tr>
<td>Genetec</td>
<td>+27 (0)82 854 1278</td>
<td><a href="mailto:bercy@genetec.com">bercy@genetec.com</a></td>
<td><a href="http://www.genetec.com">www.genetec.com</a></td>
<td>43*</td>
</tr>
<tr>
<td>Gianni Industries</td>
<td>+886 222 677 986</td>
<td><a href="mailto:inquiry1@gianni.com.tw">inquiry1@gianni.com.tw</a></td>
<td><a href="http://www.gianhi.com.tw">www.gianhi.com.tw</a></td>
<td>75*</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>82</td>
</tr>
<tr>
<td>Halo Technology</td>
<td>+27 (0)12 997 7107</td>
<td><a href="mailto:deon@halotechnologo.co.za">deon@halotechnologo.co.za</a></td>
<td><a href="http://www.halotechnologo.co.za">www.halotechnologo.co.za</a></td>
<td>5*,72</td>
</tr>
<tr>
<td>Helukabel South Africa</td>
<td>+27 (0)11 462 8752</td>
<td><a href="mailto:doug.gunniewegh@helukabel.co.za">doug.gunniewegh@helukabel.co.za</a></td>
<td><a href="http://www.helukabel.co.za">www.helukabel.co.za</a></td>
<td>84</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*,1*,78</td>
</tr>
<tr>
<td>Hi-Tech Security Solutions</td>
<td>+27 (0)11 543 5800</td>
<td><a href="mailto:dominique@technews.co.za">dominique@technews.co.za</a></td>
<td><a href="http://www.technews.co.za">www.technews.co.za</a></td>
<td>6*,45*</td>
</tr>
<tr>
<td>HiTech Security Distributors</td>
<td>+27 (0)21 946 3344</td>
<td><a href="mailto:sales@hitsecurity.net">sales@hitsecurity.net</a></td>
<td><a href="http://www.hiteksecurity.net">www.hiteksecurity.net</a></td>
<td>53*</td>
</tr>
<tr>
<td>iFacts</td>
<td>+27 (0)11 453 1587</td>
<td><a href="mailto:jenny@ifacts.co.za">jenny@ifacts.co.za</a></td>
<td><a href="http://www.ifacts.co.za">www.ifacts.co.za</a></td>
<td>20,22,23</td>
</tr>
<tr>
<td>Johnson Controls</td>
<td>+27 (0)11 921 7141</td>
<td><a href="mailto:neil.cameron@jci.com">neil.cameron@jci.com</a></td>
<td><a href="http://www.johnsoncontrols.com">www.johnsoncontrols.com</a></td>
<td>28</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>16,17</td>
</tr>
<tr>
<td>Managed Integrity Evaluation (MIE)</td>
<td>+27 (0)12 644 4000</td>
<td><a href="mailto:info@m.ie.co.za">info@m.ie.co.za</a></td>
<td><a href="http://www.m.ie.co.za">www.m.ie.co.za</a></td>
<td>30</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>14,57*</td>
</tr>
<tr>
<td>Milestone Systems</td>
<td>+27 (0)82 337 4172</td>
<td><a href="mailto:arms@milestone.com">arms@milestone.com</a></td>
<td><a href="http://www.milestones.com">www.milestones.com</a></td>
<td>14,66</td>
</tr>
<tr>
<td>MiRO distribution</td>
<td>086 123 MIRO (6476)</td>
<td><a href="mailto:sales@miro.co.za">sales@miro.co.za</a></td>
<td><a href="http://www.miro.co.za">www.miro.co.za</a></td>
<td>39*</td>
</tr>
<tr>
<td>ModRac</td>
<td>+27 (0)11 990 6120</td>
<td><a href="mailto:brent@modr.ac.za">brent@modr.ac.za</a></td>
<td><a href="http://www.datanet.co.za">www.datanet.co.za</a></td>
<td>64,65*</td>
</tr>
<tr>
<td>Modular Communications</td>
<td>+27 (0)83 456 9542</td>
<td><a href="mailto:cliff@modular.co.za">cliff@modular.co.za</a></td>
<td><a href="http://www.modular.co.za">www.modular.co.za</a></td>
<td>54</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.com">www.morpho.com</a></td>
<td>7*,8</td>
</tr>
<tr>
<td>Morse Watchmans</td>
<td>+1 203 264 4949</td>
<td><a href="mailto:morse@morsewatchman.com">morse@morsewatchman.com</a></td>
<td><a href="http://www.morsewatchman.com">www.morsewatchman.com</a></td>
<td>74</td>
</tr>
<tr>
<td>Naxian</td>
<td>+27 (0)87 820 0620</td>
<td><a href="mailto:bernard@naxian.co.za">bernard@naxian.co.za</a></td>
<td><a href="http://www.naxian.co.za">www.naxian.co.za</a></td>
<td>10,12,13,31*</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>35*,47*</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>11*,76</td>
</tr>
<tr>
<td>Powelltronics</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>OFC*,18,19*</td>
</tr>
<tr>
<td>Progroug Manufacturing</td>
<td>+27 (0)11 493 1545</td>
<td><a href="mailto:sales@progroug.co.za">sales@progroug.co.za</a></td>
<td><a href="http://www.progroug.co.za">www.progroug.co.za</a></td>
<td>17*</td>
</tr>
<tr>
<td>Reditrion</td>
