Re-empower the coax with Dahua revolutionary HDCVI 3.0
The Best Way to Get Panoramic Views and Incredible Detail in One Camera!

Hikvision PanoVu Series Panoramic Cameras

Pan out to get the whole scenario in one frame. Then zoom in to see a single face in the crowd. And get the most advanced surveillance technology at the same time.

Sensors inside the PanoVu Series Cameras stitch together multiple video streams into one panoramic shot much more efficiently than software. Bring entire stadiums, plazas, airports, and open areas of all kinds into 180- and 360-degree panoramic view. Then, from the panoramic view, swiftly zoom in on a target for incredibly close-up detail with 36X optical zoom. With PanoVu, you get the most powerful “Vu” in security surveillance.
Dr Craig Donald believes effective operators are the key to effective surveillance projects.

Securex 2016 was a hit with visitors and exhibitors reporting a successful event.

Are multi-sensor cameras the way to go for surveillance security in the entertainment industry?

Hi-Tech Security Solutions takes a look at the issue of key management and how best it can be approached.

Hosting your security solution offsite is a big decision, but one that more companies are making.
Who is responsible? You are!

Gone are the days of installing IP cameras without a care about security; and by that I mean information security or cyber security, or whatever you want to call it. A security company, Sucuri, was recently asked to help a small jewellery business suffering a distributed denial of service (DDOS) attack. The business’s website was receiving around 35 000 requests per second, which basically made the website useless for everyone.

Sucuri dealt with the attack, only to find the number of requests increasing to almost 50 000 after the site came back online. This is where the IoT (Internet of Things) comes into the picture. IoT devices have been used in attacks before, but this time the IoT devices were surveillance cameras that were connected to the Internet. To be more specific, Sucuri was able to identify over 25 000 IP addresses from cameras located around the world.

The cameras were located in 105 different countries. What is nice is that for once South Africa wasn’t in the top 10, although it was one of the 105.

The key issue here was the vulnerability the attackers took advantage of dates back to 2014. The software was developed in China and affects over 70 vendors who use it in their DVRs – which means the cameras attached to the DVRs can be compromised. You can read a technical investigation into the vulnerability at www.securitysa.com/*ksrce1, as well as a list of the affected vendors.

Fortunately, most of the vendors are small companies you probably haven’t heard of, but there are enough recognisable names to make one nervous. Of course, one doesn’t know who may have bought from these vendors and put their own branding on the product.

We also don’t know which vendors may have patched their products since the article was published, but we do know there are over 25 000 cameras out there that are still vulnerable. But these are only the ones discovered in this incident, how many more may be out there?

You can read the story at www.securitysa.com/*subot1, but the moral of the story is simply that you can not expect security when you are on the Internet for any reason. It would be nice if we could expect our vendors and service providers to do their jobs and ensure security, but at the end of the day it’s you who must take responsibility for your own kit.

This means buying trusted brands from suppliers and service providers who know what they are doing and won’t vanish into thin air after the account is paid. It also means taking responsibility for your own upgrades and security patches – even on cameras, NVRs and DVRs, as well as computers, laptops and servers. At the very least, include it in your SLA and check that it’s done.

This won’t solve all the malware and similar problems, but it will make it harder for malware deviants to ply their trade. Also, maybe it’s time for physical security vendors to upgrade their patch release schedules?

Andrew
About 1.25 million people die each year as a result of road traffic crashes. Road traffic injuries are the leading cause of death among young people, aged 15–29 years. Without action, road traffic crashes are predicted to rise to become the 7th leading cause of death by 2030.

——— From World Health Organization

Behind the Global Efforts to Forge A Safer Traffic, Dahua Provides A Rich Set of Solutions to Prevent Road Tragedies.

**A BETTER AND SAFER WORLD**
Dahua Intelligent Transportation Solution (ITS)

**ANPR**
Record the vehicle image and recognize the plate number even at the speed of 180km/h

**Speed Measurement**
Detect and record the over-speed vehicle with corresponding vehicle classification and lane No. by integrated radar and camera

**Red Light Enforcement**
Detect and record the red light runner with the tracking of ITS camera and 3D radar

**Mobile Surveillance**
Ensure the driving safety and simplify the work of vehicle dispatching and management.
EXHIBITIONS, CONFERENCES, SPECIALISED EVENTS

TAPA 2016 Conference
27 July 2016
Emperor's Palace, Gauteng

The 2016 TAPA (Transport Asset Protection Association) Conference will focus on a regional perspective on cargo crime: The challenges faced by authorities and advancements made in crime prevention and detection. The keynote will be by Dr Johan Burger from the Institute of Security Studies, with additional presentations from the Hawks and the SAPS Forensics Department.

There is no cost for TAPA members; cost for non-members is R1 200 excl. VAT.

For the full agenda and to book, contact Andre Duvenage, 083 463 2047, 011 391 6268, andre.duvenage@securelogistics.co.za.

The Association of Residential Communities conference
27 – 30 July 2016
Midstream Estates

All homeowners living within a residential community or anyone interested in community living will benefit from attending this event. Apart from showcasing residential estates in South Africa, visitors will experience what community living is all about. Visitors will be able to attend discussions and debates focused on community living.

Contact Jonathan Gilmour, 083 286 5939, info@hoasupport.co.za, www.arcexpo.co.za.

Camprosa International Conference 2016
4-7 September 2016
Zimbali Hotel, KZN

The Campus Protection Society of Southern Africa is set to host its 2016 international conference at Fairmont’s Zimbali Hotel in KZN from the 4th to 7th September 2016.

For more information on the full programme, go to www.camprosa.co.za.

Security Essen
27 to 30 September

The No. 1 for more than 40 years: Security Essen is the world’s most important trade fair for security and fire prevention. The world market for security is booming – it is presenting itself with all its facets in Essen. From fire prevention and cyber security and CCTV to the protection of outdoor areas: experts, decision-makers and buyers from this industry will be meeting in Essen.

Further information at www.security-essen.de.

Securexpo East Africa 2016
8-10 November 2016
Visa Oshwal Centre, Nairobi, Kenya

This event is dedicated to suppliers involved in the homeland, security, fire and safety industries and offers you a unique prospect to get an early foothold in the fast-developing East African market. If you want to see your business become part of the burgeoning East African economy – now’s your chance! Book a stand at Securexpo East Africa today and get a prime position on our exhibition floor.

Contact, Alexander Angus, alexander.angus@montex.co.uk, +44 (0) 20 7886 3034

Events

TAPA 2016 Conference
27 July 2016
Emperor's Palace, Gauteng

The 2016 TAPA (Transport Asset Protection Association) Conference will focus on a regional perspective on cargo crime: The challenges faced by authorities and advancements made in crime prevention and detection. The keynote will be by Dr Johan Burger from the Institute of Security Studies, with additional presentations from the Hawks and the SAPS Forensics Department.

There is no cost for TAPA members; cost for non-members is R1 200 excl. VAT.

For the full agenda and to book, contact Andre Duvenage, 083 463 2047, 011 391 6268, andre.duvenage@securelogistics.co.za.

The Association of Residential Communities conference
27 – 30 July 2016
Midstream Estates

All homeowners living within a residential community or anyone interested in community living will benefit from attending this event. Apart from showcasing residential estates in South Africa, visitors will experience what community living is all about. Visitors will be able to attend discussions and debates focused on community living.

Contact Jonathan Gilmour, 083 286 5939, info@hoasupport.co.za, www.arcexpo.co.za.

Camprosa International Conference 2016
4-7 September 2016
Zimbali Hotel, KZN

The Campus Protection Society of Southern Africa is set to host its 2016 international conference at Fairmont’s Zimbali Hotel in KZN from the 4th to 7th September 2016.

For more information on the full programme, go to www.camprosa.co.za.

Security Essen
27 to 30 September

The No. 1 for more than 40 years: Security Essen is the world’s most important trade fair for security and fire prevention. The world market for security is booming – it is presenting itself with all its facets in Essen. From fire prevention and cyber security and CCTV to the protection of outdoor areas: experts, decision-makers and buyers from this industry will be meeting in Essen.

Further information at www.security-essen.de.

Securexpo East Africa 2016
8-10 November 2016
Visa Oshwal Centre, Nairobi, Kenya

This event is dedicated to suppliers involved in the homeland, security, fire and safety industries and offers you a unique prospect to get an early foothold in the fast-developing East African market. If you want to see your business become part of the burgeoning East African economy – now’s your chance! Book a stand at Securexpo East Africa today and get a prime position on our exhibition floor.

Contact, Alexander Angus, alexander.angus@montex.co.uk, +44 (0) 20 7886 3034

Keynote Presentation: Dr Johan Burger,
Senior Researcher: Institute of Security Studies
Dr Johan Burger will cover the dual threat of crime and public violence in SA and the challenges faced by crime fighting agencies.

Nico Snyman, International Risk Management Consultant
Nico will explain the need for a structured, strategic, tactical and operational approach to cargo risk management.

Roger Truebody, Senior Manager Cyber Risk & Resilience: Deloitte
In his presentation Roger will cover the threat and impact of cyber crime on current and future business. He will also highlight the structures business should have in place to mitigate cyber attacks.

Spokesperson from Hawks
We will hear the Hawk’s perspective on regional cargo crime activity and how they are addressing organised crime in this sector.

Spokesperson from the Forensics Department SAPS
This presentation will cover the exciting advancements in DNA forensics and how they are assisting in combating crime.

Spokesperson from the Department of Home Affairs
This presentation will highlight the security changes in ID documentation.

Massimo Carelle, Risk Manager: Ingram Micro
Massimo will explain the TAPPA FSR standard in a practical way and will demonstrate how a risk profile can change pre- and post-FSR implementation.

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.
Our focus is to make darkness totally visible.

starlight. The inventors take it to the next level. Bosch cameras with new starlight technology are the gold standard in low light video performance. We’ve upgraded the original with better light sensitivity, a choice of resolutions, dynamic ranges up to 120 dB and up to 60 frames per second. Plus video analytics at the edge as standard, with no additional investment of license fees, to make high quality images more relevant.

Learn more at www.boschsecurity.com/hdsecurity
Hikvision focuses on verticals

By Andrew Seldon.

Hikvision has made a name for itself over the past couple of years as a fast growing surveillance manufacturer. The company has made inroads into most sectors of the surveillance market while also opening an office in South Africa in late 2015.

Hi-Tech Security Solutions spoke with Matthew Guo, technical director of Hikvision’s Johannesburg office about its new seminar programme and the products the company was promoting.

The local office is pushing the Hikvision brand in South Africa, not only the products available from the Chinese surveillance giant, but is also focusing on approaching the integrator market directly with solutions designed for specific verticals. The company has embarked on a range of seminars this year, focused on its thermal cameras and its Automated Number Plate Recognition (ANPR) solutions.

The reason for Hikvision’s seminar programmes is to ensure the company is seen as a solutions provider and not only a technology provider. Guo says this is why the events were aimed at system integrators and their customers.

When it comes to thermal cameras, the seminar started out defining what thermal cameras were and how they worked, identifying the areas where they will deliver the best results. Hikvision’s second generation of thermals not only work on perimeters and discovering people in large areas, such as warehouses, the company has also developed thermals with the purpose of detecting fires. The new generation of thermals includes two-lens solutions that offer thermal as well as optical views in one system.

Guo explains that the cameras are able to detect a difference in temperature of as little as 2 degrees Celsius. Not only will this raise the alarm when a fire starts, allowing quick reaction before it spreads, but it can also be used to monitor the temperature of machines in a factory to ensure they don’t overheat.

ANPR solution

One of the verticals Hikvision is focusing its efforts on is ANPR. With global car ownership at 1.2 billion in 2014 and the ANPR market expected to grow to over $850 million in 2018 according to IHS, it’s definitely a growing market. Trends in South Africa also show a steady increase in rollouts of ANPR systems in many locations, some of them fully implemented by the SAPS and even some Metro Police units.

Guo explains that Hikvision has two cameras designed for ANPR (the DS-2CD4A26FWD-IZS with different lenses). Different lens choices will determine where the cameras are best suited and the quality of the image captured. The number plate recognition software is embedded in the cameras, allowing for faster processing and less stress on servers or NVRs.

It’s iVMS 5200 Professional management software is able to provide for various decision making and reporting features, such as white and black lists of number plates. A vehicle on a white list will be granted automatic access, depending on the location’s policy, while black listed vehicles will not be able to enter or will require human intervention before being allowed to enter. Many functions are built into the system waiting for users to configure them to their specific requirements.

While Hikvision has a complete solution, Guo says it realises it needs to cooperate with other sources of information and the system is designed to allow for easy integration to ensure the best solution available is delivered to the end user.

The company plans more seminars this year, the next to be hosted in Durban.

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

Sunell expands operations in South Africa

No stranger to South Africa’s security surveillance industry, Sunell Security recently announced the expansion of its local operations. The expansion includes the appointment of new distributors for Sunell’s products, as well as the opening of a new branch in Cape Town along with the appointment of a new business development manager.

Well known in the local security industry, Craig Herbst has been appointed as Sunell’s business development manager for the region. His role will be to ensure the Sunell brand is well represented in all areas of the country and that customers have access to all the technical and implementation support they require.

Part of this focus on the customer is the opening of the surveillance company’s first branch in Cape Town, where the demand for the Sunell brand has soared over recent months. Being close to customers is critical for Sunell, and it will be in a better position to accomplish this goal with a direct presence in the Western Cape.

Meeting customers’ requirements is also the reason for Sunell’s new distribution agreements. The company’s products will now be distributed by four South African companies: ADI Global, Eurobyte Technology, Pentagon, and TPA Security Distributors.

In the next issue of Hi-Tech Security Solutions, we will delve further into the distribution agreement and ask the four distributors why they have opted for Sunell.

For more information contact Sunell SA, +27 (0)11 469 3598, sales@sunellsecurity.com, www.sunellsecurity.com.
2N announced on May 30 that it had signed an agreement to be acquired by Axis Communications in a strategic decision to add intercom to its IP security portfolio.

2N is a leading player in the field of IP intercom and also operates in other areas, for example, IP audio and IP lift intercom. The company has well-established sales channels through electricians and telecom installers as well as lift manufacturers, which can serve as a complement to Axis’ present global sales channels. At the same time, 2N will benefit from Axis’ strong market position and R&D resources.

“The acquisition supports our ambition to contribute to a smarter and safer world. There is an increased customer demand for integrated solutions with open standards that deliver enhanced security. Together with 2N we can meet that demand,” says Peter Lindström, VP new business at Axis Communications.

According to Aaron Dale, analyst for IHS, “2N’s route to market and IP focus makes this a logical acquisition for Axis, which is in strong position to develop and market 2N’s existing product line.

“This acquisition will also give Axis a stake in the market for audio and video door phones, which IHS forecast will reach nearly $2.6 billion by 2020. However, the true value in the acquisition is not likely to come from Axis’s ability to penetrate the audio and video door phone market, but in its strengthened ability to provide a more complete IP security solution (a position that Axis have been building in recent years).”

The market for open IP audio and video door phones is forecast to grow much faster than the alternative market for traditional analogue door phones. However, in recent years there has been the emergence of a third market, in the form of video doorbells, which has the potential to hamper sales of IP video door phone. These products have similar functionality to a residential video door phone, with two-way audio and an integrated HD camera. The main difference is the outdoor unit is synced to the user’s smartphone rather than a fixed indoor unit.

“Vendors have already announced partnerships with large residential security companies and the video doorbells will offer additional product options in the smart home and residential security businesses,” adds Dale. “The video doorbell market also attracted considerable investment over the two years to 2016, which has allowed for comprehensive marketing and advertising campaigns.”

The 2N brand will remain and the company will operate as a subsidiary within the Axis group. The joint operations will concern knowledge sharing and assisting each other in R&D and market access. An important joint task is to accelerate the convergence from analogue systems towards IP intercom and the development of new opportunities.

“We plan for development and growth for Axis as well as for 2N. The market is growing and by acquiring 2N we can continue to drive the change in the market,” says Lindström.
Hudaco acquires MiRO

The Hudaco group has acquired IP convergence company, MiRO Distribution. The deal was completed by 1 May 2016 and MiRO now operates as an independent subsidiary of the group.

Graham Dunford, chief executive at Hudaco, says that the MiRO acquisition is a particularly attractive one for the Hudaco Group and will allow both the Group and MiRO to expand their respective footprints in a collaborative manner. He explains that this agreement comes on the back of Hudaco’s ongoing strategy to diversify from its traditional mining and manufacturing base into the delivery of high-quality brands to various industrial market sectors.

According to Dunford, a prerequisite for any company that Hudaco acquires is the absolute commitment from the existing management to a long-term future with the group. This has resulted in the development of an earn-out arrangement that sees the management of any acquired company continuing to drive the business for a three-year reviewable period. Not only does this allow Hudaco to put a succession plan into place in the event that the management contract is not renewed, but it also provides customers and employees with the assurance that product quality, as well as service and support, will remain of a consistently high standard.

Bertus van Jaarsveld will remain as CEO of MiRO. He notes that nothing has changed as far as the company’s operational processes are concerned. “We have new shareholders, but MiRO will continue as a standalone company,” Van Jaarsveld says. “Hudaco has a reputation of buying successful companies and letting them get on with business, and MiRO will be no different.”

The MiRO acquisition is Hudaco’s latest foray into the security market, with Elvey Security Technologies and Pentagon already in the group. The acquisition will not cause any friction between the three security companies as the overlap between them is minimal according to Van Jaarsveld. In fact, it may see improved cooperation between the companies, each of which has its own strengths.

Incorporation into the Hudaco Group also affords MiRO more resilience as an integral part of a large and well-established group of companies, thereby allowing MiRO to grow beyond the capabilities and capacities of its current shareholder. MiRO’s offerings will add value to the entire group and more specifically, it will synergistically support the offerings of Hudaco’s Elvey, Pentagon and Global Communications businesses.

Dunford says that each business within the Hudaco Group is incentivised to grow organically and through bolt-on acquisitions. This has allowed the group offerings to accommodate products from more than 750 international suppliers, with a stockholding of more than 225 000 line items.

With no disruptions to the functioning of the company, MiRO will continue its role as an IP convergence leader in South Africa while also focusing on expansion within the country and across its borders.

For more information contact MiRO Distribution, 086 123 MiRO, lerize@miro.co.za, www.miro.co.za

Suprema at FireTech Expo in Namibia

Suprema recently participated at a security expo hosted by Fire Tech Systems, a value added Suprema distributor, in partnership with Connect 24, a local security solutions provider, in Windhoek, Namibia. The event showcased the latest security industry trends and technologies, from cutting edge biometric access control and time and attendance terminals to innovative fire suppression systems. A major theme and feature of the show was integrated solutions that add value by synergising with existing systems.

Chris Lelicanin, distribution manager for Suprema Southern Africa, attended the event to showcase Suprema’s range of products. Highlights included BioStation 2 and the brand new BioStation A2 as well as Suprema’s latest integration with Avigilon.

Avigilon Access Control Manager helps organisations keep people, property and assets safe with an easy-to-use system that won’t waste your time. A high-end, secure, IT-friendly, role-based system that can grow with you, it has the flexibility to work with the systems you already have – helping to eliminate extra work and increase productivity.

ProSync Synchronization Engine, developed by neaMetrics, effectively works in the background managing the data between both the Suprema and Avigilon systems. The enrolment platform is seamlessly overlaid over Avigilon’s identity capture site, making it user friendly and indistinguishable from the end user’s perspective.

“Suprema believes in strong partnerships, both through active participation in market development with its distribution partners, as well as co-operation with leading access control providers. The results of these are evident through exceptional market growth, in Namibia as well as other areas, and we are always looking for opportunities to participate in delivering the benefits that Suprema offer to end-users across Africa,” says Walter Rautenbach, MD of neaMetrics, exclusive Suprema distributor in southern Africa.

For more information contact Suprema, +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za.
Delivering peace of mind around the world.

More and more customers everywhere let us know every day how much they appreciate the work we do to help them protect, control and track their keys. We invented key management, and we just keep making it better for you.

Visit morsewatchmans.com to learn more
MIA converges into IP surveillance market

MIA Telecoms is known as a Samsung distributor in the telecommunications, networking and office printing market in South Africa. The company has been in business for over 17 years, building up a loyal installer and integration channel that builds long-term client relationships based on a rental agreement. The rental agreement offers set costs to customers, which includes maintenance and repairs over a five-year period, after which the clients can refresh their installations.

Bryan Driessel, MD of MIA Telecoms says the company has standardized on the Samsung brand because of the quality and reliability of the Korean products. MIA has also invested in ensuring it has the local skills to support the brand from installation through to maintenance. As a result, the company has over 50,000 customers serviced by its channel.

Recently, Driessel says the company noticed that many of its installers were expanding their scope of operations and installing surveillance solutions for clients. These installations were mostly non-Samsung brand cameras and recorders, which did not live up to the quality customers had come to expect.

The Samsung brand of IP surveillance solutions is a major player globally, commanding about 10% of the worldwide market share. However, in South Africa the brand has lagged and its market share is around 1% or less. This has proved a great opportunity for MIA to expand its scope of operations, boosted by the recent release of the Samsung WiseNet Lite range of products.

MIA has therefore launched MIA Samsung, a division of the company devoted to Samsung IP CCTV solutions and the company has been appointed as the master distributor for the region. (Samsung recently sold its surveillance division to Hanwha, one of the 10 largest companies in Korea, but will continue to use the Samsung brand for the short term.)

Samsung surveillance equipment are tier 1 products, but Driessel says the price MIA can sell the solution for is significantly less than other tier 1 brands. Not only are individual products cheaper, but MIA can beat the five-year total cost of ownership (including repairs and maintenance) for a surveillance installation by about 50% when compared to other tier 1 brands.

MIA will sell Samsung IP CCTV solutions on five-year rental contracts, as well as on a project basis. The company has invested heavily in stock to ensure it can meet the needs of customers immediately and not have to wait for shipments from Asia, and it has also invested in in-house skills to ensure it has the best team of Samsung surveillance technicians in South Africa that are able to handle repairs down to board level. Driessel is adamant that MIA will continue its business model of client loyalty and build a long-term business instead of box dropping in order to move stock.

The products

When it comes to Samsung surveillance products, Driessel notes that the pricing structure makes it easier for MIA to offer cost effective deals. For example, the Samsung Security Manager (SSM) is a full-featured video management system (VMS) but it forges annual licensing fees. Customers pay once for a long-term licence for the product. Samsung products are also natively integrated into third-party VMS solutions such as Arteco and Axxon.

The partnership with these third parties has allowed Samsung to develop video analytics solutions specifically designed to run on its cameras, such as motion detection and automated licence plate recognition applications, among others. The company’s NVRs are also designed to meet stringent quality standards and are able to offer added features such as POS integration. Moreover, they are designed to handle throughput from all the attached cameras at their maximum resolution.

To do justice to the brand and to be able to demonstrate its capabilities, Samsung and MIA are building a demonstration room in Sandton, which will contain all the brand’s products. Driessel says system integrators will be able to visit the location with their customers to see exactly what the Samsung brand can do for their projects.

MIA Samsung is also ready to engage integrators involved in project work. Proof of concept implementations will be provided when required and MIA already has more trained and certified Samsung surveillance technicians than any other company in South Africa. The company will also assist in risk assessments to help end users determine the best security solutions for their environments.

MIA Samsung is focused on the surveillance market, but MIA Telecoms is able to offer clients a converged IP solution, both wired and wireless, that will deliver a reliable network to handle voice, printing and security services, all based on the products designed and developed by Samsung.

For more information contact MIA Telecoms, +27 (0)11 799 7720, stephan@mia.co.za, www.mia.co.za.

Arecont Vision promotes Sanjit Bardhan

Arecont Vision has announced the promotion of Sanjit Bardhan to vice president, Middle East, Africa, and India (MEA).

“Under Sanjit’s leadership, MEAI has become one of the fastest growing and most important regions for Arecont Vision,” said Scott Schafer, executive vice president, Arecont Vision. “We fully expect that with his new role, Sanjit will continue to accelerate company growth, market presence, and customer satisfaction in the region.”

Bardhan leads an experienced team for the complex, multi-national region which supports Arecont Vision end user customers, integrators, and distributors with expert level sales, training, and technical assistance. He joined Arecont Vision in 2011 as regional manager for the Middle East and North Africa. He successfully drove the business across the region in this role, and in 2013 was promoted to director of the expanded territory of Middle East, Africa, and India.

“Bringing Arecont Vision’s industry leading mega-pixel camera products to the Middle East, Arica, and India is extremely rewarding as customers learn of the benefits, quality, and reliability of our unique made-in-USA technology,” said Bardhan. “We will continue to rapidly increase our customer base and provide world-class support throughout the region.”

Prior to Arecont Vision, Bardhan held sales assignments with Clipsal Datacomms by Schneider Electric and later with Anixter Middle East. Bardhan holds a B.E. (Honours) in Computer Science and Engineering from the Birla Institute of Technology and Science. He is based with his family in Dubai, United Arab Emirates.
Reditron has announced the appointment of Jacques Bester as its new national sales manager with immediate effect.

Bester will be responsible for contributing to Reditron's overall sales and business development strategy and increasing offerings to both existing and new clients. He will oversee sales strategic partnership and will report to Mel Labuschagne, Reditron's MD.

Bester is not a new staff member at Reditron, previously known as Norbain SA, he has held various roles since 2003. His last role, as national key accounts manager saw him responsible for business development for the company's key accounts portfolio.

Prior to this, he worked for companies such as Westec Electronics, Ultrak SA, Panasonic, Securicor, Plessey & Siemens.

Commenting on the new appointment, Labuschagne said: “Jacques brings valuable knowledge to Reditron and will continue to be an asset to the management team. His knowledge of the CCTV and access control industry will be valuable as we look to define more innovative solutions for our clients and grow our presence in this industry.”

For more information contact Reditron, 087 802 CCTV (2288), marketing@reditron.co.za, www.reditron.co.za.
Elvey’s 3rd annual expo a success

In Elvey’s 70th year of bringing technology to life, the company embarked on its third annual nationwide Expo. Held in three of our country’s most vibrant cities; the Elvey Expo has proven to be a success. The 2016 Expos took place in Durban at the Moses Mabhida Stadium; followed by Cape Town at the Cape Town Stadium and ended in Midrand at the Kyalami Grand Prix Circuit.

The Expo format was similar to the previous year featuring some of the most prominent brands in the security industry under one roof. These brands included Risco, DSC, Optex, RDC, Siemens, NetworX, Impro, Suprema, Sherlotronics, Fermax, ET Systems, Dahua, Cathexis, HeiTel, Nemtek and FireClass. Visitors at the show were exposed to the latest in electronic security technology; interacted with highly qualified product specialists and were invited to enjoy good food and good company at the cocktail evening. Centred on Elvey’s Heritage pillar, the Expo also provided a platform for the company to share its rich history with attendees.

“Elvey prides itself on its long history based on teamwork, ethics, passion and caring,” says Jack Edery CEO of Elvey Security Technologies. “The Expo provided Elvey with one of the biggest platforms to showcase not only leading class solutions, but also these core values. An event of this magnitude would not be as successful without the team that put this together in an ethical and passion driven manner. All stakeholders in the Expo managed to pull together because of a shared feeling of care towards the industry and the customers it supplies.”

When asked how the show was for him, Patrick Mfueni, general director of ITM Secure Systems in the DRC had this to say: “Visiting the Elvey Expo was such a worthwhile experience. There is definitely room for growth in a country such as DRC to bring in technology such as that offered by Elvey.” Repeat exhibitor and supplier to Elvey, account manager Dene Alkema from Cathexis said that the Elvey Expo brings value to both Elvey and Cathexis. He stated that the Expo was a good platform to better educate people and provide a holistic offering for customers.

The 2016 Expo ran numerous competitions ranging from Elvey’s Land Rover Experience; the FireClass kit competition; Risco’s HandyApp/Stars Programme giveaway; pop-a-balloon fun. Winners of each competition will be announced shortly.

Launched at the show

Intrusion

Risco launched its new intrusion solution called Home Automation. This is one of the brand’s latest developments geared towards the creation of a connected and smart home. Further, Risco launched its new and exciting rewards programme, the Risco Stars Partners Programme.

DSC launched its wireless outdoor PIR mirror detector with an integrated camera. This detector provides a solution for outdoor visual alarm verification and is available in 433 MHz and 868 MHz. The DSC PowerSeries Neo Go App proved popular at the Expo. This app allows for anytime anywhere access to your security system.

Optex showcased its SL-TNR Series. This series represents Optex’s new short range IR beams with versatile power options. The product’s cost effectiveness in terms of battery specs was well received.

Access control

Suprema launched its new BioStation A2 and BioStation L2. These are fingerprint terminals that provide comprehensive access control and time and attendance features based on Suprema’s next generation biometric technology and security platform.

ET Systems introduced its new wireless keypad, the E-Pad O2. The E-Pad O2 is a keyless access control solution with a compact and stylish design. It is fully compatible with all ET products.

CCTV

VisionLine launched its new range of mini network IR PTZ camera. The camera’s compact design as well as its functionalities was a good selling point at the Expo.

Dahua had on show its mobile surveillance solution. The solution includes a full product portfolio ranging from mobile cameras to the fully functional control room environment. The fact that footage gained from incidents captured on this solution can serve as evidence if needed, proved to be a hit.

Cathexis Technologies showcased its CathexisVision IP Video Management Software. The demonstration included Automatic Number Plate Recognition (ANPR), Advanced Video Search, Adjacent Camera Mapping, and improved hardware efficiency.

Elvey would like to take this opportunity to thank its customers and everyone who contributed to not only making the Expo a success; but also to contributing to the company’s growth and success over the past seven decades.

For more information contact Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za, www.elvey.co.za.
FDIA conducts cable tests

FDIA tests cables to determine compliance to international standards.

The FDIA has had growing concerns of the different types of cables, at great variances in price, being sold into the industry. Based on this concern, the FDIA made arrangements to conduct tests on the cables claiming compliance with EN50200. EN 50200 provides the test requirements to ensure PH30 cables remain operational in fire conditions for 30 minutes or more. Cable core sizes and drain wires were inspected.

The competition for cable sales is fierce and by leaving certain elements out of the cable structure allows them to be price competitive, but we wish to remind everyone that these cables are for life safety systems. Should we be looking to cut corners with cable selection?

International cable standards specify cable sheaths to be halogen free. The result of burning cables that are not halogen free is the production of noxious gases and fumes, which therefore becomes an important factor for fire alarm cables.

Cable samples were collected from contractors’ stock. FDIA committee members witnessed the two sets of tests conducted on a test rig in Johannesburg.

The FDIA is not promoting any one cable over the other, or making recommendations, but the tests were undertaken to provide information to the industry as to the performance of these cables. The results reflected in the table are for information purposes only and do not form any sort of approval or disapproval by the FDIA.

For more information contact FDIA, fdia@fdia.co.za or www.fdia.co.za.

<table>
<thead>
<tr>
<th>Brand Name</th>
<th>Distributor</th>
<th>Conductor size</th>
<th>Halogen free?</th>
<th>Cable withstood 30 minute fire and shock test</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Helukable</td>
<td>Drain wire 0.22 mm² Incorrect</td>
<td>No</td>
<td>Passed</td>
<td>BS 8434-2 printed on sheath is the standard for PH 120</td>
</tr>
<tr>
<td>None</td>
<td>PKP Industrial Trading</td>
<td>Drain wire 0.22 mm² Incorrect</td>
<td>No</td>
<td>Failed</td>
<td></td>
</tr>
<tr>
<td>VIONIX Fire</td>
<td>View A Vision</td>
<td>Correct 0.5 mm²</td>
<td>Yes</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>StamnoTec</td>
<td>Stammo Cables</td>
<td>Correct</td>
<td>No</td>
<td>Failed</td>
<td>Cable sheath states PH30 to IEC 60331. Not EN 50200</td>
</tr>
<tr>
<td>Cab-Tech Fire</td>
<td>Cabcon</td>
<td>Correct</td>
<td>Yes</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Cableon</td>
<td>Cabletronics</td>
<td>Correct</td>
<td>No</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>FR Tech</td>
<td>Technoswitch</td>
<td>Correct</td>
<td>Yes</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>PKP Industrial Trading</td>
<td>Correct</td>
<td>No</td>
<td>Failed</td>
<td></td>
</tr>
<tr>
<td>Aco Tech</td>
<td>Stammo cables</td>
<td>Correct</td>
<td>No</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Ram Firecro UTC</td>
<td>UTC Fire and Security</td>
<td>Correct</td>
<td>Yes</td>
<td>Passed</td>
<td></td>
</tr>
<tr>
<td>Noburn</td>
<td>ADI</td>
<td>Correct</td>
<td>Yes</td>
<td>Passed</td>
<td></td>
</tr>
</tbody>
</table>
Dahua launches HDCVI 3.0

Dahua Technology has announced the release of HDCVI 3.0, its next-generation analogue-to-HD video surveillance solution.

HDCVI, also known as high definition composite video interface technology, was developed and introduced by Dahua in November 2012 to address an industry need. Since then it has become a standard for HD-over-coaxial-cable video transmission that allows reliable, cost-effective, long-distance HD transmission, offering improved performance and functionality.

Dahua HDCVI 3.0 technology includes full compatibility with a wide range of industry platforms and technologies, higher video resolutions such as ultra HD and 4K, as well as intelligent features similar to those found in IP systems.

“The worldwide adoption of HDCVI technology is testament to Dahua’s ability to address an industry need,” said Liquan Fu, president of Dahua. “With nearly two hundred million analogue security surveillance systems deployed globally, HDCVI 3.0 is expected to have a far-reaching impact on the security industry for the years to come.”

Full compatibility
HDCVI 3.0 integrates with five popular industry platforms – HDCVI, AHD, TVI, IP and analogue – and can accept input from IP systems. DVRs equipped with HDCVI 3.0 technology can act as an access point to integrate with external passive infrared sensors, smoke detectors and other types of sensors to further provide comprehensive security services.

Ultra HD
HDCVI 3.0 delivers a true end-to-end ultra HD experience to existing coaxial systems. It realises 4-megapixel resolution over coaxial cabling and also offers Dahua Starlight night vision technology that includes 2-megapixel resolution at 0.008 lux illumination and 120 dB WDR. Additionally, it features H.265 compression standard that allows the system to save up to 50% bandwidth.

Intelligence
Dahua HDCVI 3.0 features rich intelligence including facial recognition, people counting, heat map, smart tracking and smart scene adaption. Other basic smart features include intrusion, virtual tripwire, missing object, abandoned object and scene change. Defogging and a voltage overload alarm are also included.

Simplicity
HDCVI 3.0 systems offer the same simplicity and ease of installation as analogue systems of the past, as the cameras can be plugged into the DVRs using coaxial cable. HDCVI 3.0 systems are low-cost and easy-to-build. Video travels long distances with no delays/latency and power can be directly supplied over coaxial cable.

Another advantage of HDCVI 3.0 is the transmission distance compared to other analogue systems. When transmitting general media, the signal can be extended as far as 1 200 m by using 75-5 cable, with a low signal distortion rate.

HDCVI 3.0 not only offers high definition across long distances, but also features no-latency capability for outstanding real-time performance, because there is no compression processing required to maintain its original effect, resulting in vivid image quality.

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

By Dr Craig Donald.

Effective operators are the key to effective surveillance projects.

In an Australian government sponsored review some years ago about what factors influenced how good a city CCTV scheme was, the project looked at a number of factors including the technology, the relationships and involvement with police on the ground, and the standard procedures, among other things. The conclusion to the report contained this statement though: “The effectiveness of CCTV may be very dependent on a whole range of issues but in particular the monitoring strategies adopted by camera operators” (Australian Research Council, 2006).

What effectively came out of the research is that where operators have a clear idea of what to look for, have the decision making capabilities to follow through on looking for specific people or activities of interest, and have the ability to recognise the signs of something happening, performance will be greatly improved.

This, for me, is a result of a number of factors:
1. A willingness to do the job and especially a passion to catch people.
2. A situational awareness of the areas being viewed, the layout, activities, people, and likely suspects and risk areas.
3. The use of individual initiative and skills in thinking through target acquisition and monitoring.
4. Visual analysis skills and observation skills to assist in picking up the issues and anomalies in the areas being viewed.
5. Training in what to look for, an understanding of body language, and how crime develops and incidents occur.
6. Clear and defined responses to events, as soon as signs of a developing incident is occurring, and good communication skills to follow this through.

Things like good SOPs, knowledge of the law, understanding of the control systems, and ability to switch to relevant cameras and track people using systems provide a useful base for people to work from. But these activities do not help catch people. It is like having a racing car that is ticking over but can’t be driven anywhere except up and down the driveway.

If I were to interview someone for a position as an operator, the first question I would ask is how many people have you caught before, and follow this up with additional questions like “how recently?” “What signs did you see?” If somebody has demonstrated a willingness to catch people and the ability to do so, it’s likely to happen in the new operation as well.

I’d follow up on the standard selection tools with assessments to check the observation skills, ensure that they have training in how to pick up the body language involved in crime behaviour and look at their communication skills. Communication skills may be an optional extra at times, in that many people who are good at working with systems and observing people are not necessarily very extraverted or good with communication.

All too often we try and manage and structure the process of security or surveillance excessively and in doing so restrict its usefulness. Guards have to follow a precise route to badge at specific check points to show they are working, and in doing so give criminals a predictable route and show the timing of where and when to break in to the premises. The UK police have a “stop and search” capability where they can stop anyone and search them, but the documentation that has to now get filled in is so onerous that it reduces the chance of this happening. We may define and structure surveillance duties so much that it reduces the potential for initiative and acquisition of the targets we are looking for.

To get the surveillance outcomes we want, we need to empower operators with the skills, training, knowledge, and scope for initiative and independent action to allow them to deliver detection performance. We need to ensure we have the right people for this, and the right rewards – where operators deliver they need to be recognised, and where they don’t deliver the required performance, we need to provide a development strategy to get them to the right point. This involves ensuring they are equipped with the right skills and have the right kind of environment to shine. It also means that we have to have the managers who can facilitate this kind of process.

Dr Craig Donald is a human factors specialist in security and CCTV. He is a director of Leaderware which provides instruments for the selection of CCTV operators, X-ray screeners and other security personnel in major operations around the world. He also runs CCTV Surveillance Skills and Body Language, and Advanced Surveillance Body Language courses for CCTV operators, supervisors and managers internationally, and consults on CCTV management. He can be contacted on +27 (0)11 787 7811 or craig.donald@leaderware.com
We currently face a societal behavioural change in that online shopping is rocketing alongside a global trend towards ‘cocooning’. Combined, these factors threaten long term return on investment (ROI) in the retail property sector. Retail remains the largest GDP sector in SA, so who will take the spoils over the next 20 or 40 years?

Online shopping is being driven by the availability of ever decreasing cheap data connectivity, ease of online purchasing, product research and price comparison. Added to this is that we all value our time in an extremely competitive global marketplace where we’re pressurised to constantly increase productivity. And then there’s marketing pushing the instant gratification factor and “cutting out the middle man” – a major industry disruptor.

Factors leading to an increase in “cocooning” are security, connectivity, social media etc. – gone are the days when you had to drop by a friend’s house in order to arrange a social function if you couldn’t get hold of him on the landline. There’s no need to leave the safety of home and children are hardly ever seen riding bicycles to friends, sport or to the mall – the roads are just too dangerous – whether in South Africa, Australia or America. Asian countries still tend to buck this trend – but that’s a topic for another day.

A mind shift in terms of measurement of ROI on the part of retailers and landlords/investors is required in order to ensure that malls remain relevant in today’s society – with the ultimate objective being to protect their investments.

ROI is normally measured purely in financial terms and investors largely look at the numbers in assessing the value of a property in their portfolio. In the South African context we believe that our 22 000 plus retail centres need to start delivering on an intangible ROI by engaging and investing intensely within their catchment areas, thus ensuring their long term relevance. This requires visionary leadership on a large scale, and could even be a game changer in assisting communities to throttle crime.

Relevance could or can be obtained by ensuring that retail centres are safe destinations which serve additional socialisation needs whilst delivering for retailers … beyond coffee shops and restaurants as part of the tenant mix.

Perhaps sections of a centre’s basement parking could be offered as free space for pop up churches during quiet Sunday morning trading times or night schools, thus attracting potential shoppers while serving a community need. The community must see the centre as being “their centre” – a valuable community asset and a safe destination for their children. Small Crimewatch/CPF office accommodation could be provided along with space in the security office server room for community/local councillor, ward allocation funded licence plate recognition cameras – thus entrenching the centre with local crime fighting initiatives. A community liaison officer could oversee driving/leading these initiatives – linking in with broader initiatives by the City Metro, SAPS etc.

A safe community will be far more likely to support a safe centre which is seen to be a major sponsor of the crimewatch in the area and is seen to be giving back. The knock-on effect is that the footfall should grow or at least be maintained.

Working models of this are Constantia Village and Blue Route Mall in Cape Town, where local crimewatch structures are strongly supported with great reciprocal benefits and results. As security becomes more tightly controlled at a mall, the surrounding community in turn benefits. Criminals are deterred from the area in general and will have to ply their “trade” elsewhere.

Health services or sports facilities could further attract footfall – secure parking areas can be offered after hours to cycling/running clubs as congregation points, with users tipping car guards, thus no cost to the mall (maybe parking revenue forfeited to members). Perhaps the centre’s sports retailers can engage with these clubs/groups as local sponsors etc., thus driving a local marketing catchment approach.

Imagine the knock on effect if 20 000 of our retail centres are safe zones, along with the suburbs/towns in their immediate catchments.

For more information contact Verifier, 086 111 6023, info@verifier.co.za, www.verifier.co.za.
System Integrators

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

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

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

4C Technology
4C Technology is an ‘Electronic Security Technology Integration’ company wholly dedicated to the security needs of medium to large enterprises. We design, supply, install and maintain electronic security systems for customers on a capital and rental basis with contracted service level agreements in place for maintaining systems.
Tel: 0861 42 8324
sales@4c-technology.com
www.4c-technology.com

C3 Shared Services
C3 Shared Services specialises in the design and implementation of intelligent video, fire and perimeter security solutions. The combination of best-of-breed thermal technology and intelligent video analytics ensures that C3’s clients benefit from real-time situational awareness, instant visual verification and the location of any potential perimeter breach threat – even in total darkness.
Tel: +27 (0)11 312 2041
marketing@c3ss.com
www.c3ss.com

EOH Security and Building Technologies
EOH Security and Building Technologies offer you the “best fit” for all of your facility needs whether it is intrusion protection, fire detection, video surveillance, access control, workforce management, energy control or systems integration – we have the system solutions you need. With a Pan-African footprint and either outright purchase or bespoke leasing offering with maintenance and support options we offer the full turnkey solution.
Tel: +27 (0)11 844 3255
wayne.schneeberger@eoh.co.za
www.eohii.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: +27 (0)21 531 1918
info@jcmtech.co.za
www.jcmtech.co.za

Ringmaster Security
Ringmaster Security offers an effective, quality security technology service to the commercial, industrial, retail, education, hospitality and allied industries. We have an intimate understanding of the industry standards applicable to integrated security systems and take pride in the standard of installations, workmanship, neatness, serviceability and levels of customer satisfaction offered.
Tel: +27 (0)11 476 3381
sales@ringmastersecurity.com
www.ringmastersecurity.com

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
Securex 2016 was a hit with visitors and exhibitors reporting a successful event.

Securex 2016 was, by all accounts, a successful event for both exhibitors and visitors. The halls of Gallagher Estate were packed with people from the first day to the last, with a significant number of people attending the various presentations put on throughout the event.

ESDA Breakfast
The event was kicked off early on the Tuesday morning with the ESDA breakfast. ESDA, the Electronic Security Distributors Association, hosted a full house of members and their customers to a hearty breakfast, hosted by the chairperson, Lee-Ann Andreka.

Andreka welcomed everyone to the event and introduced Specialised Exhibitions’ Joshua Low, the event director. Low made a short speech welcoming everyone to Securex 2016, mentioning there were 160 exhibitors from over 20 countries, with 45 new companies on the show this year. Andreka then introduced the keynote speaker of the morning, Alderman JP Smith, Cape Town’s Mayoral Committee Member for Safety and Security.