<td>+27 (0)87 802 CCTV(2288)</td>
<td><a href="mailto:marketing@reditrion.co.za">marketing@reditrion.co.za</a></td>
<td><a href="mailto:marketing@reditrion.co.za">marketing@reditrion.co.za</a></td>
<td>27*</td>
</tr>
<tr>
<td>Regal Distributors</td>
<td>+27 (0)11 553 3300</td>
<td><a href="mailto:info@regularso.co.za">info@regularso.co.za</a></td>
<td><a href="http://www.regulser.co.za">www.regulser.co.za</a></td>
<td>73*,83</td>
</tr>
<tr>
<td>SAIIBA</td>
<td>+27 (0)11 845 4780</td>
<td><a href="mailto:saidsa@mweb.co.za">saidsa@mweb.co.za</a></td>
<td><a href="http://www.saidsa.co.za">www.saidsa.co.za</a></td>
<td>34*</td>
</tr>
<tr>
<td>SALTO Systems</td>
<td>+27 (0)11 534 849</td>
<td><a href="mailto:info.za@saltosystems.com">info.za@saltosystems.com</a></td>
<td><a href="http://www.saltosystems.com">www.saltosystems.com</a></td>
<td>37*</td>
</tr>
<tr>
<td>Seagate South Africa</td>
<td>+27 (0)76 268 3450</td>
<td><a href="mailto:martin.krujer@seagate.com">martin.krujer@seagate.com</a></td>
<td><a href="http://www.seagate.com">www.seagate.com</a></td>
<td>49*</td>
</tr>
<tr>
<td>Secu-Exports</td>
<td>+27 (0)11 794 7834</td>
<td><a href="mailto:info@secuexports.com">info@secuexports.com</a></td>
<td><a href="http://www.secueexports.com">www.secueexports.com</a></td>
<td>58*</td>
</tr>
<tr>
<td>Securion AG</td>
<td>+41 31 910 1398</td>
<td><a href="mailto:info@securion.com">info@securion.com</a></td>
<td><a href="http://www.securion.com">www.securion.com</a></td>
<td>9*,13*</td>
</tr>
<tr>
<td>Secu-Systems</td>
<td>+27 (0)11 794 7834</td>
<td><a href="mailto:charles@securesystems.co.za">charles@securesystems.co.za</a></td>
<td><a href="http://www.securion.co.za">www.securion.co.za</a></td>
<td>58,59</td>
</tr>
<tr>
<td>Specialised Exhibitions</td>
<td>+27 (0)500 033 0600</td>
<td><a href="mailto:leigh@specialised.com">leigh@specialised.com</a></td>
<td><a href="http://www.securex.co.za">www.securex.co.za</a></td>
<td>51*</td>
</tr>
<tr>
<td>Sperosens</td>
<td>086 177 3767</td>
<td><a href="mailto:marilette.hattingh@spere.co.za">marilette.hattingh@spere.co.za</a></td>
<td><a href="http://www.spero.co.za">www.spero.co.za</a></td>
<td>67,69*</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>32,35*,47*</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.co.za">www.teleeye.co.za</a></td>
<td>83</td>
</tr>
<tr>
<td>Tyco Security Products</td>
<td>+27 (0)82 566 5274</td>
<td><a href="mailto:email@tyco.com">email@tyco.com</a></td>
<td><a href="http://www.tycosecurityproducts.com">www.tycosecurityproducts.com</a></td>
<td>21*,75,73,75</td>
</tr>
<tr>
<td>Utef Fire &amp; Security</td>
<td>+27 (0)11 579 7300</td>
<td><a href="mailto:utef.ssa@uts.utc.com">utef.ssa@uts.utc.com</a></td>
<td><a href="http://www.utefiredandsecurity.eu">www.utefiredandsecurity.eu</a></td>
<td>61*</td>
</tr>
<tr>
<td>VRDI Distribution SA</td>
<td>+27 (0)11 454 6006</td>
<td><a href="mailto:deon@virde.co.za">deon@virde.co.za</a></td>
<td><a href="http://www.virdtech.co.za">www.virdtech.co.za</a></td>
<td>32</td>
</tr>
<tr>
<td>White Rose Training and Development Institute</td>
<td>+27 (0)83 402 4002</td>
<td><a href="mailto:terry@whiteoseinstitute.co.za">terry@whiteoseinstitute.co.za</a></td>
<td><a href="http://www.whiteoseinstitute.co.za">www.whiteoseinstitute.co.za</a></td>
<td>70</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>25</td>
</tr>
</tbody>
</table>
More reasons why KEDACOM is a leading surveillance technology brand

- Advanced Search Algorithms
  - ID: 00006
  - Color: Yellow
  - Direction: East
  - Type: Car
  - Speed: Fast

- Object, Facial and Body Snapshot and Tagging

- Object Tracking Functionality

- EMap with Integrated Alarm Management

Our Recognitive NVR’s feature some of the most advanced search algorithms

KEDACOM / Recognitive IP Video Solutions
Video Surveillance Business

Forbatt SA
Energy, surveillance technology and home automation

www.forbatt.co  011 469 3598  @Forbattsa  sales@forbatt.co

Products available exclusively from:

KEDACOM is a listed company that manufactures surveillance equipment.
Solo Agent: FORBATT SA