Alderman Smith spoke about the role technology plays in combating crime, with specific examples from Cape Town’s remarkable successes. (A brief overview of Smith’s five pillars to a safer city can be found at www.securitysa.com/8533a.) These successes not only include bringing crime statistics down, but also a reduction in the number of deaths as a result of residential fires (from 7.9 per 100 000 of the population in 2009, to 3.6 per 100 000), and a remarkable decline in road deaths (from 2 200 down to 1 200) as a result of a Metro Police Service focused on traffic enforcement instead of revenue collection.

Smith explained that government is not an early adopter of technology and therefore needs industry to support it in rolling out working solutions. The standards adopted in Cape Town’s safety initiatives were co-opted from a variety of sources, including local neighbourhood watches and private security companies. The city has also drawn on the expertise available from international police forces who have shared best practises with Cape Town’s law enforcement members.

Bringing the statistics down has not been an easy journey, nor is the journey completed. Smith says the city tried several things, failed on some and succeeded with others. One of the success stories, which will be expanded, is that of specialised units. Instead of having a police force that is meant to deal with everything, specialised units focus on specific areas of crime and have produced good results. Part of the success is finding and hiring experienced leaders to bring proven expertise to the units. Using specialised Metro Police units, gang crimes, for example, have seen a 20% reduction in two years.

Of course, the successes obtained came after the city took responsibility for its own safety initiatives and over the course of a few years increased its policing resources by 70%. This includes 500 ‘Rent-A Cops’ which work in various City Improvement Districts. It is also a result of commitment and involvement from citizens who ‘do their bit’ to help secure the environment they live in.

The city’s CCTV usage will also expand, both from cooperation with private concerns determined to play their part in making Cape Town a safe environment for everyone, as well as the city’s own cameras, more of which will be rolled out in the coming year. There are already over 460 ANPR (automated licence plate recognition) cameras the city can access to track vehicles of interest.

The coming year will also see a larger reliance on intelligence in effective policing, with data gathered from cameras and other locations accessible via dashboards in the control centre as well as on tablet computers in Metro Police vehicles. Cape Town will also be commissioning drones to assist in its safety initiatives, allowing authorities to ‘get eyes on a situation’ quickly and safely.

In summing up, Smith said that cooperation from the business world and private citizens has played a significant role in Cape Town being able to turn the seemingly unstopable growth of crime, something other cities can only hope to emulate.

On with the show
Following the breakfast, the show itself opened and the first day proved to be an extremely busy one with visitors flocking to the stands (traditionally the first day is the slowest). While a couple of the ‘big names’ were missing, their absence was hardly noticed as their places were filled with a host of other companies showing off their wares, which included everything from security clothing to remote controls, access control, perimeter and guard management solutions, to CCTV, intrusion, safes and a host of other systems and solutions.

It goes without saying that we can’t feature all the companies on show in a short review such as this one. What we have done is highlight a few of the companies we met; with additional input later in the review form others.

On the CCTV front we start with Axis. The company had a large stand as always with a host of products on display, from its multi-sensor panoramic cameras, through to its XF40-Q1765 explosion protected fixed network camera and XP40-Q1765 explosion protected PTZ network camera. Which both feature a 316L stainless steel housing certified for hazardous areas according to, amongst others, ATEX, IECEx, cExius and Class I, II/Div 1 for OSHA.

Axis also showed off its first 4K PTZ dome camera, a discrete 720p modular camera, its light finder technology which allows cameras to see in almost total darkness as well as an impressive demonstration of its Zipstream technology which can reduce the bandwidth video requires without compromising important images.

Also on display was the company’s access control systems which, while still fairly new, are creating a new market for the company, especially with its acquisition of 2N (see the news section of this publication).

Bosch Security was also at the show, a first-time exhibitor, demonstrating a range of products. The display included Bosch’s surveillance cameras, including one which spent the show submerged in water while the images it produced were displayed on a screen. Bosch also had four IP cameras in a dark box, where it showed their low-light capabilities. With minimal light, the cameras were able to display the scene in the box, with the 5 MP camera leading the way in terms of clarity.

The company also had its public address systems on display. These systems can serve multiple zones and provide the ability to create individual emergency messages (or announcements made in the normal course of business) for each zone. They can be linked to fire alarms to ensure the occupants of buildings are evacuated as soon as a fire is detected, thereby ensuring maximum safety for all concerned. Bosch also has PA systems designed for

Continued on page 20
Focus on verticals

Powell Tronics’ decision to move the focus away from pure products to a concentra-
tion on four distinct vertical market sectors at Securex 2016, has paid dividends for
the company. John Powell, CEO of the company says the strategic design elements of
the stand resulted in a pleasing number of qual-
ified leads.

A variety of decision makers from large
corporate companies as well as installers,
major utilities and government departments
took the opportunity to discuss customised
solutions with the Powell Tronics technical
and sales specialists.

The back wall of the stand displayed an
integrated solution that included Morpho’s
Sigma family, including the new Sigma Lite
products and Impr’s Portal range, standard
biometric terminals and Morpho 3D face
readers all running on a Portal backbone
and incorporating short-range and long-range
RFID via Impro and NEDAP products.

There was great interest in Powell Tronics’
own ATOM software solutions. Particularly
attractive is the functionality and cost effec-
tiveness of the web-based ATOM time and
attendance software, providing users with
many of the time and attendance capabili-
ties of much more capital-intensive soft-
ware. Furthermore, because the software is
developed locally, it is highly relevant to the
local market and technical backup is readily
available.

Powell Tronics used Securex as an oppor-
tunity to promote team building, with its
entire sales and development team con-
stantly interfacing with potential customers
and suppliers. “Securex 2016 has once given
us an opportunity to expand our customer
footprint and based on its unrivalled brand
promotion ability, we have already secured
our stand space for 2017,” Powell concludes.

Management software can manage, which
includes hundreds of surveillance cameras
from a variety of manufacturers.

Among the latest features Catvision was
talking about were its automatic number
plate recognition (ANPR) capabilities, the new
Advanced Video Search and Adjacent Camera
Mapping features, as well as its improved hard-
ware efficiency which allows more cameras to
be managed on the same server.

Graphic Image Technologies (GIT) was also
there. GIT supplies a range of product, both
hardware and software, including the Flir
range of cameras (which includes the DV Tel
range). GIT also supplies the SerVision range of
solutions for transmitting video over very low
bandwidth connections, as well as body worn
and mobile solutions.

GIT demonstrated its DV Tel (now Flir)
NVRs as well as its VMS, which offers adaptive
streaming. This functionality allows a company
to stream 4K video at a lower resolution to
a control room. When the operators need to
view a specific area of the image, they can
zoom in on that area and the system automati-
cally increases the resolution to allow them
to see the details clearly. While this is happening,
the full image is still being recorded and can be
viewed on other screens.

The system also allows for intelligent
searching, which can for example, show all the
movement in a specific area over time. The
system delivers all the images within that time
period when movement was detected. When
searching for missing objects, for example, the
user can use the search function to steadily
narrow down the time surrounding the objects
description to quickly find the footage of it
being taken.

Once again, Milestone Systems occupied a
large stand at Securex with numerous solu-
tions from the company and its partners on
display. Of the various solutions on the stand,
the new Husky M500 NVR with Milestone
XProtect Expert preloaded, with the option to
select XProtect Corporate, stood out.

What makes the M500 different is that
its internal systems have been optimised to
provide the best video surveillance handling
possible. This means that it can support 512
720p cameras with a guaranteed recording

Continued on page 22
CLASS-LEADING PERFORMANCE

Instant Matching & Authentication
Enlarged sensing area with new fingerprint capture and processing techniques

Live Finger Detection
Enhanced security using a combination of proprietary optics and algorithm technology

Expanded Memory Capacity
- 500,000 Users (1:1), 100,000 (1:N)
- 5,000,000 text logs; 50,000 image logs

Extended Versatility
- Extensive RF card options
- Various interface options

www.suprema.co.za
Continued from page 20

performance of 600 Mb/s. The NVR has a versatile design to be a recording server, failover server, management server and can also be used as an all-in-one video solution.

To ensure it provides the optimal surveillance experience, the Husky M500 Advanced uses Western Digital Purple hard drives, which are designed for video surveillance operations. It also supports up to 48 TB of internal raw storage and has the ability to archive to network-attached storage appliances when additional storage is required.

Artecto also put in an appearance at Securex, demonstrating its open platform VMS software, which has integrated numerous camera and other manufacturers’ functionality into its core. Artecto produces hardware and software for the video surveillance industry.

A bit of networking

IP convergence company MiRO was once again at Securex, exhibiting its range of products in the wireless and surveillance arenas as well as its software and analytics offerings. MiRO offers holistic security solutions and would fit into a variety of categories in the security market.

In the surveillance market, MiRO took on the Uniview brand of cameras, recorders and software this year. Uniview boasts some advanced networking auto adaptability protocols in its cameras that allow uninterrupted communication, even where slow or low bandwidth is an issue, such as remote monitoring over the Internet. Vivotek products, a brand known for its software and analytics offerings, have evolved from simply delivering products and partnerships again with the next Securex.

Quality visitors and interactions

Suprema Securex 2016

This year’s show was a big success. It was well organised with quality visitors and extremely valuable interactions that opened several new partnerships with well-established system integrators, security consultants and security related manufacturers and distributors. It also provided a comfortable platform for strengthening relationships with current clients.

This year Suprema launched the new revolutionary high-end A2 and essential L2 Access and Time Attendance terminals. Both presenting the new international standard for access and time architecture, offering 100,000 fingerprint matches per second, Live Finger detection and ultra-user data transfer speeds. This will be the minimum standard for all Suprema terminals going forward. Reinforcing this, is the launch of BioStar 2.2, which offers extended T&A functionality through its web and mobile platforms while enabling cloud functionality where required.

As always the custom value-adds were one of the major attention grabbers which included the new Android™ T&A extension and EasyRoster workforce management. The R&D team showed off the integration of the IoT with Bluetooth proximity, biometric passport and automation control wrapped up in a custom mobile application to register visitors at the stand.

We were also extremely proud to win the best stand (48 m² plus) this year and want to thank DK Design, employees and partners that made this possible! We are looking forward to increasing our presentation, products and partnerships again with the next Securex.
**MORPHOACCESS® SIGMA LITE SERIES**

SLIM AND POWERFUL FINGERPRINT ACCESS TERMINALS

- **World’s #1 fingerprint technology inside**
  1:10,000 user identification in 1 second

- **High capacity**
  30,000 templates, 250,000 IDs in authorized user list, 1 Million logs

- **Anti-fraud features**
  Fake finger detection, duress finger, timed anti-pass back

- **Flexibility**
  Prox®, iClass® or MIFARE®/DESFire®/NFC contactless card reader as an option

- **Tough design**
  IP65 rated and vandal resistant (IK08)
companies seen as one entered the hall. With an even larger stand than 2015, ZK offered visitors an overview of numerous products it has on offer, from simple access, electronic locks and biometric products to more complex solutions for T&A and more. It also demonstrated its entrance control turnstiles and barriers, allowing visitors to experience them in action.

Morpho, now simply known as Safran, was another regular on the show. Although the MorphoWave was launched in South Africa at Securex 2015, the system still impresses in recognising four fingerprints as the user simply glides their hand over the sensor. Of course there were more products on display, such as the recently launched MorphoAccess Sigma Lite Series which includes two design options, one offering an interactive 2.8-inch colour touch screen and the other features a LED indicator to assist users in the access control process. Both designs offer multiple card reader options (Prox, iClass or MIFARE/DESFire).

Safran partner, Powell Tronics was also there, not only demonstrating its product range, but its integration capabilities that work with the products it distributes. This resulted in the company talking about and showing its own P-Tron and ATOM product ranges, as well as Safran, Impro and Golmar solutions.

No stranger to Securex, Suprema’s stand invited visitors to view and talk about the various products on display as well as the integrated solutions Suprema’s distributor, neaMetrics could offer the security market. Securex marked Suprema’s début of its new fingerprint IP terminal, BioStation A2, which features a quad-core CPU. The terminal can match up to 150 000 fingerprints per second, which makes it the fastest biometric terminal in the world. Along with an increased 8 GB memory, BioStation A2 can store up to 500 000 users and provides instant results with minimal lag time.

Suprema also offered the BioStation L2 fingerprint terminal. A mid-range device that can support enterprise-level requirements in both access control and time and attendance applications, along with Live Finger Detection and the latest OPS sensors. Incorporating the latest fingerprint algorithm and powerful 1.2 GHz quad core processor, the L2 uses parallel processing techniques that result in fast matching speed that rival higher-end models. Loaded with 2 GB flash and 256 MB RAM, BioStation L2 stores and manages up to 500 000 users and 1 million logs.

Visitors to the Suprema stand could also hear about various value-added integrations into Gallagher, Avigilon Access, Impro Portal, Saflec Access Control, Paxton Access, CathexisVision and Milestone VMS, to name a few.

Ideco hosted the networking lounge once again and had its new Biometric Identity Management System (BIMS) on display. BIMS was recently launched in the USA to rave reviews and is sure to establish the company as a world-beater when it comes to identity management in the 21st century.

BIMS offers six biometric modalities in one portable device and delivers a full range of connectivity options, including Bluetooth, Wi-Fi, GSM and LAN. Multi-functional and configurable, the unit has been designed to the world’s most stringent hardware and software security standards, and harnesses intelligent power management for prolonged battery life of up to 12 hours.

Intrusion and perimeter
Nemtek was back at Securex again, displaying its various products for the electric fencing industry, including its new energiser which can be integrated into other security solutions. The company also spoke to Hi-Tech Security about its certified training facility for electric fence installers.

Paxton was also on show with its network access systems. Dan Drayton, country manager for Paxton said: “Securex was a successful event for us as it provided an excellent opportunity to meet with our existing installers and distribution partners. Some very productive meetings were held on the stand enabling us to introduce our product range and easy to install solutions to a number of new customers. Plus, our licence-free software and market-leading 5-year swap out warranty continue to be an attractive offer to installers across the country.”

FSK Electronics took the opportunity to introduce visitors at Securex to its new locally manufactured Rhino high performance hybrid alarm panel and the Raptor remote. The Raptor is the first bi-directional, shock resistant, water resistant long-range remote control that operates on its own licensed frequency, not 433 MHz or 868 MHz, thereby reducing potential jamming threats. It is also immune to false decoding and interference. It includes additional facilities to control other household equipment, such as switching on the lights etc.

A mobile app has been designed that makes managing the whole process much easier, allowing users to have insight into their own security alerts in collaboration with their service providers. It also allows users to remotely arm or disarm their systems, or certain areas of their house. For example, when the family is home, they may decide only to arm the perimeter and not the internal systems.

The above were only a few of the attractions at Securex 2016. The show was packed with exhibitors and there was also the seminar theatre where numerous presentations were heard. We only heard a few of the presentations, but from what we saw, they were definitely worth the time.
Securex 2016 saw a phenomenal growth in visitor numbers of almost 20%. A total of 6 374 visitors (excluding the flow-through from co-located A-OSH EXPO) was the exhibition’s highest attendance number since 2010.

The exhibition welcomed 314 international visitors from 25 different African countries, again an increase of 12% from the 2015 event. Joshua Low, Securex event director at Specialised Exhibitions explains that a targeted marketing strategy, encompassing a traditional media and social media campaign, in the 12-month run-up to the exhibition has definitely paid dividends.

“We have received extremely positive feedback from both our 168 exhibitors and the visitors. It is worth noting that the 2016 event was the debut event for 45 exhibitors, who have expressed their satisfaction at the calibre of visitors who came through their stands,” says Low.

A number of exhibitors have spent the weeks after the exhibition following up the large number of qualified sales leads they received at Securex. “We have been in business for 27 years and never marketed ourselves. We decided to use Securex 2016 as our official launchpad and we were extremely impressed with the volume and calibre of visitors. We saw a lot of visitors from cross border which is an area we are definitely targeting. Securex allowed the visitors to appreciate the look-and-feel of our custom built banking environment solution,” said Bennie Luyt, ITAS.

And that’s not all
Visitor attractions at Securex 2016 included a New Products Display, the Ideco Networking Lounge and the Business Matchmaking Service sponsored by Ideco, which allowed visitors to be pre-matched with relevant exhibitors. This initiative provides the opportunity for meetings to be arranged in advance of the exhibition, thereby maximising the visitor’s time at Securex 2016. The InFiRES seminar, hosted by FPASA was run once again.

Debuting this year was the SAIDSA Tech Man Competition. The event involved 20 of the top certified technicians in South Africa competing to wire up an intruder alarm system within a specified time, according to strict criteria. They were judged on neatness, correct standards and installation techniques.

Another first for Securex was the co-location of the PSiRA (Private Security Industry Regulatory Authority) Pan-African Forum which tackled subjects such as promoting partnerships for crime prevention between state and private security provider.

The Securex Seminar Theatre was packed to capacity with visitors flocking to hear talks by prominent industry speakers on topics such as understanding violent crime in SA and what to do about it, and ensuring data security in a hyper connected world. FPASA held its successful InFiRES seminar for the second consecutive year.

“Bookings for stand space at next year’s Securex, being held once again at Gallagher Convention Centre from 30 May to 1 June, are brisk so we encourage security and fire technology and service providers to ensure they don’t miss the bus,” Low concludes.

To reserve their prime spot interested companies should contact Sven Riddle or Zelda Jordaan on: svenr@specialised.com or zeldaj@specialised.com or visit www.securex.co.za
Multi-sensor surveillance

By Andrew Seldon.

Are multi-sensor cameras the way to go for surveillance security in the entertainment industry?

Surveillance is a critical security factor in the entertainment industry. Operators in control rooms need to see as much as possible and as clearly as possible in order to protect people and property, and in the case of casinos, to catch the sleight-of-hand professionals.

There are numerous options when it comes to surveillance solutions, from high resolution to panoramic cameras and many others, all of which have their pros and cons. One of the newer types of cameras we’re seeing today is the panoramic camera made up of multiple cameras instead of a single fisheye lens.

Of course, multi-sensor cameras are not exactly new; some companies have been promoting them for years. However, there seems to be a drive in the market today from many companies offering multi-sensor solutions. These cameras do have their benefits, one being the ability to retain an overall view of an environment while zooming in on one area, but a multi-sensor camera is not the ultimate or only solution to the entertainment industry’s surveillance problems (or any other industry for that matter).

To find out more about these cameras, and a potential competitor from the 4K fold, Hi-Tech Security Solutions asked Axis Communications, Hikvision and Graphic Image Technologies (GIT) for their take on multi-sensor panoramics, and an alternative.

Hi-Tech Security Solutions: What surveillance solution can you suggest that will offer a panoramic view of the area being monitored as well as the ability to zoom in on the footage?

Roy Alves, Axis: Multi-sensor cameras are gaining huge market acceptance, the major benefit being their ability to increase the camera’s field of view. Instead of using many cameras, it’s a case of using fewer. The challenge still remains, however, in their inability to see around a corners. So as popular as they are there still needs to be a balance of standard and multi-sensor cameras based on the environment under surveillance.

We see them as overview cameras. In a casino environment, a mix of single-sensor and multi-sensor cameras should be used. For the casino floor or large open areas, a number of multi-sensor cameras could be used, however, for details over the table the suggestion would be to use single sensor, high frame rate cameras with low-light capabilities. These cameras would be dedicated to watching for any criminal activity.

Using a combination of these different cameras would further provide for better overall coverage together with in-depth detail over a particular vulnerable area, such as the casino table. The critical success factor would be the choice of video management software allowing for seamless viewing for the operator as well as video playback and retrieval.

Caihan Shen & Changzhi Ke, Hikvision: Hikvision’s Panovu camera with PTZ functionality can achieve this. The all-in-one camera is the whole system, which could capture the whole scenario and at the same time allow users to zoom onto a specific image to magnify tiny details with its PTZ tracking cameras.

Laurence Smith, GIT: We’d be looking at multiple 4K/Ultra HD cameras that offer the ability to get a wide perspective of the area (based on the lens chosen); these cameras would be focused according to the client’s viewing
requirements. Because the 4K camera has the ability to deliver additional resolution above a standard camera, it is possible to electronically zoom in to areas of the picture without losing too much detail.

These 4K cameras can produce up to four times more detail at full 30 fps than today’s top full HD 1080p cameras and legacy 10 MP cameras. Such a setup envisages a 4K camera system which is linked to a digital NVR (network video recorder), such as DVTel’s Latitude platform, as this software offers the ability to watch multiple views from the same camera without losing detail, depending on whether it’s an overall perspective or zoomed in on a local area within the camera.

It would also be useful to integrate a few isolated pan-tilt-zoom cameras in the area, so that if there is a specific incident happening while live, you can also electronically zoom to that specific location with PTZs. This would only be helpful for live viewing incidents, after which 4K cameras can give you the overall picture once the event is over.

**Hi-Tech Security Solutions: What are the storage implications for such a solution?**

Roy Alves: Generally, in critical areas like casino gaming floors, all cameras are recording all the time at maximum frame rate to reduce the chance of a camera not picking up an activity. Using cameras that are bandwidth and storage efficient will result in the ability to have much higher frame rates and for recording at the camera’s full capabilities in terms of resolution. In terms of multi sensor cameras, all viewable footage is recorded, e.g. even if the camera is zoomed into a particular area of view, the peripheral overview visual is also recorded and playback is available.

Caihan Shen & Changzhi Ke: The panoramic images and zoomed images of PanoVu are streamed individually. Operators cannot only view the panoramic image, but also control the image in detail at the same time, for instance to zoom into a specific area to see what’s happening. Since the images are streamed individually, the panoramic and detailed images can be stored separately.

Laurence Smith: The benefits of 4K cameras when implemented with the DVTel Latitude NVR solution are impressive. These cameras are low on bandwidth usage due to adaptive streaming. There’s also the handy fact that the system records total image at all times, regardless of what the operator is viewing, the original image is still recorded as a single feed. If multiple operators are looking at the same footage, the system will still bring this footage through as a single feed.

As for storage implications, because of adaptive streaming, the client can use standard PCs and workstations without requiring massive storage capacity on the back of the NVR. The biggest draw card for such a solution is the fact that it enables single video recording at 4K resolution with the ability to let multiple people view multiple different images from the same single feed, without requiring specialist equipment or infrastructure to do so.

**Hi-Tech Security Solutions: Does this solution enable fast searching and discovery from recorded footage?**

Roy Alves: Yes, all retrieval of footage can be achieved by simply selecting an area in the scene that could have changed, allowing for much faster video playback.

Caihan Shen & Changzhi Ke: Yes, PanoVu supports event searching and playback.

Laurence Smith: There are three different ways to locate and isolate footage after an incident. The first is time – or motion-based and it is possible to examine the video where an exception is triggered by motion and view those particular events. Other functionalities include the ability to thumbnail search and narrow the search down by bringing up thumbnails within certain time parameters. The third option is Smart Search, which allows the operator to highlight a small area of the screen and search for and bring up any changes within that picture.

**Hi-Tech Security Solutions: Where would it be useful to deploy such a solution, particularly with reference to the entertainment sector?**

Roy Alves: We see multi-sensor cameras as a complement for most video surveillance systems, used mainly in open areas or for the coverage of large areas that would normally have required many single cameras.

Caihan Shen & Changzhi Ke: Our PanoVu cameras are perfect solutions for casinos, stadiums, parks and public events where there are crowds. PanoVu could help to clearly see the whole scenario at 180-degrees or 360-degrees, for users to understand every critical event that happens and also to allow them to quickly locate the region in the panoramic scene to zoom in to see the details. This function could hardly be achieved by other security products such as a fisheye camera.

Laurence Smith: Such a solution would work well in casinos, stadiums, theme parks, hotels, stadium security, public events, parking lots, shopping malls and the like. Anywhere where you need video coverage with enough detail to see what’s happening, there’s the possibility for this solution.

For more information contact Graphic Image Technologies, +27 (0)11 483 0333, laurence@git.co.za, www.git.co.za
Hikvision South Africa, Evan Liu, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com
Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com
Multifocal for the big and small picture

Dallmeier offers a new approach to video surveillance of large areas.

Video technology has become an indispensable element of the security arrangements in sports stadia. With its introduction of the Panomera multifocal sensor system, German developer and manufacturer Dallmeier unveiled a new approach to video surveillance of large areas. This technology offers many advantages for those responsible for stadium security.

Roland Meier, director of Panomera Multifocal Sensor Systems at Dallmeier explains further.

What is so innovative about the Panomera system?
With the Panomera multifocal sensor system, a huge area can be monitored from a single location extremely efficiently. The most impressive aspect of the product is that it combines the overall view with simultaneous top detail resolution. Even more distant objects are displayed with the same resolution as objects in the foreground of the picture. In principle it is exactly what the user wants from a video surveillance camera. The entire area observed by the camera should be displayed in uniformly high quality. But anyone who has ever zoomed in on an image will notice a marked difference: The further you ‘move to the back’ of the scene, meaning, zoom into the picture, the greater the loss of detail, causing the picture to become blurry. While objects in the foreground are certainly displayed with sufficient resolution, when the user attempts to enlarge objects from the background, they appear as many ill-defined blocks.

Let’s consider an example from real life, such as an image of a large stadium. The faces of people in the front rows are still recognis-able, but when the image is enlarged the rows further back become blurred and faces become unrecognisable. This is why, when we developed the Panomera, one of our objectives was to ensure that the resolution never fell below the specified parameters, not even in the most distant areas of the image.

How is this high resolution possible?
We are using a completely new lens and sensor concept. In conventional cameras, the pixels are used uniformly within the sensor, that is to say, the available megapixels are distributed evenly throughout the entire image. But the actual scene is not two-dimensional like the sensor, it is three-dimensional – and the expanse of the lateral and depth perspectives becomes progressively larger the further back you go. Now if the pixels are distributed evenly on the camera sensor, this means that the same number of pixels is available for capturing a much larger background area as is available for the foreground of the image. And logically, as a result, more distant objects cannot be resolved any more when you zoom in.

With Panomera on the other hand, we can guarantee uniform resolution over the entire object space. We do not use just a single optical device, but a multifocal sensor system, meaning several lenses with different focal lengths. In this way, we ‘slice up’ the scene so that each area has the optimum focal length assigned to it.

What advantages does this have for monitoring stadia?
Panomera works well both for very wide panoramas and for areas involving great distances. An entire stadium can be monitored permanently with just two Panomera systems. In effect, it is as if you were to combine the advantages of an overview camera and a high optical zoom PTZ camera: Panomera records the entire area continuously, like an overview camera – unlike a PTZ camera for example, where only the currently active zoom area is recorded. But at the same time you can move and zoom anywhere in the entire coverage area – and individuals are clearly recognisable even at distances of more than 160 metres.

So continuous recording of the entire surveillance area is not standard practice?
Until now, no. Of course, fixed dome or box cameras always record the whole of the area they are monitoring. But these cameras are not equipped with an optical zoom, so they
SECTOR FOCUS: ENTERTAINMENT/HOSPITALITY

are not suitable for monitoring expansive areas, or at least only as overview cameras. This is why a lot of PTZ cameras are being used at the moment. These can be used to zoom and move within the scenes. But at the same time PTZ cameras have a definite disadvantage: They can only ever record the area that the operator is currently watching live.

Let’s revisit the example of our stadium: If the operator is currently zooming in on the front left portion of the image, only this area is being recorded. So if an incident were to take place at a different location at the same time, it would not be possible to review it afterwards. With Panomera, on the other hand, the entire scene is recorded continuously and in maximum detail resolution – regardless of which area the operator is viewing live. This makes it possible to analyse incidents after they have occurred.

Couldn’t you also achieve this effect by using several HD cameras in conjunction with each other? An operator can work much more efficiently with a single, synchronised system than he ever could with multiple HD cameras strung together in line. The operator would have to concentrate on lots of individual images simultaneously. Moreover, the field viewing angles could never be synchronised with one another as well as is possible with a single, integrated multifocal sensor system. Quite apart from the fact that the operator would be engaged in a constant ‘battle for resources’ in order to obtain comparable resolution.

Another advantage of the Panomera sensor concept is a substantially higher dynamic range. Panomera works with several sensors, each of which selects its own exposure strategy in order to achieve ideal saturation. While with other cameras an average value is determined, Panomera can make distinctions more effectively: Light areas are exposed for a shorter time and dark areas for a longer time. As a result, situations with a large dynamic range can also be recorded with good quality, without overexposure or ‘drowned’ black areas.

If the entire scene is monitored by just one camera, is it only possible for one security operator to work with the camera or can several operators access it? In contrast to PTZ cameras, with which only one operator can control the camera, with Panomera, an unlimited number of operators can navigate across the entire scene independently of each other. Although all operators are connected with the same camera, each of the individual users can select his view individually and zoom or pan as he desires. Or he can perform evaluations of the recordings at the same time. So analyses can be carried out by any number of employees at various workstations simultaneously, for example one may be watching the overview image live, another may zoom in on suspicious fans in real time, while yet another is looking at the recording from an hour ago to see how the stadium filled up.

Do you not need enormous bandwidth for this? Owing to the multicast capability, several users can view the images from Panomera without requiring repeated transmission of the data via network. This reduces the necessary bandwidth significantly.

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

---

ELECTRONIC SECURITY DISTRIBUTORS ASSOCIATION

Annual Charity Golf Day

Modderfontein Golf Club
18 August 2016 from 11:15

This year we will be supporting the Rand Aid Association

R2800 per 4 ball
Includes dinner & prize giving
Excludes golf carts and caddies
To book contact Pro Shop directly
(Limited golf carts)

Sponsorship Opportunities
Wine for dinner tables 10 bottles white or 10 bottles red
Longest drive or nearest to the pin includes branding T-Box and green – R2000 each
Branding T-Box 1 or 18th green – R1000 each
Watering holes – R500 + drinks purchased directly from golf club
4 ball prizes

Email Shirley to take advantage of these marketing opportunities

To book please contact: Shirley: shirley@esda.org.za
T-off times will be allocated when payment received

Don’t delay – book now to avoid disappointment!
Beyond hospitality security

IP based security systems can greatly reduce total cost of ownership.

Safety and security of guests, employees and visitors are paramount for every hotel operation. However, hospitality is a very competitive business, and so security systems must not only be functional, but also cost efficient and easy to operate. Modular and scalable systems based on standard network technologies allow for integrated solutions which increase security while reducing investments and operational expenses.

Most hotel operators have a clear view when it comes to security systems: They are necessary, legislation requires some of them, and they are costly. The result is that they usually try to comply with the existing regulations with a minimum of capital investment. However, more often than not this approach will turn out to be a bit shortsighted in the long run.

First, capital investment is only one factor in a pretty complex equation. Operational expenses should not be forgotten as these may easily exceed the depreciation and substantially drive up the cost of ownership. Open architectures based on international standards are much better suited to meet such changing needs as they are scalable and flexible by nature.

Security can even drive business

There are a few things to consider when investing into security systems. But it is not only about cost. What is often overlooked is the fact that security systems can even add to the bottom line. Business travellers and tourists alike are becoming more aware of the security threats and risks affiliated with travelling and are increasingly making security a major criterion when choosing their accommodation.

A high security level which is also proactively communicated can thus drive revenues and increase occupancy. More hotels worldwide do therefore opt for voluntary certification procedures, marketing themselves as safe hotels.

On the other hand, a major security breach can have devastating effects on a hotel’s brand, which is usually its most important asset. Whether it is a fire or a terrorist attack, in today’s information driven world a major incident will immediately hit the news and drive potential guests away, if it does not shut down operations altogether.

As we have seen, a high security standard can be very beneficial for a hospitality company, but of course it remains a cost factor. Every hotel operator will therefore have to find the right balance between security and cost levels. When doing a serious evaluation of their security needs, most operators will find that it is simply not enough to invest into mandatory systems only, such as fire detection and extinguishing.

Video surveillance of public areas and floors will today be expected by most guests as it gives them a good feeling of safety and security. Of course this needs to be done without compromising privacy, but today’s video technologies allow hotel operators to securely store and automatically delete all videos after a certain amount of time, unless they are needed for forensic purposes. Access control will more directly be in the interest of most operators, as it allows them to restrict access to and prevent theft from non-public areas such as kitchens, service elevators, storerooms, stairways and utility rooms.

Some intrusion detection system is usually required for critical facilities such as the server or the HVAC room (Heating, Ventilation, Air Condition), as these are prime targets for any kind of sabotage.

Integration is key

So how can hotel operators guarantee a maximum of safety and security while keeping cost under control? The keyword here is integration.

What we see today in most traditional hotels is a security environment that has evolved over time and comprises individual solutions for fire protection, public address, video surveillance, building automation and maybe access control and intrusion detection. However, not all systems are necessarily up to date, and operation and maintenance of a multitude of individual systems results in high operational expenses. The integration of these individual systems therefore has considerable potential for rationalisation. While this is of course more easily done in a green field development, the replacement of aged systems in existing hotels can often be justified as well due to higher security levels and dramatically increased operational efficiency.

Today, integrated safety and security systems are considerably easier to implement than ever before. For the first time, the increasing use of traditional networking technologies such as Ethernet and IP has created a common and cost-effective technical platform for all security technologies. Information from video cameras, fire and smoke detectors or door controllers can be consolidated via common protocols such as TCP/IP.

Further, this kind of integration allows displaying multiple applications on a shared, flexible and configurable user interface – usually Windows based systems and standard web browsers. Using standard networking technologies as the backbone of all security systems enables the operator to run security applications over the existing IT network rather than maintaining two separate infrastructures.
This will very obviously reduce both capital and operational expenses. Adding to this, using IP technology allows the hotel to benefit from economies of scale, as IP components are produced in very large numbers.

Another benefit of open and standards-based systems is interoperability. Initiated back in 2008 by Bosch, Axis, and Sony, ONVIF for example has developed into a worldwide standard for IP based video solutions and guarantees seamless interoperability of video components from a multitude of vendors. For a hotel operator, this means reduced cost and a freedom of choice, as he is no longer stuck with the original vendor of his solution but can always pick additional components that best fit his needs and budgets. In addition, some hardware vendors do have tight relationships with multiple developers of video management systems, making sure that each operator can use the system that best suits the individual environment.

Standards initiatives like Onvif can greatly reduce complexity when it comes to designing integrated security solutions and do ease interoperability between individual systems. Some vendors, specifically those with a wide solution portfolio, have gone a step further and developed intelligent interfaces between say fire detection and public address systems as well as other components such as intrusion detection and video in order to facilitate integration even further. In such an environment it also becomes even easier to implement central operations, management and control.

**Efficient coordination**

However, a shared infrastructure is just one of many benefits of an integrated solution. An integrated approach allows storing all application-related and other data in a unified database. This also enables automatic correlation of events triggered by intrusion detection, access control and video management systems as well as many other components. This in turn means that the operator can automate a lot of tasks that would otherwise require human attention.

As an example, video cameras can be used to automatically verify alarms from an intrusion or fire detection system, alerting the operator only when needed. This allows to greatly reduce false alarm rates from all subsystems – good news for any hospitality business, as false alarms can be very annoying for the guests and just as expensive for the hotel operator. Even more, using IP in video surveillance introduces the possibility of automatic and intelligent video analysis, so that no operator needs to permanently monitor the videos. Alarms are then automatically triggered upon detection of specific events only, such as detection of a human in the kitchen at night when it is supposed to be closed. This does almost eliminate both human labour and human error.

So while integration and the use of standard networking technologies greatly increase operational efficiency and thus save the hotel real money, they are also suited to substantially increase security levels. Event correlation and intelligent analysis enable a much faster reaction and more targeted intervention, potentially reducing the impact of any incident.

Security will always be a substantial cost factor for any hotel operation. But there are ways to reduce both capital and operational expenses and ultimately even make security systems contribute to the hotel’s business and success.

SECTOR FOCUS: ENTERTAINMENT/HOSPITALITY

Crime family stopped at the zoo

Dublin Zoo stops the taking of ostrich eggs by local wild badgers, with a little help from Milestone XProtect video surveillance.

A more comprehensive centralised video management system was needed to manage a growing number of IP cameras that were being deployed to serve a range of needs at Dublin Zoo, including perimeter security, animal welfare, and animal behaviour studies. Zookeepers also had concerns about a few overnight incidents on Dublin Zoo’s flamingos by wild animals. Ostrich egg numbers were down too. Keepers wanted to explore the use of cameras to help study the behaviour, and ensure the welfare, of all animals under their protection.

New Axis thermal and infrared (IR) cameras were integrated with Milestone XProtect Corporate video management software, providing live and recorded video to be viewed on 17 different PC viewing stations around the zoo via XProtect Smart Client. A total of 140 new Axis network cameras were installed by Milestone Expert Certified Partner Kelcom.

The system provided clear evidence of the taking of ostrich eggs by wild badgers. It also discovered unwelcome late night visits by wild otters that harmed a small number of flamingos. Ostrich egg numbers were down too. Keepers wanted to explore the use of cameras to help study the behaviour, and ensure the welfare, of all animals under their protection.

The large eggs were being rolled under a gate, up a hill and then smashed on a rock, whereupon a badger set was getting a tasty meal at our ostriches’ expense. We were able to lay humane traps to catch these badgers and then resettle them in the park land beyond the outer perimeter of the zoo,” explains Gerry Creighton, operations manager, animal and grounds, Dublin Zoo, Ireland.

The new IP video management system has also proved vital in studying animal behaviours, including group dynamics and sleeping habits.

“Through intensive study of images gathered on the Milestone XProtect video system from infrared cameras installed in the bull and cow elephant houses, we learned a great deal about the varied sleeping patterns of elephants at different ages. Elephants sleep on average about four hours per night. They get this sleep in chunks, which tend to get longer as they get older.

“For example, a young elephant will wake up more than 20 times per night, but older ones may only rise four times between the hours of 12am and 7am. That said, the oldest cow of the group – the matriarch – will sleep very little when elephant calves are around, as she sees it as her job to alert them to any impending danger.”

Dublin Zoo also has several cameras deployed in the elephant training area, where animals are taught to do a variety of activities, from presenting their feet for a routine pedicure or making it easier for keepers to perform routine medical inspections. Recordings from this training area are sent to Alan Roocroft, a world-renowned expert in elephant behaviour based in San Diego, California.

Alan reviews these recordings each week and talks to Dublin Zoo about any issues via Skype, all without the expense of flying him over to gain these insights. Veterinary consultants can also be sent these recordings if keepers have health concerns for the animals they are looking after.

For more information contact Milestone Systems, +27 (0)82 377 0415, arms@milestonesys.com, www.milestonesys.com.
MORE IS LESS!

Get more features with superb quality in our 4MP cameras for far less than you’d expect to pay!

**4MP Network IR Bullet Camera**
- VF Lens 3.0-12mm
- 4MP@15fps,3MP@20fps,1080P@30fps
- Triple Streams
- IR Range 20-25m
- Smart IR
- Low bitrate, Excellent low light performance
- 3D DNR,dWDR,ICR
- ROI,Defog,HLC,Corridor mode,DIS

**4MP Vandal Proof Network IR Dome Camera**
- VF Lens 3.0-12mm
- 4MP@15fps,3MP@20fps,1080P@30fps
- Triple Streams
- IR Range 15-20m
- Smart IR
- Low bitrate, Excellent low light performance
- 3D DNR,dWDR,ICR
- ROI,Defog,HLC,Corridor mode,DIS

**4MP Network IR Mini Bullet Camera**
- 3.6mm,6mm optional
- 4MP@15fps,3MP@20fps,1080P@30fps
- Triple Streams
- IR Range 20-30m
- Smart IR
- Low bitrate, Excellent low light performance
- 3D DNR,dWDR,ICR
- ROI,Defog,HLC,Corridor mode,DIS

**4MP Vandal Proof Network IR Mini Dome Camera**
- 2.8mm,3.6mm optional
- 4MP@15fps,3MP@20fps,1080P@30fps
- Triple Streams
- IR Range 6-7m
- Smart IR
- Low bitrate, Excellent low light performance
- 3D DNR,dWDR,ICR
- ROI,Defog,HLC,Corridor mode,DIS

Why pay more when you can get much more for far less?
Contact us on sales@sunellsecurity.com for more information or visit our website.

Shenzhen Sunell Technology Corporation
1, 3-5F Aerospace Microeomotor Bldg Langshun 2nd Rd, Hi-Tech Industrial Park, Nanshan District, Shenzhen, CHINA 518057
Tel: +86-755-88222666
E-mail: sales@sunellsecurity.com
Fax: +86-755-86020152

www.sunellsecurity.com

DON’T BE CAUGHT OFF GUARD... GET RELIABLE SECURITY
Investigating electronic locks and keys

By Allyson Koekhoven.

Hi-Tech Security Solutions takes a look at the issue of key management and how best it can be approached.

The million-dollar question is whether you would be happy having your keys fall into the hands of someone who might have criminal intent? Rhetorical question? Perhaps. But what are you actively doing to ensure that each key your business owns is traceable and remains within your facilities?

As a precursor to the discussion, it is important to point out that there is a marked difference between electronic keys and mechanical locks. Wouter du Toit of Salto Systems says that his company has been in the business of designing and manufacturing electronic locks for a wide variety of industries over a number of years.

The beauty of an electronic lock is that it can use some of the elements of existing mechanical locks and is accessed with RFID cards. These electronic lock sets work with mechanical mortice locks in the door itself. In addition, Salto’s range also includes escutcheons which are finding growing popularity for use at fire doors and emergency exits. All Salto locks require no external power supply and they are completely wireless.

Electronic locks, says Du Toit, can be integrated with a building’s access control element on the door to provide additional security. These locks are quicker to install than a standard access control reader and can be accessed and controlled via a mobile phone or fob.

Hosea Malope of Zonke Monitoring Systems (ZMS), says that monitoring of keys, whether electronic or manual, will provide organisations with greater assurance that their assets are protected. A reputable key management system should both log keys and track them, with predefined instructions on who is permitted to take a specific key and when the key must be returned to the safety of the key box. In addition, the system should have the ability to raise an alert when the key is not returned within the given time parameters.

Tracking can be performed through a web based system that is accessible via a mobile device or PC. This system will provide a real-time indication of where a key is at all times and can remotely allocate a key, as well as the specific function of the key, to a particular person.

Du Toit says that electronic locks can be integrated with access control systems through a mobile phone using mobile apps with Bluetooth functionality or near field communication (NFC). The connection with the remote server will establish whether you have the pre-programmed functionality to enter the door. Presently, Salto locks are enabled to work on Samsung Android devices and iOS phones.

“Rather than opening the door as such, this technology is used to update the RFID card which performs the role of a key for the door in question. This is particularly useful for mobile workforces, specifically where no network infrastructure is available. One therefore uses one’s phone for updating the credentials of the card,” says Du Toit.

Mobile solutions via Bluetooth started this initiative in the hospitality sector, where guests were sent the credentials of their hotel room access. They then use a mobile app and Bluetooth on their phone which is activated to unlock their particular room on the correct day. The benefits derived from applications in the hospitality arena have spilled over into the business access control sector, where consumer driven demand has resulted in a growing number of applications. Consumers concerned about phone batteries dying will not be left high and dry as the RFID card is used as a backup.

Du Toit says that the Salto locks use their own software and systems but they have also been integrated with the software and hardware of many leading access control developers. These integrations are enabled through both web interfaces and a cloud based system.

Malope says that ZMS key box units currently interface with 11 of the more well-known access control systems and the company continues to develop interfaces to further systems as the need arises or consumer demand dictates.

What about electronic keys?

Both Du Toit and Malope are wary about the use of electronic keys due to both the additional initial outlay as well as the cost involved in replacing them should they be lost or stolen. In addition, backup batteries are expensive, so it is always a good idea to ensure that one closely monitors the current battery level to ensure that these keys remain operational. They point out that the upside, however, is that they are difficult to duplicate, adding an additional element of security.

Another advantage of electronic keys that both interviewees acknowledge is that if a key is lost or stolen, it can be invalidated online. Systems can also call for regular revalidation of keys and when this does not occur, the key will be taken offline and will therefore stop working. If someone then tries to revalidate the electronic key at a revalidation point the...
KEY MANAGEMENT & ELECTRONIC LOCKS

Product focus

All Zonke key boxes allow a number of access control modes to be used, including biometric fingerprint, card and PIN, either individually or in combination, depending on the security levels required. The key boxes range from a simple box built into the wall with a PIN used to open it, to more sophisticated vault-style applications. Options are available for private households and also for remote sites.

The Security Asset Manager (SAM) range includes key boxes in 8, 16, 32-, 64, or 96-key designs that house various options such as direct entrapment, interchangeable cores, custom cylinder mounting, tamper-proof key rings as well as KSI keys. The company’s electronic Tamper-Proof Key Rings provide high level security. After the key(s) are attached to the Tamper-Proof-Key Ring, the ends are sealed using a crimping tool. Every ring is stamped with a unique serial number, allowing complete audit of the ring and key.

SAM offers a self-contained fingerprint reader that stores biometric profile data directly in ZMS’ GFMS database. PIN and fingerprint verification provides dual security at the time of authorisation and users may enrol from either a desktop workstation or directly at any device within the GFMS network.

Salto has in fact instituted a system whereby revalidation is required and customisable time periods set for various people’s security levels – hourly, daily or weekly. An online solution using controllers can send a blacklist of users to any device by updating the card.

Du Toit suggests that where possible, one should use a mortice lock rather than a mag lock as this is the most secure element inside the door and is always fail secure unlike a mag lock which is fail-safe.

Ultimately, the goal is to safeguard company assets and this can be assisted through knowing where the keys are at any given point and by protecting them through the use of an appropriate key box system. Furthermore, where budget allows, electronic door locks combined with RFID cards, will provide enhanced security due to their ability to be activated and deactivated remotely.

Mechanical keys are in many instances being superseded by technology such as RFID cards embedded with data that allow access by the allocated user. Lost cards for electronic locks can be cancelled on the fly, allowing an extra level of security not provided by conventional offline access card based systems.

GET STAFF ON-SITE QUICKLY AND SAFELY

Lifeloc Sentinel operator-free breathalysers provide you with the reliability, accuracy, longevity and the speed you need to keep your workforce safe and productive. Lifeloc helps get the right staff on-site everyday with ease and minimal supervision and can integrate into existing access control systems. Law enforcement, oil & gas refineries, construction, maritime and general industry choose Lifeloc to maintain their zero tolerance environments because our high manufacturing standards outshine other low cost breathalysers on the market.

When safety isn’t an option, Lifeloc is your only option.

Choose fast, safe and accurate breathalysers from Lifeloc.

Contact PSA Africa or visit our www.psafrica.co.za to see our full range of fixed and portable Lifeloc breathalysers.

PSA Africa are Lifeloc approved exclusive distributors for Sub-Saharan Africa. Certifications: ISO 9001:2008 / DOT/NHTSA / SAI GLOBAL / SABS

T: 0860 543 356
E: inquiries@psafrica.co.za
www.psafrica.co.za
Secure, durable locks

The GEM ML-350 series electronic lock from Gianni is designed with a high preload release capability that allows smooth operation under varying loads on the door, such as air-conditioning pressure, changes in the weather, warped doors or doors with weather stripping. Made of stainless steel, it has a failsafe mode and handles up to 220 kg preload (side load) pressure and has been fire tested to international standards.

The GEM GL 1200-FS-OITB is an electromagnetic lock in a stainless steel housing and it sealed with fire-rated epoxy. It is available for surface and mortise mount installations with a range of brackets for different uses. It boasts a holding force of over 500 kg.

For more information contact Gianni, inquiry1@gianni.com.tw, www.gianni.com.tw.

Smart locking system

Now there’s an app for opening your doors at home.

Imagine you no longer have to worry about house keys or having to have spare keys made. Imagine your smartphone transforms into a key. Brought to you by ASSA ABLOY, ENTR is a smart locking system that is safe and easy to operate, ensuring the safety of your family by securing your home, and putting an end to lost or stolen keys.

By fitting an ENTR lock you will be able to enter your home by simply using a smart device including a smartphone, tablet or an iPad, biometrics, a remote or a code. Using an encrypted Bluetooth smart device and the ENTR app, you can seamlessly manage access to your home – create, duplicate, and self-manage virtual keys to lock and unlock doors, programme scheduled access authorisation and automatic locking once the door is closed. Your smart device will also notify you that the door is locked or unlocked so you will know at all times when someone who is entering or leaving your home, putting you in full control.

In addition to a smart device, you can also use a touchpad wall reader, a fingerprint wall reader or a remote control which enables you to code up to 20 family members and friends. Installation is simple, remove and replace of the old door cylinder with a new high security Mul-T-Lock door cylinder. No drilling or wiring is required as the system communicates wirelessly.

The battery-operated system is simple and easy to keep fully operational and will not be affected by power outages. The powerful eco-friendly rechargeable batteries can be charged with a wirelessly or wire charger to deliver 24/7 door lock control for a safe and secure home environment.

For more information contact ASSA ABLOY (SA), +27 (0)11 761 5000, www.assaabloy.co.za.

it all comes together… in the …

CONTROL ROOM

CONTROL ROOM DESIGN, MANUFACTURE AND INSTALLATION
+27 (0)11 493 1545 | sales@progroup.co.za | www.progroup.co.za

PROGROUP MANUFACTURING cc
PRODUCT FOCUS: IP ACCESS CONTROL

SCW offers Amatec readers
The Amatec range of readers provide a total solution for time and attendance and access control requirements. All readers are bundled with the basic Mi-Time Lite time and attendance software which can be upgraded to Mi-Time Premier for a fully detailed time and attendance application.

A few of the products in the range include:
• The Amatec Sparrow reader has fingerprint, RFID card and PIN password functionality. It is aimed at SMEs with a user capacity of 1,000. It can do a basic one-door access control application or if configured with the Amatec Wolf controller it will have a fully functional access control system.
• The Amatec Stinger reader has fingerprint, RFID card and PIN password functionality. It is aimed at SMEs with a user capacity of 1,000. It can do a basic one-door access control application or if configured with the Amatec Wolf controller it will have a fully functional access control system. Together with the Stinger rainshield and mounting plate, the Stinger offers an IP65 solution.
• The Amatec Black Widow is an access control reader which caters for PIN, password and card access control requirements.
• The Amatec Wolf is a two-door controller for advanced access control including biometrics, RFID cards or passwords.

For more information contact Security & Communication Warehouse, +27 (0)12 653 1005, marketing@securitywarehouse.co.za,

Integrated lock for access control
Tyco Security Products announced the integration of its C-CURE 9000 security and event management system from Software House with SALTO offline locks for seamless access control of an entire building through a single user interface.

The C-CURE 9000/SALTO solution is ideal for access control systems that require varying levels of security for interior and exterior access points. The solution deploys SALTO offline locks for interior doors that require a moderate level of security, such as storage and office areas, while Software House hard-wired door controllers are used for high security and perimeter access points. With this solution, security operators can control access to all doors into and within the facility through the C-CURE 9000 user interface, based on communications between C-CURE 9000 and the SALTO server.

The solution supports a nearly unlimited number of offline locks and uses SALTO online readers to update cards for offline reader access. The use of access cards for doors instead of mechanical keys results in cost savings, saving human and monetary resources previously spent on lost key replacement. The C-CURE 9000 guided user interface and single sign-on credentialing makes access control management more efficient and user-friendly. No cabling is required for lock installation and offline locks can be installed on almost any door type.

For more information contact Tyco Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com.
Suprema BioStation A2

Wrapped around with rose-gold coloured rim finish that serves as a centrepiece while blending in beautifully with any environment, Suprema’s top of the range IP fingerprint terminal, provides class-leading performance through excellent matching results, uncompromised security and accuracy along with top-notch usability.

BioStation A2 carries a massive 8 GB memory to store up to 500 000 users, 5 000 000 text logs and 50 000 image logs to accommodate enterprise-class sites with room to spare.

BioStation A2 is equipped with the new OPS sensor and Suprema’s improved fingerprint algorithm with the benefit of a reduced capture error rate in various environments. The A2 also features Suprema’s new Live Finger Detection technology which allows it to clearly distinguish fake fingers made from a number of different materials to prevent any fraudulent activity.

BioStation A2 is easy to use and has been designed to secure maximum usability for users, from fast and accurate matching through to smooth graphics and quick response times. A 5-inch IPS LCD touch screen provides wide viewing angles and easy operation that is further extended by a special reinforced glass screen that ensures maximum screen visibility.

For more information contact Suprema, +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za.

Suprema BioStation L2

An essential IP-based fingerprint terminal that delivers comprehensive access control and time and attendance features. BioStation L2 embeds the fastest clocked processor to be implemented in Suprema’s terminals. An abundance of power is used for incredible matching speed of 100 000 in less than a second that can accommodate an enterprise sized user database. The processor attributes to performance increase in a number of aspects from data transfer speed to enhanced image processing, and quick fingerprint authentication.

Featuring a full capacitive touch keypad along with dedicated programmable TA function keys BioStation L2 offers versatility and a friendly user experience through its full colour 2-inch LCD display and intuitive GUI that is easy to understand and self-explanatory.

Administrators can easily add, remove, modify user data or access information from the device.

Add Suprema’s new Live Finger Detection technology, which implements a liveness decision engine using dual light source imaging to block fake fingerprints made from numerous different materials, and you have an IP fingerprint terminal that provides exceptional value, increased convenience and security to users and administrators.

For more information contact Suprema, +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za.

Access control with IP surveillance

Access control should not only focus on the technology typically associated with visitor management and time and attendance such as card and biometric readers, and physical elements such as booms and guards. This is according to Marco de Ru, CTO at MiRO, who says that IP surveillance has a large role to play in an integrated holistic solution.

He explains that Milestone Professional VMS allows business estate managers to run licence plate recognition (LPR) alongside traditional access control solutions at entrances and exits to estates. Milestone’s XPPro LPR reads licence plate information from vehicles and links the licence plate information with video. Advanced matching logic makes it possible to compare recognised number plates with pre-defined lists and initiate automated actions, such as opening a gate, thus increasing work productivity.

De Ru suggests the use of this Milestone solution in conjunction with VIVOTEK IP cameras. The deployment of a 60 fps vari-focal P-iris camera such as the VIVOTEK IB9381-HT is ideal for entrance point to estates. VIVOTEK’s sophisticated Smart Stream II technology enables the camera to optimise quality for desired regions and thereby maximises the efficiency of bandwidth usage.

This day/night camera is also equipped with WDR Pro and SNV, ensuring superb image detail in all lighting conditions. A robust IP66-rated and IK10-rated metal housing provides protection against the elements as well as acts of vandalism and other physical impacts.

At the entrance to buildings, De Ru posits the use of the Milestone Professional system with additional third party analytical software and the VIVOTEK FD9171, to provide accurate counting of people entering and leaving the premises. This is particularly useful at closing time to ensure that everyone who earlier entered the building has also exited the building.

For more information contact MiRO Distribution, 086 123 MiRO, lerize@miro.co.za, www.miro.co.za.
SURVEILLANCE STORAGE EVOLUTION

DATA RESCUE COMING SOON

Best-Fit Applications
- NVR
- Embedded SDVR
- Hybrid SDVR
- Surveillance DVR

FEATURES

The New Generation SV Drive
- The industry’s first surveillance-optimised hard drive precision-tuned for high write surveillance workloads operating 24x7
- Engineered for workloads of 180TB/year, three times that of desktop drives
- Low power consumption and startup current to minimise heat and vibration emission, improving long-term drive reliability
- Tamper-resistant components to help protect drive from environmental elements, increasing field reliability
- Customise power settings for incremental savings during system downtime without compromising time to record
- Reliable performance in multi-drive systems with support from RV sensors
- Coming Soon! Optional 3-year + Rescue Data Recovery Service plan to help protect against data loss from viruses, software issues or mechanical and electrical breakdowns

Available at 25 Branches Countrywide

www.REGALSECURITY.co.za
Hosted security a growth market

By Andrew Seldon.

Hosting your security solution offsite is a big decision, but one that more companies are making.

Hosting is in. In almost every market and industry around the world, companies and individuals have been persuaded to host many of their systems and applications with a service provider. The idea is that you no longer have to worry about technology, but simply use whatever you need as a service.

Accounting software is a good example of this. In the past, companies would have their own accounting software installed on site, probably on the accountant’s computer, from where the financial person or people would manage the business’s money.

Today these same accounting packages are not sold on a CD, but as a service. To use the software you log onto a site on the Internet and away you go. No updates are required, no hardware specifications, all you need is a web browser and faith that your service provider can protect your sensitive financial information.

In the security world, things are going the same way. Hi-Tech Security Solutions has regular features on remote monitoring and hosted services. Many companies out there are looking to rent you a surveillance solution (or any number of other solutions) for a monthly fee. In return, they promise to look after the hardware and make sure it’s working, while often also providing monitoring services.

The benefits they offer are impressive. You don’t have to lay out a large chunk of cash or get a loan to pay for the solution as you rent it month to month. All the additional costs one often forgets, like maintenance and repairs are included so there are no surprises. And you get tax breaks.

What’s not to like?

When discussing hosted solutions, the question of privacy often comes up. Who has access to your data or to your video feeds etc.? To get under the hood of a hosted solution from a local company, Hi-Tech Security Solutions asked Barry East, sales & marketing director of Impro Technologies for some insights into the company’s solution.

Impro has a long history in the South African market and manufactures locally as well. So, what is it doing in terms of hosting and how have clients reacted to the option of paying for a service?

East explains that Impro’s access control software, Access Portal, is available as a single site installation in the cloud. The traditional access hardware, such as the door controllers and readers are still installed on site naturally, however the operator and management software is hosted in the cloud.

It is also where one enrols personnel, such as employees, into the system. All configuration changes and tag holder details are downloaded to the hardware on the site as and when they happen. The hardware then requires no real-time interaction with the server to operate 100% as configured – a critical factor in an environment where connectivity may not be reliable.

“This software is at the heart of the access control solution, East says. “This is where the rules for access are created, or where operators are able to view live actions on the site. Authorised personnel at the client’s business can access reports from the site as well.”

Where there are bandwidth issues, Impro’s solution can also make use of high-speed GSM connectivity. “Through the continued investment and drive of the GSM sector, it has had a strong ripple effect onto other industries such as ours because we are able to use GSM as a backup solution for our cloud services.

“For example, a customer may have a fixed line connection, however, we’ll install a dual SIM GSM backup system so that if their fixed line should fail, they’re still able to access their system 24/7. In addition, Impro’s hardware has been designed so it’s not reliant on a live connection to the server, allowing it to operate in environments with intermittent connectivity.”

Different, but the same

While the service provided may carry the ‘hosted’ tag, the result isn’t really any different to a traditional onsite solution. East says that the service is the same as the traditional onsite solution in that customers receive the same functions and features. The benefits, however, are that the client doesn’t require a full IT infrastructure, servers and the associated skills to maintain and manage that infrastructure.

“In addition, the service can be rapidly expanded even if there is no fixed line infrastructure in place – often a challenge in more remote locations, or when going into certain African locations,” he notes.

When it comes to security, East says the threat to security data is the same as it would be for any Internet connected server – whether in the cloud or on premise. The key is to ensure the correct measures are taken to mitigate and prevent any illegal breach. This is where a cloud or hosted solution may be a better option for some customers, as they are able to pass that responsibility onto their service provider.

“At Impro, we take the security of data very seriously. To this end, we use high security servers within the Microsoft fold, which provides customers with guaranteed server uptime. These are also coupled with a service level agreement, so in the instance of a problem, customers are assured of resolution within an agreed framework.

“Further to this, we use industry-leading security frameworks for the database. To further enhance the data protection, client connectivity to the cloud server is through HTTPS with security certificates.”

Some like it, some don’t

East has found that the market is split over the utility or desirability of a hosted solution. He says the market segment is quite specific. At the entry level, companies enjoy the convenience of a hosted cloud solution, however, at medium to large sites they still prefer on-premise solutions.

This is slowly changing as the world evolves with more products going into the cloud. For example, Microsoft Office 365, a cloud based office software suite; or there’s Salesforce.com which is a cloud CRM system.

“Big global companies are adopting these technologies and so in the next two to five years I expect we’ll see a lot more large companies in South Africa doing the same as they become more accustomed to and trusting of cloud services.”

For more information contact Impro Technologies, +27 (0)31 717 0700, vikkiv@impro.net, www.impro.net.
Kaspersky Lab exposes massive underground market selling over 70 000 hacked servers.

Kaspersky Lab researchers have investigated a global forum where cybercriminals can buy and sell access to compromised servers for as little as $6 each. The xDedic marketplace, which appears to be run by a Russian-speaking group, currently lists 70 624 hacked Remote Desktop Protocol (RDP) servers for sale.

Many of the servers host or provide access to popular consumer websites and services and some have software installed for direct mail, financial accounting and point-of-sale (PoS) processing. They can be used to target the owners’ infrastructures or as a launch-pad for wider attacks, while the owners, including government entities, corporations and universities, have little or no idea of what’s happening.

xDedic is a powerful example of a new kind of cybercriminal marketplace: well-organised and supported and offering everyone from entry-level cybercriminals to APT groups fast, cheap and easy access to legitimate organisational infrastructure that keeps their crimes below the radar for as long as possible.

A European Internet service provider (ISP) alerted Kaspersky Lab to the existence of xDedic and the companies worked together to investigate how the forum operates. The process is simple and thorough: hackers break into servers, often through brute-force attacks, and bring the credentials to xDedic. The hacked servers are then checked for their RDP configuration, memory, software, browsing history and more – all features that customers can search through before buying. After that, they are added to a growing online inventory that includes access to:

- Servers belonging to government networks, corporations and universities.
- Servers tagged for having access to or hosting certain websites and services, including gaming, betting, dating, online shopping, online banking and payment, cell phone networks, ISPs and browsers.
- Servers with pre-installed software that could facilitate an attack, including direct mail, financial and PoS software.
- All supported by a range of hacking and system information tools.

From as little as $6 per server, members of the xDedic forum can access all of a server’s data and also use it as a platform for further malicious attacks. This could potentially include targeted attacks, malware, DDoS, phishing, social-engineering and adware attacks, among others.

The servers’ legitimate owners, reputable organisations including: government networks, corporations and universities, are often unaware that their IT infrastructure has been compromised. Further, once a campaign has been completed, the attackers can put access to the server back up for sale and the whole process can begin again.

The xDedic marketplace seems to have opened for business some time in 2014, and has grown significantly in popularity since the middle of 2015. In May 2016, it listed 70 624 servers from 173 countries for sale, posted in the names of 416 different sellers. The top 10 countries affected are: South Africa, Brazil, China, Russia, India, Spain, Italy, France, Australia and Malaysia.

The group behind xDedic claims that it merely provides a trading platform and has no links or affiliations to the sellers.

“xDedic is further confirmation that cybercrime-as-a-service is expanding through the addition of commercial ecosystems and trading platforms. Its existence makes it easier than ever for everyone, from low-skilled malicious attackers to nation-state backed APTs to engage in potentially devastating attacks in a way that is cheap, fast and effective. The ultimate victims are not just the consumers or organisations targeted in an attack, but also the unsuspecting owners of the servers: they are likely to be completely unaware that their servers are being hijacked again and again for different attacks, all conducted right under their nose,” said Costin Raiu, director, global research and analysis team, Kaspersky Lab.

Kaspersky Lab advises organisations to:

- Install a robust security solution as part of a comprehensive, multi-layered approach to IT infrastructure security.
- Enforce the use of strong passwords as part of the server authentication process.
- Implement a continuous process of patch management.
- Undertake a regular security audit of the IT infrastructure.
- Consider investing in threat intelligence services which will keep the organisation informed of emerging threats and offer an insight into the criminal perspective to help them assess their level of risk.

Read more about xDedic at Securelist.com
As we hear more about how cloud solutions and services are becoming more popular in the business world today, Neil Cameron at Johnson Controls discusses the pros and cons of security in the cloud.

Putting a security platform in the cloud is today highly feasible and beneficial for companies with a national or multi-national footprint. The connectivity and bandwidth is there, it's cost effective and it's reliable. It facilitates integration of multiple business, building and security systems, offers sophisticated control and management features, and drives best practices across the organisation.

But, more importantly, with the right solution or platform in place, it's safe.

Adoption of cloud-based security solutions is growing significantly, but it's important to understand the features and limitations of the platform that you select.

Today, 'cloud' connectivity and services are a commodity. Security is taken very seriously by companies offering cloud solutions as well as enterprises, so a lot of investment has gone into making cloud platforms robust and redundant.

When it comes to a cloud-based security solution, it's a no-brainer for companies with a physical presence in multiple locations and geographies. It not only extends their investment in their security solution by making it accessible via a central cloud location to multiple sites, it adds flexibility and control, as well as assurance that regulatory requirements are being met.

Big benefits to cloud-based security
Cloud security solutions may encompass data, communication, business transactions and physical onsite security such as access control and perimeter security. The benefits include:

- Flexibility, ease of access to data and ease of expansion. A cloud solution makes company data available and accessible from anywhere. This makes it easy for travelling and remote workers to access data and work from anywhere, securely. It also makes it easy for the company to open up a new branch or establish itself in a new location quickly and easily, because all it takes is putting in the hardware – reader and door controller.

- Analytics. With a single scalable platform in place to manage data, video, access control, authentication and security events, analytics becomes easier to do. When security and other systems are on servers in separate buildings, it becomes difficult to interrogate data and discover insights.

- Business crises. In cases of emergency (e.g., fire, terrorist attack, etc.) having an off-premise solution in place is highly beneficial. Data is safe, business critical functions will continue to run, and standard procedures and protocols will be initiated to safeguard people, assets and business systems.

- Standardisation. One of the greatest benefits of having a single centralised security platform is that security standards and policies across locations will be standardised. This means in any situation, standard regulatory procedures will be initiated to ensure regulatory and safety requirements are met and risk is suitably managed.

- Remote control. A cloud platform makes it easy to monitor facilities from anywhere in the world, and escalate any incidents locally. This provides a huge operational saving. It means not having to invest in a local 24x7 control room but gives the company all the benefits of a 24x7 investment.

And if the network goes down?
That's when it becomes really important to have the right system in place to keep facilities open, control access to sensitive areas and ensure important events, such as HR-driven interventions (e.g., maximum overtime, body searches or scans, etc.) will raise alerts. Sophisticated intelligent onsite access control controllers are today available for high-end solutions such as Johnson Controls' P2000 platform.

The controllers have sufficient intelligence and storage capacity to ensure the data, security configurations and policies remain accessible in offline mode. This provides, among others, access control at over 99% efficiency.

Each onsite P2000 access control controller has a built-in server with robust processing capability, sufficient RAM to store a database of critical access information, an IP-based OS, and wireless peer-to-peer communications capabilities to ensure uninterrupted and uncompromised access control.

There are huge benefits to be had from taking security into the cloud but companies need to be aware of the potential pitfalls and find a solution that will meet their needs in on- and offline scenarios.

For more information contact Johnson Controls, +27 (0)11 921 7141, neil.cameron@jci.com, www.johnsoncontrols.com
Security management by cloud

By Paul Williams, major account manager at Fortinet South Africa.

Cloud-based managed security services are the way of the future.

There is no doubt that cloud-based managed security services will be the only way for most enterprises to handle their information security in future. Frost & Sullivan predicted that the market for Managed Security Service Providers (MSSPs) would grow from $6.66 billion in 2011, to $15.63 billion this year, while a new report by Markets and Markets predicts the market size will grow from $35.54 Billion this year to $76.73 Billion by 2021. Infonetics Research says the managed security market will exceed $9 billion by 2017. In EMEA, a 2014 Frost & Sullivan report predicted the MSSP market would grow to $5 billion by 2018. A growing share of this MSSP market is cloud-based, particularly in small to mid-sized enterprises and for non-critical data and systems.

This growing confidence in cloud-based hosted solutions for securing critical enterprise data is a marked change from attitudes just a few years ago, when enterprises feared for the security of any data hosted in the cloud. They expressed concerns about losing control of their data, the implications of hosting it across borders, and accountability for security breaches.

Now, organisations are moving to benefit from cloud-based managed security services in growing numbers, thanks to the cost savings, advanced protection and operational efficiencies they offer. In South Africa, we are seeing steady growth in the number of MSSPs running multi-tenant solutions.

Cloud-based hosted managed security allows even small and mid-sized businesses to benefit from high-level security skills and solutions they would not be able to procure independently. In many cases, the security services are provided by the same service provider supplying other hosted services, simplifying the overall management of the organisation’s systems and applications.

Concerns about where data is hosted are falling away as local hosting centres proliferate and organisations become accustomed to regularly using internationally-hosted cloud-based tools.

The benefits are proving to be significant: access to specialised security skills and the latest threat protection, a lower total cost of ownership, less management complexity and greater ease of use. The only potential drawbacks of using a cloud-based MSSP would be the loss of a certain amount of control over the organisation’s data, and the potential for SLAs to inadequately spell out all processes and accountability.

For this reason, it is crucial for in-house IT and risk management to carefully scrutinise the credentials and SLAs presented by MSSPs, addressing questions like guarantees on DDoS protection, risk audits, recovery times and penetration testing procedures. Responsibilities, liabilities and penalties must be clearly spelt out. Organisations must also take responsibility for those components of information security that are out of the hands of the MSSP – including employee risk, mobile risk, unsecured corporate Wi-Fi hot spots, the effective encryption of data in transit and the need to have backups of back-ups to mitigate the impact of data being wiped.

Effective cloud security

Mayleen Bywater, senior product manager for security solutions at Vox Telecom discusses cloud security services.

Using the cloud for services and data storage is a common solution for many companies today, but we hear about breaches and hacking almost every day. With this state of affairs, is the cloud a reasonable option?

Mayleen Bywater, senior product manager for security solutions at Vox Telecom answers a few questions about the sensitive issue of security when it comes to cloud services – specifically security services.

What is the current state of cloud services when it comes to security, especially surveillance?

Bywater: Cloud computing is becoming a serious feature with regards to surveillance. Businesses which previously did not have the correct security measures in place, are now adopting cloud solutions as the need for more holistic security increases. There is much to be considered when it comes to surveillance, however, and questions inevitably arise around who has the right to monitor whom, and what the acceptable parameters are as far as surveillance goes. For this reason, the cloud in its current state is constantly evolving and it will be some time before it is clearly defined.

What questions do users need to ask of their cloud provider?

Bywater:

a. Are there policies in place to safeguard data, what are these?
b. Which policies, as a business, should I have in place to protect data internally?
c. Where is my data stored?
d. Who has access to my data?
e. Can I access the audit logs?
f. What authentication is used to verify the person accessing my data?
g. Are systems updated continuously? Do you upgrade/ maintain in batches when necessary or do you rely on yearly updates as they roll out?
h. Do you research the latest threats that are target driven and how soon do you implement fixes to ensure the environment is secure?

Who offers these services and what are the benefits for users?

Bywater: Larger ISPs are likely to offer hosted services, the benefits include:

- No costly CAPEX.
- Ease of access to maintenance updates.
- Access to IT skills that may not be available in-house.
- Affordable model, where you can keep upgrading your environment.
- Maximise in house IT skills to benefit your company more efficiently.
- Solution which grows with your business needs.
Intruders? There’s an app for that!

Using mobile apps to enhance remote intruder detection.

The ability to remotely monitor and interact with home and business intruder detection systems has driven the development of intelligent mobile device apps. While there is a proliferation of these apps, similarly to all technology on the market, not all of them are equally up to the task of providing a direct line of communication for business and homeowners. Users need to be aware of the large disparity in app quality and also need to be cognisant of the fact that some apps are proprietary, while others are generic.

This is according to Jack Edery, CEO of Elvey, who says that on the whole, users are comfortable using their mobile devices to log into their remote security systems and have taken the concept a step further by being able to control not only security devices but also other systems that could include HVAC and lighting.

With over 2.6 billion active smartphone (excluding other smart devices) users globally and an anticipated 6.1 billion smartphones in circulation by 2020, there is little doubt that an increasing number of security system owners will leverage the benefits of mobile apps.

There are a number of advantages to using mobile security management apps to interact with your security system, foremost of which is the flexibility this provides you, irrespective of where you are currently located. In turn, productivity is enhanced since multiple locations can be managed from one device. Certain research has found that business owners attributed a 25% increase in productivity to their ability to work remotely.

By adding email and text alerts to systems, business and homeowners are able to stay on top of security system monitoring as events happen. This means faster response times and ultimately, fewer losses.

Elvey has two apps which complement their Tyco PowerSeries and RISCO intruder detection product ranges. The PowerSeries Neo Go app from Tyco has an interactive menu with multiple languages for ease of use. The app allows users to manage up to eight partitions individually in Away, Stay and Night Mode arming options. Compatible with both iOS and Android devices, the app is also compatible with all Power Neo panels and provides the ability to check the status of wireless and hardwired zones. In addition, users can remotely bypass zones, check system faults and institute real-time push notification for alarms, tampering, faults and system event.

The iRISCO app from RISCO allows users to conveniently and remotely arm and disarm security systems. The latest version of the app has enhanced system operations, whereby users can navigate the app during alarms without the need to re-arm or disarm the system. Images and video can also be zoomed-in, viewed to fit the screen and rotated to landscape mode for more flexible viewing.

This live video verification solution seamlessly integrates RISCO’s indoor and outdoor IP cameras with the company’s professional security systems. Users can monitor intrusion events using snapshot images and live video directly on the intuitive interface. Alerts and live video are sent in real-time, ensuring the ability to instantaneously react to events for extended peace of mind.

“There has been much consternation around the risks associated with the use of cloud-based services and mobile apps. However, RISCO has designed its system to deliver higher levels of security than many traditional on-premise solutions. Using its own cloud-based services to control and access its security and intrusion systems on the renowned Microsoft Azure platform, the company assures the highest levels of security, data protection and data privacy,” Edery points out.

“The benefits of mobile security applications, combined with cloud based solutions like hosted or managed services for intruder detection, video and access control systems, are very clear. This holistic package will help users in terms of increased flexibility, greater mobility, and improved peace of mind,” Edery concludes.

For more information contact Elvey Security Technologies, +27 (0)11 401 6700, info@elvey.co.za, www.elvey.co.za.
Data communication is critical

Effective security relies on effective communications.

It is a common belief in large sections of South African society that living in residential estates or closed communities greatly enhances security levels and contributes to a more open and free lifestyle. Due to consistently high levels of crime and attacks on residential properties, people have gradually bought into communal living and quite understandably believe that the 'safety in numbers' approach is the best way forward.

While there is a valid argument for this approach, one needs to bear in mind that as security barriers are introduced, the ability of criminal elements to overcome these is also evolving. Most reputable security companies offer a multi-level solution focused on back up and redundancy based systems. This takes various forms and includes the human element as well as a number of technology-based layers.

Regardless of the type of on-site security resources such as guards, vehicles and CCTV elements, one of the critical denominators is always communication. This includes the on-site point-to-point aspects as well as the links to off-site control rooms, monitoring centres and vehicle assets.

An important part of the security solution is to be able to offer honest and consistent assessments to the providers and customers regarding which types of products and which service providers should be used. A number of consultants tend to push either a single range of their own products or products closely related to theirs.

We at RDC have always held the belief that a wide range of different manufacturers and products is in the best interest of the clients as this spreads the risk and the customer is not trapped or tied in too tightly to one or two providers.

If one accepts that the basics of estate security are in place, walls, gates etc., the next step is to identify the critical elements that are needed and how these will form an integrated turnkey solution. These can be broken up as follows:

3. Electronic visual monitoring – CCTV.
5. Incident management – armed response units.

The key to providing a manageable and trustworthy solution lies in being able to communicate quickly and reliably with the various components listed above. Current technology platforms are widely used by manufacturers and herein lies one of the challenges. The question is “which type of platform do we use?” The answer is not quite as easily reached when one considers the strengths and weaknesses inherent in electronic solutions. Once again we are directed back to the RDC philosophy of using a multi-layered approach to support the basic security components and provide redundancy. RDC offers VHF radio, GPRS and SMS communication options.

For more information contact Roelene Taylor, RDC, +27 (0)11 452 1471/2, exports@radiodata.co.za, www.radiodata.co.za.
ONVIF: The evolution of a standard

By Per Björkdahl, ONVIF Steering Committee Chair.

Per Björkdahl discusses the evolution of the ONVIF standards.

ONVIF has achieved a lot since its founding in 2008. ONVIF has nearly 500 members and there are more than 5,000 ONVIF-conformant products in the market today. Like many other standards, ONVIF has evolved incrementally. Other standards like the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE) and Bluetooth have evolved in many of the same ways that ONVIF has.

Building a foundation

ONVIF was founded by Axis, Sony and Bosch to create a global standard for the interface of network cameras and video management systems. It sought to provide greater freedom of choice for installers and end users to select products from a variety of different vendors. By establishing a basic standard for video in its early days, the founders also hoped to simplify product development for manufacturers.

Early on, ONVIF realised it had to make some adjustments to its approach to creating a standard. Although members had agreed on how to specify APIs for video, the way the manufacturers deployed these in their products varied. As a result, ONVIF turned to the profile concept. The idea with the profile concept was that if manufacturers developed products in accordance with the profile, their products would work together regardless of the manufacturer of the VMS or camera.

ONVIF: The evolution of a standard

By Per Björkdahl, ONVIF Steering Committee Chair.

device was manufactured. A new profile with a new name was created when future changes were needed. ONVIF is using the same approach: if a product is Profile S conformant, for example, it will always be conformant, regardless of when it is manufactured.

A broadening vision

Two years after its founding, ONVIF extended its scope to include access control. Because of the framework established on ONVIF’s formation, the group’s scope for standards can include any discipline within the physical security industry and is no longer solely focused on video. Like ONVIF, other standards organisations have also extended their scope over time.

What is today IEEE and its standards body began in the 1880s as an organisation for electrical engineers whose mission was to standardise electricity. It grew to encompass other industries and is now considered one of the biggest and most influential technology standards in the world. Similarly, the IEC began their standards work in the electricity industry, eventually expanding its scope as well.

IEC and ONVIF

As the demand for interoperability between all devices increases and the concept of the Internet of Things becomes a reality, standards groups are increasingly working together. ONVIF and the IEC are working together in this collaborative way.

The ONVIF specification has been included in the new international IEC 62676 standard for video surveillance systems, the first international standard for video surveillance systems. The IEC’s standard for Electronic Access Control has also incorporated ONVIF’S newest access control specification in its soon to be released IEC60839 standard. This cooperation between standards organisations like ONVIF and IEC will likely continue in order to provide the highest levels of interoperability, which ultimately benefits the end user.

By examining the evolution of other standards, we can see how vital they are to industries, often beginning with a relatively small focus on one specific market and expanding to include others as acceptance and use grows. What comes next for ONVIF depends on its members and the physical security community, who ultimately are together at the helm, driving us forward as new technology develops and evolves.
The benefits of ONVIF membership

ONVIF members speak on ONVIF’s standards, benefits and future.

“Being a member of ONVIF means being at the forefront of video management software, and it means being at the leading edge of driving security solutions forward,” says Stuart Meyers, managing director for Meyertech. “Adopting these global standards has afforded us extra resources to focus on product development and support, rather than having to spend time on individual integration. As a result, we pass on these benefits to our customers, ensuring that their investment is better protected.”

“As a member of ONVIF, Hanwha Techwin has the opportunity to participate in the development of interface standards for network products,” reports Lucas Lee, director of global marketing, Hanwha Techwin. “Companies that establish market standards are generally those who pioneer and lead the market, and Hanwha Techwin’s participation in the establishment of such market standards has led to its sustainable growth.

“In addition, using ONVIF has increased our brand exposure and recognition, enabling more people to learn about our products. As our products have been improved to be ONVIF-compatible with video management systems and cameras from third-party manufacturers, we have had more opportunities to provide outstanding solutions to a greater variety of projects.”

Tim Shen, Dahua’s marketing director, adds, “As a member of ONVIF, we benefit from receiving new protocol delivery specs from ONVIF and also receive indirect market promotion. At the same time, Dahua promotes ONVIF, educating the market on ONVIF and how its standards are positively impacting manufacturers, end users and the industry at large. ONVIF is engaging with Chinese engineers and manufacturers more and more in the development of new profiles. This is a positive step, as the Chinese market can contribute innovative ideas and features that can strengthen ONVIF’s profiles even more.”

According to Bob Dolan, director of security solutions technology at Anixter, “As part of ONVIF, Anixter is able to act as the voice of the client with the engineers at industry manufacturing companies when it comes to the potential requirements that are needed in a standards-based system. This includes installation applications for integrators and their clients, as well as system performance. ONVIF also allows Anixter to work more closely with manufacturers’ engineers to understand new products and features that customers request or that manufacturers want to offer.”

Ottavio Campana, product manager for Videotec, explains why being a contributing member of ONVIF is crucial for Videotec: “Videotec products are designed to be used in uncommon scenarios, for example in hazardous locations or extreme environments. In these applications, we have specialised requirements that are not always used by other manufacturers. By joining ONVIF, we have been able to introduce these new functions to the standard, and after five years of participation in ONVIF, we see that there are clients that now support our advanced functions, so as a company, we do not need to establish a dedicated partnership programme. Furthermore, ONVIF is a good vehicle to make new connections and for networking, both with other manufacturers and with clients.

“So I would summarise the benefits by stating that thanks to ONVIF, we have increased both our direct and indirect relationships with the industry and with customers,” said Campana.

ONVIF’s Impact

According to Shen of Dahua Technology, standards benefit the entire industry: “I believe ONVIF’s standards have aided the growth of the IP product market. When manufacturers use ONVIF’s specifications, they can spend more time and resources on development, rather than expending human resources on ensuring their products are compatible with other manufacturers’ products.”

“Standards and their evolution have a positive influence not only on our products, but also on the whole company,” says Campana.

“Thanks to the adoption of standards, efforts to guarantee interoperability are reduced and we can use the time that we save from this easier interoperability to develop new and unique features.”

“The benefits coming from the adoption of standards are reflected in sales and support, because R&D, sales, support and customers finally share a common language,” Campana continues. “When we all talk about the same topics with the same terms, it is easier to transfer the product value to the customers and to provide satisfying answers to our users when they have doubts or uncertainty regarding interoperability.”

“Anixter is not a technology manufacturer, but a value-added distributor that helps customers understand products and technologies. Customers are increasingly demanding that products and systems meet various performance levels, provide true open architectures and interoperate with their existing systems,” notes Dolan.

“A standard allows customers to know what minimum performance level they can expect from a device or system,” he explains. “As IT departments become more involved in the decision process for security systems,
their reliance on standards-based systems allows them freedom of choice, ease of maintenance and improved performance for their companies. Anixter can guide clients toward these standards-based systems in order to meet their performance expectations. As manufacturers, ONVIF members can also contribute to the development of new standards based on what is happening in the market, which also motivates the entire industry to perhaps be more innovative in developing new technologies and products.” Meyers reports, “We have received a positive impact from ONVIF in the security industry. It has provided opportunities to focus on the core development road map of our products and less attention is required for bespoke integration development.”

“As the security industry changes, global standards are also continuously evolving. ONVIF is the most important standardisation tool in the security sector and is developing global open standards to ensure compatibility between different products from different manufacturers,” says Hanwha Techwin’s Lee. “As ONVIF is increasingly adopted and adds new profiles, we are better able to integrate our systems with related technologies, which enables us to keep pace with the latest trends. Our efforts to develop an interface conformant with ONVIF’s profiles has not only allowed us to integrate with third-party products, but has also given us the opportunity to expand our markets and customer base.”

**ONVIF vs. single system, single manufacturer solution**

“Some businesses and end users do prefer an integrated solution developed by a single vendor,” says Lee. “But I think this will change over time as manufacturers work to improve their own features and launch more diverse products. A lack of effort to establish standards ultimately will narrow the customers’ right to choose what satisfies their needs using a wide range of products made by different manufacturers.”

“Yes, many customers are asking for all-in-one solutions because they can reduce the costs of purchasing multiple devices and/or services and can also reduce the cost and time spent buying from different suppliers. That’s why these solutions are so popular,” says Shen. “But even all-in-one solutions need the support of standardised protocols, which is in part why ONVIF’s profiles have been created to be simple, but also flexible.”

“A guiding rule of thumb is this: simplicity means 80 percent of the features are easy to use and stable, flexibility means 20 percent of the profile’s features are innovative and should anticipate the needs of both manufacturers and end user in the near future.”

“I don’t think all-in-one systems negatively impact ONVIF. In the markets in which Videotec is most active, it is almost impossible to have an all-in-one solution from a single vendor,” explains Campana. “Special environments require special devices and dedicated software, and interoperability is essential in this scenario. But also in small systems, standards can provide vital help to customers.”

“Here’s how: buying a complete solution from a single vendor is not a problem by itself, but end users should try to have a system based on standards, in order not to be bound to a single manufacturer. A single manufacturer exposes the user to two main threats: the cost of proprietary hardware in the future, which can be much higher than the price of standard-compliant hardware, and, even more dangerous, the risk that the manufacturer may not stay on the market forever, which can limit the end user’s ability to extend their systems in the future, even if they accept the risk of paying more for the equipment.”

“No, definitely not,” says Meyers. “Our experience has shown that end users are more tech savvy and don’t want to be locked into proprietary solutions. We have also seen an explosion in consultants requiring ONVIF conformance in the bid process.”

Bob Dolan of Anixter states, “Although some customers have chosen single manufacturer solutions, they are still looking for the assurance that their systems meet minimum performance levels. In addition, industry standards are critical for customers that become dissatisfied with the performance of a particular component in their solution.”

“By embracing manufacturers that adhere to industry standards, they can change direction to a different manufacturer without impact to their overall application. That level of confidence in their decision is more of a safety net and allows them to be in control of their solution.”

**ONVIF’s next profile**

“ONVIF is addressing several disciplines already, through profiles for video and access control,” says Dolan. “IT departments have more influence over how security components and systems communicate and integrate with each other, and other building subsystems and their management of these systems will advance.”

“ONVIF should look at other building subsystems that are being pulled into network-based communication methods and offer a channel for manufacturers to collaborate efforts to on standardisation. This shift to network-based communication across all building subsystems is fuelling The Internet of Things. As a result, and with the assistance of ONVIF, video surveillance and access control devices have become standards-based sensors on the network.”

“Although there is more demand for integrated control in video surveillance, access control, intruder alarm and fire solution sectors, it is not easy to integrate all of these systems together precisely because their related protocols are not standardised,” according to Lee. “As the most widely used international standard in the global security market, ONVIF should expand its coverage to include more security sectors beyond CCTV and access..."
control so it can develop an integrated solution that can be used across all security platforms. If ONVIF expands its coverage to include intruder alarm or fire, not only manufacturers but also end users and even businesses will benefit. The question of what direction ONVIF will take must be answered collectively, and is something that all of us have to be involved in.”

“There are a few product segments that I think ONVIF could focus on with future profiles,” posits Shen. “First, matrix and decoder products could be addressed, as they are very popular in central monitoring centres and stations. Support for intelligence functions is another one, especially since currently each manufacturer defines intelligence functions differently. Thermal products and thermal features should be supported as well.”

“I expect support for thermal imaging soon and for applications exploiting geo-information,” says Campana. “After that, I think that a natural extension of the protocol could be for building automation: we have perimeter security and CCTV and we have access control, both interfacing with HVAC and lighting systems, so building automation seems to be the next natural step. With this extension, even small offices and homes could benefit from advanced functions that now are only available in PSIM systems. I would be happy to install in my house a small system based on ONVIF that can leverage access control with HVAC systems to achieve home automation.”

Meyers states, “There is enough happening in the video market to continue focusing on video, as it is so fast moving and there are many features that are yet to be integrated into the standard, such as analytics access and video content analytics. There also needs to be more ways of accessing manufacturer-developed features. Standard development should proceed to include intruder fire alarms and alarm reporting, as this is frequently requested.”

The future of ONVIF and physical security

“In my personal opinion, ONVIF is most impactful in the IP video sector,” says Shen. “I expect it will continue to help the IP video surveillance grow, perhaps at an even faster pace than it is currently.”

“The video surveillance market has moved fully into the concept of leveraging open APIs to create open architecture systems. ONVIF is leading the charge to true open architectures, and its continued evolution of its profiles will lead to that level of interoperability,” according to Dolan. “The access control market is just starting to get into the open API concept, but it is still many years away from true open architecture. The demand for standards in all of security will help end users and integrators plan more effectively for how and what they implement.”

“I see that system integrators who are working in highly specialised applications of CCTV already know ONVIF well and use it every day,” states Campana. “In more general scenarios, the adoption of ONVIF isn’t as prevalent and I think it is because this market is more driven by price than by the features and warranties that only standard-compliant devices can offer. I expect that if customers are hit by problems induced by a proprietary solution, they will start to ask more actively for standard-based products.”

Meyers of Meyertech notes, “In the past 12 months, ONVIF standard adoption appears in nearly every specification. End users continuously submit inquiries regarding ONVIF, which indicates to me that although the standard is moving forward rapidly, there is a lot of education to be done. A future consideration could be support of camera manufacturers’ features and the breadth of functionality offered across manufacturers’ products.”

“The importance of the hybrid environment is going to grow and become more widespread in physical security. For this reason, it is necessary to promote the use of such standards as ONVIF in order to enable easier system integration that does not require each manufacturer to develop special protocols to make their products compatible with other manufacturers’ products,” concludes Lee. “In order to meet the demand for hybrid security systems, a wide range of perspectives and views must be embraced, where not only manufacturers, but also system integrators are engaged in designing interoperable systems. This collaboration will also be required in meeting the demands of today’s customers.”
The world market for professional video surveillance equipment grew by 1.9% in revenues in 2015. This is according to recently published estimates from IHS, through its Video Surveillance Intelligence Service. This is a much lower rate of growth than in 2014 (14.2%) and 2013 (6.8%).

Lower growth of 4.9% in the Chinese market played a big role; the Chinese market grew by 26.7% in 2014. The slowdown of the market in China in 2015 was largely because of price erosion. Unit shipments of security cameras in China grew quickly, but the average prices of cameras and recorders fell sharply. The Chinese branded supply base became more consolidated, with the two largest estimated suppliers (Hikvision and Dahua) accounting for 47.2% of the market in 2015 compared with 42.8% in 2014.

Slightly higher revenue growth in both the global market and the Chinese market is forecast for 2016, at rates of 6.4% and 11.6% respectively. Product demand will continue to grow quickly and price erosion, though high, is forecast to ease somewhat. This will mean that the world market for video surveillance equipment will be worth $15.8 billion in 2016.

IHS has just added new global and regional market statistics, forecasts and market share estimates to its Video Surveillance Intelligence Service. In addition to the above, other key findings include:

- The supply base for professional video surveillance equipment is gradually becoming more consolidated, with the two largest estimated suppliers (Hikvision and Dahua) accounting for 47.2% of the market in 2015 compared with 42.8% in 2014.

- China is estimated to have been the largest regional market for video surveillance equipment, accounting for over 40% of global revenues in 2015.
- Network cameras accounted for 53% of all security cameras shipped in 2015.
- Less than 1% of network cameras shipped were 4K compliant.
- There has been a rapid transition from standard-definition analogue cameras to HD CCTV cameras (most notably HD-CVI, TVI and AHD).
- In 2016, for the first time, there will be more HD CCTV cameras shipped globally than standard definition analogue cameras.
- Only 24% of HD CCTV cameras sold in 2015 were sold in China.

For more information contact Jon Cropley, IHS Technology, +44 1933 408 075, jon.cropley@ihs.com

Blazer Express

Blazer Pro

Regal Distributors has introduced two new powerful servers from Hikvision. The two products are the Blazer Pro all-in-one server and the Blazer Express intelligent video management software station.

Blazer Pro combines powerful video management system (VMS) with a video storage device for up to 256 network cameras for recording, live view and playback. The VMS included with the Blazer Pro allows for sophisticated alarm management while the VMS add-ons includes licence plate recognition, POS integration, business intelligence, GIS map and access control management.

Blazer Pro is a true all in one server that provides both powerful storage and advanced centralised video management capabilities. Features include up to 7 SATA hard disks and 1 miniSAS can be connected for data storage, it supports HDD hot swap with RAID 0, RAID 1, RAID 5 and RAID 10 storage, two self-adaptive 10M/100M/1000M network interfaces.

Blazer Express is a 16- or 32-channel intelligent video management software station combined with a preinstalled operating system and IVMS software. Blazer Express is easy-to-use and ideal for small retail store and complex surveillance installation with multiple sites.

Features include; automatic device discovery for easy device addition, setup wizard for basic settings, pluggable mSATA design for convenient OS/IVMS maintenance and multiple video search options (tag, lock, interval and segment). Blazer express allows for the connection of multiple Blazer Express stations at remote sites with the use of the Blazer Express Client for centralised management.

For more information please contact Regal Distributors, +27 (0)11 553 3300, info@regalsecurity.co.za, www.regalsecurity.co.za

New servers from Hikvision

Regal introduces surveillance storage servers for large and smaller installations.

Surveillance market slowed in 2015
Tyco Security Products introduces facial biometrics within VideoEdge video surveillance systems for immediate detection and verification of individuals.

With Face Detection analytics, operators can be proactively notified that the surveillance system has detected a person of interest, for example, known criminals, ex-employees, VIPs or other persons of importance. This technology can be useful in protecting stock and assets by alerting security to potential risks much sooner than normal, to increasing customer retention by alerting the store manager to greet an important customer entering the store.

Face detection is built into the VideoEdge network video recorder (NVR), eliminating the need for external servers dedicated to powering the analytics. Up to 1 000 individuals can be easily enrolled and stored in VideoEdge’s on-board database, with the ability to store multiple faces for each person in the system for the highest possible accuracy in identification.

Face detection analytics can also be used ‘post-event’ to speed investigation times by searching video only for specific persons, enabling operators to search video for certain criteria – for example, those individuals who had access to the surrounding area of the incident. Known faces can also be enrolled with video associated for faster future investigations. For example, a retail store can add a photo of a shoplifter at one of its locations to the database so he/she can be seen across the enterprise of sites. If that person enters another store location, operators receive an instant alert to take action to aid in preventing costly shoplifting occurrences.

When used in conjunction with the C-CURE 9000 security and event management system and the victor Unified client application, operators and guards can be visually alerted if a mismatch is detected between the live video image and the stored access control credential image of a card which has just been used on the system. Visual verification of the cardholder greatly increases security to the most vulnerable areas of a business.

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

---

**Squeezed storage.**

Keep the essence with Axis’ Zipstream technology.

Optimized for video surveillance, Axis’ Zipstream technology is a radically more efficient H.264 implementation. Zipstream lowers bandwidth and storage requirements by an average 50% or more for many common 24/7 surveillance use cases - all without losing forensic details.
Bandwidth friendly compression

By Laurence Smith, executive at Graphic Image Technologies.

The correct technology makes remote monitoring over low-bandwidth connections possible.

One of the challenges businesses face today as they expand their global footprint is monitor their sites – in real time – without blowing up their operational costs. This is especially relevant in instances where these businesses venture into areas that have limited communication infrastructure, or where they have so many sites across borders that their monitoring activities could become costly unless consolidated.

The good news is that CCTV technology has made huge strides with the introduction of compression capabilities that enable live video transmission over low-bandwidth networks.

Developed by SerVision, this technology can compress a video stream to four frames per second (fps) at 1 kilobyte per second (KBps), making it easier to stream live and recorded video footage, even from areas that are limited to GPRS or EDGE networks.

Compression technology is key

A standard CCTV camera may record three to 30 frames per second, requiring up to 1 megabyte per second (MBps) to transmit this video stream to a control room or other location.

A CCTV camera that uses compression, such as SerVision’s UVG400, allows the user to, in theory, stream footage from around 1000 cameras over a 1 Megabyte (MB) link relatively easily. This is a big difference in the amount of data that one can transmit, allowing companies to expand their potential exponentially to oversee multiple sites regardless of their location and seamlessly creating CCTV networks across localities, provinces and countries.

Cameras that use compression technology are ideal for deployment at any location where cable Internet connections are not readily available, making it easy to stream live and recorded video footage, even from areas that do not have broadband coverage.

The UVG400 DVR also has the ability to stream bi-directional audio, enabling the security operator to not only listen to sounds transmitted by the microphone at the remote site, but also to transmit audio back to the remote site. By connecting external speakers to the DVR, operators can talk to the local guards, give instructions or give verbal warnings to intruders, or even play pre-recorded audio sequences such as police sirens or warning messages to warn off intruders.

The benefits

CCTV compression technology is ideal for deployment at any location where cable Internet connections are not readily available, or at fixed sites where a backup cellular connection is required. As an example: suppose your company is in the process of constructing a building at a remote location where you do not have broadband access. This technology allows you to run live video footage from any site as long as you can push this footage onto a number of IP networks, whether it’s ADSL, DigiNet, VSAT or GSM.

From a security standpoint, this enhances the ability to monitor the site remotely. For example, a supervisor or manager can remotely observe delivery of materials, how they are stored and if unauthorised persons are on site, assisting to reduce theft or shrinkage.

Analyses of CCTV footage also assist at a project management level by enabling key personnel to better plan and monitor operational activities at the site. This ensures that important tasks take place on schedule and in the prescribed manner.

Staff members who have project oversight are also able to view live video footage from multiple sites – different locations, even different countries – on their computers, tablets and mobile phones. This cuts down on travel time and financial resources spent on physical site inspections while still enabling staff to review the operations on site without actually being there.

These principles apply to all types of businesses including retail stores, where you can for example, monitor multiple stores and warehouses simultaneously or, financial services companies who can monitor their ATMs set up in remote locations. Mining sites can also be reviewed from head office to see what is happening on site without having to be physically present.

Savings in operational costs

While the initial investment to install high-compression video systems must be considered, the savings in the company’s operational costs generally offer enough savings to make up for the expense. Because the system compresses video four times better than traditional technology, the data costs are typically around three to four times cheaper. It also allows the ability to get the video offsite, even if there is no 3G environment.

In conclusion, compression has made remote CCTV monitoring easier and more cost effective, enabling companies to plan and manage their remote projects more effectively. It is an innovation that is quietly making a difference in the business sector’s ability to venture into under-resourced territories.

For more information contact Graphic Image Technologies, +27 (0)11 483 0333, laurence@git.co.za, www.git.co.za
Tyco Security Products announced the 2-Reader IP Access Control Module (IP-ACM), an Ethernet edge device that extends the scalability and cost-effectiveness of a network-based access control system.

The IP-ACM is installed near the doors it controls, helping to reduce wiring and installation costs. The door module can use a facility’s existing IT network to securely communicate via AES 256-bit encryption with an iSTAR Ultra General Controller Module (GCM), where the access control decisions are made using the local access database.

The IP-ACM is a flexible device, capable of supporting two individual doors or one door with in-and-out readers. It is scalable – in a pure IP deployment, up to 32 IP-ACMs can be networked to one GCM. The door modules can even be used in a hybrid solution in conjunction with traditional centrally wired doors for retrofit situations.

The IP-ACM is one of the industry’s IP door modules that offers a configurable offline mode to allow authorised card holders to gain access if network communications are lost. The unit can be set to allow either no access or admit the last 1 000 previous known good cards or admit personnel from a specific personnel group. Card transactions are retained and uploaded when the IP-ACM comes back online. The IP-ACM also features a unique network latency alarm, allowing operators to proactively manage network issues.

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

Matrix Cosec Panel Lite is a standalone IP-based access control solution for SMB and SME units where door controllers are connected to a small panel over Ethernet. It does not require any kind of software installation. This small panel manages up to 25 000 users and 255 door controllers, and provides all advanced access control features required for foolproof security. Standalone access control solution enhances security, improves security, simplifies installation and improves reliability required for an ideal access control.

Features:
• Controls 255 door controllers and 25 000 users.
• Storage up to 500 000 events.
• Ethernet and RS-485 ports available.
• USB for Wi-Fi, 3G/4G/LTE.
• Auxiliary input and output ports.
• Wiegand OUT port available for integration.
• Advanced access control features.

For more information, contact Matrix, +91 81 2869 0106, abhay.joshi@matrixcomsec.com, www.matrixsecusol.com
ICASA compliance for Magic 828am

Powell Tronics’ access control solution helps local radio station to become ICASA compliant.

Starting a new radio station is fraught with challenges, not least of which is compliance with ICASA’s security regulations. This is necessary given the chaos that would occur should a dissenting force take a radio station hostage and use the service to broadcast undesirable propaganda.

Magic 828am is a medium wave (MW) commercial music radio station, broadcasting to Cape Town and the greater Western Cape region. Launched in October 2015 the radio station’s studios are situated in Golf Park, Pinelands, with a transmitter sited at the centre of a geographic triangle with Paarl, Durbanville and Malmesbury as the three corner points. The station radiates a 25 kW signal to major suburban areas of the Cape, unrestricted by mountainous terrain.

Magic’s daytime coverage extends from Cape Town to the Karoo and includes Vredendal to Cape Agulhas, Cape Point to Sutherland and Stellenbosch to Still Bay. Night-time transmissions reach the Eastern and Northern Cape, KZN, Gauteng and beyond. The essential format of the station is all hit music radio from the 1960s through to 2010, mixed with very little talk, sport and news. Listenership has quickly expanded and currently sits in the region of 70 000.

Magic 828am CEO, well known radio and television personality Tony Sanderson approached Powell Tronics in 2015 to discuss the station’s specific security needs. According to Powell Tronics MD John Powell, he was excited to be a part of the growing radio station’s success story and to contribute to an admirable local initiative. A decision was quickly taken by Powell to provide a number of security components to the radio station and transmitter site through one of its resellers.

Powell Tronics’ qualified installer, Tate Skordis of Vizual Security, was an integral part of the security solution, leveraging Vizual’s extensive experience in the security sector to ensure a fully compliant installation. Skordis explains that he was first involved in mid-2015 and together with Sanderson the two companies devised a solution that would ensure that only broadcasting staff would have access to the radio station’s inner workings.

The system incorporates the latest Morpho biometric control technology, together with Powell Tronics’ own time and attendance (T&A) web-based solution, ATOM, which is used to provide time management and obtain up-to-date HR reports on arrival and departure times of employees. The system is uploaded with photographs of all employees and generates automatic reports if someone does not arrive for their shift.

Powell Tronics was responsible for providing training to Magic 828am that allows them to manage the system in-house, from enrolment on the system to setting up reports. In addition, Magic 828am is using a Powell Tronics Golmar IP intercom unit, P-Tron door furniture and a Hikvision CCTV surveillance solution for use at both the radio station and the mast location.

Skordis points out that there are a number of general security and high security areas within a radio station. General, lower-level security is required at the entrance to the premises, while the server room and the remote site where the main mast is located are deemed to be high-security, sensitive areas.

An intercom is installed at the entrance to the reception area, allowing the reception staff to admit visitors into this area. Thereafter biometric readers are installed at the entrance to the studio reception, the station’s administrative section and server room area. All onsite security system monitoring and remote monitoring of the mast is undertaken by the radio station, while Vizual Security provides day-to-day servicing of the system.

Skordis says the system allows for future expansion to other sites and the two day installation was expedited in a straightforward and seamless manner. “The personnel are biometrically controlled from a central database and remote CCTV connections are monitored in real-time for instantaneous reaction. Overall, this is an extremely easy system to use and has provided Magic 828am with a high-end solution.”

“We are thrilled with the state-of-the-art security equipment. The system has operated without glitches and completely fulfils the role it was intended for. I am so impressed with this system that I am currently looking at installing a mirror one at my home. It is something that I would recommend for all business and home owners,” Sanderson concludes.

For more information contact Powell Tronics, 0861 787 2537, marketing@powelltronics.com, www.p-tron.com
The security industry is forever evolving in terms of new trends, technologies, services and products. In order to remain sustainable, it is necessary to stay up-to-date on the latest practices and equipment. Training will meet both staff and employer needs by increasing the quality and flexibility of the business’s services. This is achieved by fostering efficiency, a safe work environment and improved customer service. Focused and targeted training is the most effective method of addressing the needs of your business in the security trade.

SCW Training Academy hosts numerous training courses that focus on the selection of specific products and their correct installation and application. SCW Training Academy is accredited by both SAQA and SASSETA.

SCW offers security training in different disciplines in July and August.

### July & August 2016 Training Dates:

- **6 to 8 July 2016**: Introduction to CCTV
- **14 to 15 July 2016**: Access Control
- **23 July 2016**: Alarm (Non Commercial)
- **2 to 5 August 2016**: Mastering CCTV
- **13 August 2016**: Electric Fencing
- **18 August 2016**: Fibre Optics
- **25 August 2016**: IP Made Easy

Should you wish to book for any of these dates, please contact Marelize Deysel on 012 653 1005 or send an email to training@securitywarehouse.co.za

---

**EDS – TSCM Training Academy**  
*Africa’s premier technical surveillance countermeasures training facility*

- **Tel (012) 665-2109 (International +2712)**
- **www.tscm-za.com**  
- **info@tscm-za.com**

---

**CCTV Surveillance Skills and Body Language Training Course**

A two-day course provided only on an in-house basis to clients in South Africa and internationally. The course focuses on how to conduct observation, increased ability to recognise and read incident risk behaviour, awareness of their surveillance area and an understanding of what to look for when conducting CCTV surveillance.

**Contact**

**Craig Donald of Leaderware**

- **sales@leaderware.com**
Kaspersky to detect targeted attacks

Kaspersky announced an expansion of its enterprise security product portfolio.

Businesses all over the world, including South Africa, have become victim to numerous targeted attacks, including those discovered by Kaspersky Lab (e.g. Equation, Red October, Careto, Flame, Turlo, Epic Turlo, Wild Neuron, Poseidon, Desert Falcons). According to the IT Security Risks Survey 2015, conducted by Kaspersky Lab and B2B International, 9% of organisations globally and 7% in South Africa said they have experienced a targeted attack in the last year.

"Kaspersky Lab has vast experience in threat intelligence and a long history of discovering some of the world’s most high-profile advanced persistent threats" says Christian A. Christiansen, IDC program vice president, security products. "IDC’s Specialised Threat Analysis and Protection Market (STAP) quantifies the opportunity for countering advanced persistent threats and targeted attacks. IDC believes the market will grow to over $3 billion by 2019, with a 5-year CAGR of 28%. This high growth rate is driven by significant adoption of STAP products to address the growing need for advanced threat detection."

Conventional protection technologies are very good at preventing generic threats and attacks from breaching the corporate perimeter. Although the number of such threats is still growing, businesses are becoming more concerned about targeted attacks and advanced cyber-weapons used for the purposes of cyber-espionage or the disruption of business activity. While these threats represent a tiny fraction (less than 1%) of the entire landscape, they present the highest risk to companies worldwide. What is even more important, the number of such attacks is growing steadily, and the price-per-attack is diminishing.

Solving the "one percent" problem requires advanced technology and proper security intelligence that has either been accumulated within the company or requested from a security vendor. The Kaspersky Anti Targeted Attack Platform is designed to identify and highlight unusual actions that constitute strong evidence of malicious intent.

The Kaspersky Anti Targeted Attack Platform is a premium solution based on the most advanced technology to date that draws on Kaspersky Lab’s expertise in the detection and analysis of the world’s most sophisticated threats.

"One of many challenges that businesses face nowadays is a requirement to overcome an array of cyber threats, including very advanced ones, for which they need knowledge of possible attack vectors, indicators of compromise, and the ability to distinguish normal operations from malicious activity. In order to win this battle, organisations need to have strong security expertise combined with technology that is capable of spotting a criminal act in the avalanche of daily activity in a large corporation. This challenge is being addressed with the Kaspersky Anti Targeted Attack Platform, together with the security services aimed at sharing security intelligence and reducing false positive alerts include Kaspersky Lab’s own anti-malware engine to rule out generic attacks that can be blocked by traditional solutions, URL analysis, threat data feeds delivered from Kaspersky Lab’s cloud security infrastructure. The solution’s sensors are responsible for data acquisition over network traffic, web and e-mail as well as endpoints. This allows the solution to detect complex attacks at any stage, even when no malicious activity is taking place, like data exfiltration. Suspicious events are then processed via different engines, including an Advanced Sandbox and a Targeted Attack Analyzer for a final verdict.

The Advanced Sandbox provides a safe, isolated and virtualised environment for analysing suspicious objects and detecting their intent. The Targeted Attack Analyzer utilises data processing and machine learning technologies to assess and combine verdicts from different analysis engines. This is where the final decision to alert the staff is made. Additional technologies that help to reduce false positive alerts include Kaspersky Lab’s own anti-malware engine to rule out generic attacks that can be blocked by traditional solutions.

The Kaspersky Anti Targeted Attack Platform is available as an independent solution or in combination with expert services aimed at rapid incident detection and response. The availability of intelligence services also enables customers to adapt the solution to specific business needs.

Learn more about Kaspersky Anti Targeted Attack Platform at its website: http://www.kaspersky.co.za/enterprise-security/anti-targeted-attacks
Tyco unveils Cyber Protection Programme

Programme highlights companies understanding of holistic approach to reduce the risk of cyber vulnerability of physical security systems.

Tyco Security Products is introducing its Cyber Protection Programme, a multifaceted initiative that provides a holistic approach to cyber security protection for physical security through each phase of the product development life cycle.

Tyco Security Products has developed its cyber security expertise after many years of providing critical solutions for the United States government and other large multinational customers, and holds several industry-firsts, including FISMA-ready access control and video solutions.

“Our Cyber Protection Programme was born from our broad experience in complying with government regulatory standards and meeting the highly complex needs of multinational deployments,” said Steve Carney, senior director, integration platforms, Tyco Security Products. “Our deep understanding of these regulatory rigors helps us to better partner with our customers to more effectively mitigate risks from hackers, activists or other malicious threats when it comes to their physical security systems.”

The Cyber Protection Programme is led by a team responsible for monitoring the product development process and authorising final product release to ensure compliance with secure development best practices. Some of these best practices include:

• Developing and maintaining the company’s security standards for product development.
• Performing security evaluations and testing on devices, applications and systems.
• Providing guidance to help users configure systems to comply with standards such as FISMA and NERC Critical Infrastructure Protection (CIP).
• Performing in-house and independent third-party security testing of Tyco products.
• Evaluating and developing responses to possible vulnerabilities potentially affecting our products as they are discovered.

The programme has already been implemented across several product lines, including Software House, American Dynamics and Illustra, and the Cyber Protection team is managing the long-term strategy for embedding the same cyber safety mindset across other product lines within the Tyco Security Products portfolio.

To learn more about the Cyber Protection Programme, please visit www.tycosecurityproducts.com/cyberprotection.aspx.

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

Gain the upper hand

Strict control of valuables, assets and people is of utmost importance in maintaining the upper hand at high risk facilities such as mines, prisons, airports and in Government and military operations.

At Johnson Controls our P2000 system offers a turnkey solution to security management and access control. It interfaces to X-Ray machines for radiation dosage-control record keeping, as approved by the Department of Health. Its unique integration capabilities also enable gender-specific full body stop and search scans to prevent theft or smuggling of concealed objects. Using the interactive GUI, random algorithm-based searches are performed to ensure employees are not able to calculate the probability of a search. And with CCTV integration and remote system monitoring, chances of collusion and fraud are reduced.

Johnson Controls helps you take care of your assets and the people you are responsible for, giving you the ultimate control, and the confidence to carry on with business as usual.
Lethal tech combo to fight crime

While CCTV systems are being installed to protect schools, banks and other public facilities, is the answer as simple as just adding more cameras? With countries across the globe continuing to face difficult economic conditions, high crime rates are adding to the climate of risk and uncertainty. While CCTV systems are being installed to protect schools, banks and other public facilities, is the answer as simple as just adding more cameras?

How are CCTV systems making us more secure? Jean Turgeon, Avaya’s VP & chief technologist, software defined architecture, speaks about CCTV, crime and whether anyone has the lethal tech combination to fight crime.

Millions of CCTV systems are being deployed around the world to catch criminals. Why is it still not working? Turgeon: Deploying more security cameras can only help in discouraging people from committing crimes – knowing they are more likely to be caught on camera – but what is really important is the quality of the video provided, the use of analytics to help prevent crimes, and ensuring that installed cameras eliminate blind spots.

CCTV has evolved tremendously from the old days of analogue, which for the most part didn’t provide the right level of required quality – so it was difficult to clearly identify individuals, but also hard, if not impossible, to perform real-time analytics. With the evolution of CCTV, cameras now offer extraordinary definition, for instance a licence plate can be read clearly from hundreds of metres away. Even in dark conditions, video surveillance can capture amazing quality images, allowing analytics to be performed in real time.

The transition from analogue to digital, combined with the IP enablement of deployments, provides many other key benefits. Centralised digital recording of high definition video, which can easily be time-stamped and indexed, not only allow whoever is committing the crime to be caught more easily, but also help authorities to be much more pro-active by fully leveraging real-time analytics.

Now suspicious individuals can easily be detected and tracked, while security authorities can be notified to hopefully prevent crimes from happening. This is big data: as you combine the video surveillance data with other relevant databases such as criminal records, arrest records, or whatever, one can easily imagine how positively impactful this technology can be to our citizens. The more CCTV we deploy, the more capabilities the world has to fight and prevent crime.

Experts say that without a strong network to support all these CCTV deployments, we continue to be at risk. Can current legacy networks support more advanced CCTV applications or do we need to look at other solutions?

Turgeon: Legacy networks were built with a series of protocols running on top of each other to meet some of the security or virtualisation requirements. For the most part, the legacy networks used a concept of unicast to communicate – think of it as a one-to-one conversation. This is very inefficient in a client/server-type environment, where the PC or device communicating is communicating with one specific server application. Now imagine this model in a CCTV implementation, where thousands of cameras need to be deployed, causing thousands of network unicast flows to be sent to the recorder and likely to a series of monitoring stations, even potentially to a police department. One unicast stream can quickly turn into three; hence it becomes very inefficient in this type of deployment.

If a camera is not used for monitoring or analytics, but only for recording – for audit purposes for instance – then unicast can likely meet the business needs. Where it gets more challenging is when your the business requirements demand not only recording, but multiple monitoring stations, and other agencies want to gain access to some of the video feeds too.

In such cases, multicast technology will come to the rescue. However, this unfortunately comes with more complexity as more protocols are required to run these IP flows in a multicast mode: protocols such as PIM-SM, OSPF, VLANs with IGMP snooping, and so on will be required to be designed and implemented on the network.

At this point there are two challenges: the recovery times when a failure occurs and the complexity associated with a network that requires 5,000 to 10,000 or more IP surveillance cameras running multicast. Recovery times due to the inter-dependency of all of these protocols can be as long as 35-40 seconds; potentially losing video recording for such a length of time makes audit capabilities pretty much impossible, and may make the video source invalid in a court of law.

Rather than deal with the complexity associated with all these protocols needed to support multicast configurations, many
organisations will choose to stay away from multicast deployments and opt for smaller separate physical networks. This is less than ideal if you are attempting to reduce your TCO.

The good news, there is a solution available in the market, which is based on an IEEE (IEEE 802.1aq) and IETF (RFC 6329) standard that eliminates the needs for all of these protocols and allows a much simpler deployment with extremely fast recovery times in the range of 150 to 400 ms. Not just that, this solution brings scales to new levels where in excess of 14 500 multicast streams have been tested and validated running over a single physical network infrastructure. For customers that need multicast, they have to very seriously evaluate this technology.

**Does CCTV + Network = lethal weapon against crime? Or do we need to go deeper and focus on early notification systems and communication-enabling processes if we are to find the right answer?**

_Turgeon:_ The combination of CCTV deployed over a highly scalable and reliable network is definitely beneficial and can largely contribute to reducing crime and potentially pro-actively preventing it. But, where the technology gets really impactful is when you also add real-time analytics integrated with business process automation. It is great to have analytics detect some abnormal behaviour, but when this becomes incredibly powerful is when an automated workflow can be triggered based on the situation analysis.

Imagine that somebody is attempting to steal something from a store – this could be detected by real-time monitoring and real-time analytics, triggering a workflow that could address the incident without human intervention. For instance, the workflow could automatically order other cameras to track all movements of the suspect, while integrating the video stream to a mobile video conferencing system that could provide full visualisation to security guards or police officers on a smart device. The system could also trigger a store lockdown through SIP-enabled door locks, sound an alarm, enable a strobe light, trigger an alert through paging systems – whatever is required.

In simple terms, the lethal weapon is when you combine a highly scalable, reliable network infrastructure optimised for multicast to support thousands of IP video cameras, with a business process automation system allowing you to customise the desired business outcome.

This is all possible today from Avaya. It is the combination of our SDN Fx architecture and Breeze, the latest iteration of our Engagement Development Platform (EDP). Business process automation and customisation over an automated network optimised for CCTV leveraging multicast makes a very powerful combination today. Now, that is lethal to crime.
More secure governing

By Andre Mundell, Alwinco.

How to ensure effective security for government buildings.

Although governmental buildings and offices, particularly those made accessible to the public, have access control, most of these properties do not otherwise have effective overall security. It is very easy once you have come in at the main entrance to go anywhere inside the building. As it often occurs, health & safety and security are confused and thought about as being the same thing. The reality is that they are not. They can be at the opposite ends of the spectrum at times. These buildings have an OHS report. None of them have their security risk assessment documentation in hand.

To my understanding, governmental properties usually make use of the tender process to procure security services, installations, and upgrades. I have no qualms against this method, but would like to suggest an improvement to enrich this process. This will ensure that the correct security action is taken from the very beginning.

I have always wondered how the specs of the tender are derived. A vast majority of governing boards that I have encountered do not always have an individual onboard with the necessary security knowledge or background. This makes it even harder for them to make the correct decisions in choosing the best security solutions. Tender applications usually consist of only a spec sheet and the price. If you are not familiar with the product or security in general; it could be very confusing.

Most of the time, the end-user doesn’t even understand what all the listed specs mean or what the actual functionality of the product is. It is only after money has been spent and the installation has been completed that many people find that their security is inefficient, incorrect or just not enough. A good security system consists of multiple facets that are interconnected and that complement each other.

Improvements for security tenders

There are two ways in which to approach these improvements. The first is for the governing board to contract an independent security risk consultant to assess their properties. All risks in regards to their physical security will be identified and explained. This will give them a definite guideline of what to request in the tender. They will also be able to judge all applicants on the same standard. Security will be based on a strong, solid foundation.

Additionally, the independent assessor will be able to help them by reviewing and explaining the recommendations made by applicants. He will be able to weed out the best solutions from the lot and to advise the board what will work for their unique security situation. The security risk assessment will also grant better budget planning. Security costs will be stabilised and can be spread out in phases over time. It is also not uncommon for the board to increase the initial security budget. This is because they now understand the risk. They will see why certain measures, upgrades, and installations are needed.

Experience has also shown that the good, professional security companies that you actually need do not always compete in the tender process. More often than not you are sitting with a handful of small companies that are not always able to provide a good service or handle a big contract. The assessor can approach the best companies on behalf of the governing body and invite them to tender for the project. As part of the assessment, the independent consultant would have already conferred with those offering the best solutions. He will thus be able to indicate to the board who the cream of the crop is.

The second method is to ask all tender applicants to hand in their own security risk assessment report with their applications. This will allow the board to see how the solutions were derived and if all the risk will effectively be addressed. It will show that the security company has done its homework and that the recommendations are not just founded on guesswork. This second method may be the better solution.

For more information contact Alwinco, +27 (0)62 341 3419, andre@alwinco.co.za, www.alwinco.co.za
High performance team connectivity

WAVE 7000 provides a high-reliability broadband push-to-talk solution.

Responding to the increasing demand for reliable, nationwide, push-to-talk networks, Motorola Solutions has introduced WAVE 7000 that offers high-performance PTT across broadband and land mobile radio networks to keep teams more connected than ever. The solution is now available globally.

With public safety agencies increasingly reliant on smart devices and data, many countries are looking to set up nationwide broadband PTT networks to augment their communications networks. Until now, the challenge has been creating those networks while maintaining interoperability with fully established networks such as LMR. WAVE 7000 combines Motorola Solutions’ best-in-class LMR integration with a high-performance PTT solution that supports millions of users.

LTE service providers can also use WAVE 7000 to provide a new service to their current customers, unlock new customer bases and increase their revenue by providing subscribers with high-performance PTT.

"Many of our customers expect that their networks over the next 20 years will be comprised of a combination of LMR and LTE systems," said Jeff Spaeth, vice president of Systems and Software Enablement at Motorola Solutions. "With WAVE 7000, customers are provided a unified experience across LMR and LTE that will keep teams connected no matter the network."

WAVE 7000 is the latest release of a wider portfolio that enables groups using any combination of smartphones, radios or other devices to communicate seamlessly. The WAVE 7000 also has high-performance features:

• Network-level priority and pre-emption that ensure high-priority PTT calls get through even when an LTE network gets congested, which is critical for public safety customers.
• Emergency calls, ambient listening and hardware-based encryption, along with other features custom designed for public safety users.
• A roadmap to meet 3GPP Release 13 standards called “Mission-Critical PTT”.
• Combined with Motorola Solutions’ Convergence Suite, unified PTT, mapping, messaging and other functions across LMR and LTE.
• Support for hundreds of thousands of users on a single server and millions with server clustering.
• Unsurpassed availability through local and geo redundancy options.
• Flexible PTT call types including emergency, broadcast, group and private calls.

With the increasing mobility in teams and need for constant connectivity, push-to-talk communications are more important than ever. Many customers look to leverage both LMR and LTE for enhanced coverage, reliability and flexibility. WAVE 7000 provides a clear solution, with unified, secure PTT so users can communicate across any network on any device.

For more information contact Susanne Stier, Motorola Solutions, +49 172 616 1773, susanne.stier@motorolasolutions.com
Data security is at the heart of PoPI
How best to prepare for PoPI.

As the implementation of the Protection of Personal Information Act (PoPI) gradually comes closer, South African organisations are wondering how best to prepare for it. The key is to understand that data security lies at the heart of PoPI compliance, argues Godfrey Kutumela, head of Security & Cyber Crimes Prevention Unit at IndigoCube.

“Personal information is part of the organisation’s total data set, so any strategy to become PoPI-compliant has to begin and end with how you manage and use data as part of your business operations. And because virtually every organisation is moving to digitise all its data assets, data confidentiality and integrity are at the heart of any data privacy and protection management process,” he says. “Once you understand this, it becomes much easier to scope, design and execute a data protection strategy that the regulator will deem reasonable.”

By way of background, Kutumela explains that while PoPI has been signed into law, full implementation has been delayed pending the approval of a regulator. Candidates for the post were shortlisted in April 2016, a major milestone on the road towards full implementation. PoPI does not stipulate how organisations should protect and manage the personal data in their possession; rather, it requires that “appropriate, reasonable, technical and organisational measures” are taken.

“We are breaking new ground here, and it will take some time before there is a body of administrative decisions by the regulator that will give greater certainty,” he says. “In the meanwhile, there are three logical steps that organisations can take to demonstrate they have sought to apply the law.”

Kutumela’s three steps to PoPI compliance are:
• Identify personal data that is collected, stored or processed in your organisation. To accomplish this, it will be necessary to conduct an enterprise-wide exercise to determine the privacy risk the organisation faces. There is simply too much data to protect it all, so it’s vital to know where the personal data covered by PoPI is, with the guiding principle being the business strategy. Those applications and data stores that directly enable strategic goals should receive the highest priority.
• Control access to personal data using a risk-based identity model. Kutumela strongly argues that identity management and access control are the cornerstones of any security system. When it comes to protecting personal data within the spirit of the Act, they are vital. “Not only must personal information be protected from cyber-criminals, it must also be used appropriately, in line with the purpose for which it was collected. That means it should only be accessed by employees or apps for the purpose for which it was collected.” The challenge here is that digital business models depend on data sharing, so access decisions need to be dynamic, and based on a clearly defined set of risk factors.
• Protect personal data, whether structured or unstructured, adequately while it is at rest. The most effective way to protect personal data—or any data—is where it is stored, in the database. When it is being used, it is dispersed and does not present a target; as a result, attempts to hack data target data repositories. “Data repositories are where the crown jewels are kept, and they should be the focus of security efforts,” Kutumela says.

For more information contact Godfrey Kutumela, IndigoCube, +27 (0)11 759 5950, godfrey@indigocube.co.za

Slimmest single wing access gate
Boon Edam International has announced the launch of the Winglock Swing, an elegant new single wing access gate. This gate is specifically designed to either coordinate with the contemporary Speedlane Lifeline series (as an additional specialised lane) or be used as a stand-alone single installation.

The Winglock Swing offers the user an effortless passageway with carefully thought-out, intuitive LED lights to guide even the most inexperienced visitor through to their destination. A combination of green, orange and red colours displaying static, pulsing and flashing signals effectively guides traffic through without any delays. Just 9 W of energy is used in standby mode and 20 W while in motion, a huge accomplishment considering the industry standard is an average of 200 W.

A new and substantial floor plate design alleviates the need for an additional supporting side post, which notably simplifies installation into the flooring. The gate comes standard in brushed stainless steel, but also has the option for a wide range of finishes or colours.

Visit www.boonedam.us/winglock-swing to learn more about the Winglock Swing and BoonTouch interface security authorisation options.

For more information contact Michelle Wortel, Boon Edam International, +31 299 38 08 00, michelle.wortel@boonedam.com
VIVOTEK announced the launch of its anti-ligature fisheye network camera, the CC8370-HV. This compact 3-megapixel camera features an anti-grip design, WDR Pro and vandal resistant housing which simultaneously ensures the safety of detainees and the efficiency of staff on duty. The CC8370-HV is specially designed for high security environments, such as detention houses, holding cells, psychiatric wards and correctional institutions.

With anti-ligature edges, the camera can act as a life saver by preventing both self-harm and conflict. Featuring 180° horizontal panoramic views with an adjustable 25° tilt angle, the CC8370-HV allows security officers to see any event in cells, with zero blind spots. Sound within a 5 metre radius can also be clearly recorded.

In addition, the CC8370-HV is armed with a robust IP66-rated and IK10-rated housing, to enable the camera’s body to withstand water and dust and to protect against vandalism or tampering. To ensure the 24/7 surveillance, it equipped with WDR Pro, which captures both the dark and bright areas of an image and combines the differences to create a highly realistic representation of the original scene.

Furthermore, with the SNV (Supreme Night Visibility) technology, the CC8370-HV is empowered to provide high quality images under low-light conditions. This superior visibility at night time further enables the CC8370-HV to eliminate unexpected and unwanted incidents.

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

**New generation of starlight cameras**

Starting in June 2016, the Bosch starlight portfolio included improved light sensitivity at 0.00825 lux in colour and 0.00275 lux in monochrome at 1080p resolution. What’s more, video analytics will now be standard in starlight cameras, enabling customers to choose the relevant data for their applications.

A full suite of Essential Video Analytics will be provided on the DINION IP starlight 6000 fixed box and FLEXIDOME IP starlight 6000 fixed dome cameras. And for mission-critical applications, the DINION IP starlight 7000 and FLEXIDOME IP starlight 7000 cameras will come equipped with the latest intelligent video analytics software.

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

**External bypass switches**

The ComNet CN-OB(M,S) external bypass switches for 100M/1G/10G fibre optic networks protect the network from failures and ensure network integrity during power loss. Each of these fibre optical bypass switches includes network ports and monitor ports. The network ports are used for connection to main-network connections and provide protection mechanism, and the monitor ports are used for a down-link local networking device. When the power is on, the operation mode of the bypass switch is set to normal, and the local networking device is connected with the main-network. When power failure occurs, the bypass switch is swiftly set to bypass mode to isolate the main-network from the local networking device.

- Supports 100M/1G/10G fibre optic networks.
- Auto bypass function during power failure.
- Bypass switching time < 10 ms.
- 2 port duplex or 4 port simplex fibre connection.
- Switch protection for network and monitor ports.
- Keeps traffic flowing without impacting the network.

For more information contact ComNet Europe, +44 113 307 6400, ymamoniat@comnet.net, www.comnet.net

**Tyco introduces RAID storage system**

Tyco Security Products has released a new version of the RAID storage system for VideoEdge network video recorders, which include enhancements in the NVR’s archived storage and improved battery back-up capabilities to significantly decrease system downtime.

The new RAID storage line of servers from American Dynamics allows users to extend archived storage to any VideoEdge network video recorder (NVR). With redundant power supplies and lockable, hot swapable drives, the RAID storage system provides its users with high reliability to store critical video and audio longer. An additional battery backup module comes with the storage server for additional redundancy. Each system uses RAID 5 to minimise video loss and maximise hard drive dependability. Designed for high performance video surveillance, the American Dynamics RAID supports iSCSI and fibre interfaces with quad iSCSI ports and dual fibre ports.

Ideal for mid to large-sized installations or cloud data centres, the RAID storage system provides a cost-effective, reliable storage solution optimised for video surveillance. Available in five different configurations including an 18, 36 and 48 terabyte system with a single RAID array and a 90 terabyte system with dual RAID arrays, users can extend their storage without the need for an additional recorder. For future expansion, users can add up to six additional expansion shelves and be scalable up to 112 hard drives with 672 terabytes of total storage. Each system comes with a three-year warranty.

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

**4-megapixel IR camera**

The WiseNet QNO-7080R is a 4-megapixel IR LED camera which uses Samsung’s WiseNet2 DSP chipset. It features a 2.8 ~ 12 mm motorised varifocal lens and smart compression function to save installation time and bandwidth by capturing greater details only for the regions of interest. Its built-in 32 IR LEDs provides the ability to capture clear images of objects which are up to 30 m from the camera, even when the area is in total darkness, and the IP66 rated waterproof function shows that the camera can be an effective choice for demanding environments.

It supports motion detection, tampering and defocus detection, as well as a micro SD (128 GB) memory slot and PoE.

For more information contact MIA Telecoms, +27 (0)11 799 7720, stephan@mia.co.za, www.mia.co.za
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alwinco</td>
<td>+27 (0)62 341 3419</td>
<td><a href="mailto:andre@alwinco.co.za">andre@alwinco.co.za</a></td>
<td><a href="http://www.alwinco.co.za">www.alwinco.co.za</a></td>
<td>60</td>
</tr>
<tr>
<td>ASSA ABLOY SA</td>
<td>+27 (0)11 761 5000</td>
<td><a href="mailto:stacey.burmeister@assaabloy.com">stacey.burmeister@assaabloy.com</a></td>
<td><a href="http://www.assaabloy.com">www.assaabloy.com</a></td>
<td>36</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>7,26,27,51*</td>
</tr>
<tr>
<td>Boon Edam International</td>
<td>+31 299 38 08 00</td>
<td><a href="mailto:Michelle.wortel@boonedam.com">Michelle.wortel@boonedam.com</a></td>
<td></td>
<td>62</td>
</tr>
<tr>
<td>Bosch Security Systems</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://www.boschsecurity.com">www.boschsecurity.com</a></td>
<td>5*,30,31,64</td>
</tr>
<tr>
<td>CAMPROSA</td>
<td></td>
<td></td>
<td><a href="http://www.camprosa.co.za">www.camprosa.co.za</a></td>
<td>59*</td>
</tr>
<tr>
<td>ComNet Europe</td>
<td>+44 113 307 6400</td>
<td><a href="mailto:ymamoniat@comnet.net">ymamoniat@comnet.net</a></td>
<td><a href="http://www.comnet.net">www.comnet.net</a></td>
<td>64</td>
</tr>
<tr>
<td>Dahua Technology</td>
<td>+86 571 8768 8883</td>
<td><a href="mailto:overseas@dahuaitech.com">overseas@dahuaitech.com</a></td>
<td><a href="http://www.dahuasecurity.com">www.dahuasecurity.com</a></td>
<td>OFF*,3,14</td>
</tr>
<tr>
<td>Dallmeier Southern Africa Office</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>28,29</td>
</tr>
<tr>
<td>Eavesdropping Detection</td>
<td>+27 (0)12 665 2109</td>
<td><a href="mailto:info@tscm-za.com">info@tscm-za.com</a></td>
<td><a href="http://www.tscm-za.com">www.tscm-za.com</a></td>
<td>55*</td>
</tr>
<tr>
<td>Solutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Security Distributors' Association</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elvey Security Technologies</td>
<td>+27 (0)11 401 6700</td>
<td><a href="mailto:info@elvey.co.za">info@elvey.co.za</a></td>
<td><a href="http://www.elvey.co.za">www.elvey.co.za</a></td>
<td>7*,12,44,53*</td>
</tr>
<tr>
<td>Gianni Industries Inc.</td>
<td>+886 2 2267 7986</td>
<td><a href="mailto:inquiry1@gianni.com.tw">inquiry1@gianni.com.tw</a></td>
<td><a href="http://www.gianni.com.tw">www.gianni.com.tw</a></td>
<td>31*,36</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>26,27,52</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*,8,26,27</td>
</tr>
<tr>
<td>Hi-Tech Security Solutions</td>
<td>+27 (0)11 543 5800</td>
<td><a href="mailto:melissa@technews.co.za">melissa@technews.co.za</a></td>
<td><a href="http://www.technews.co.za">www.technews.co.za</a></td>
<td>61*</td>
</tr>
<tr>
<td>Honeywell Building Solutions</td>
<td>+27 (0)11 695 8000</td>
<td>honeywellbuilding <a href="mailto:solutions@www.honeywell.com">solutions@www.honeywell.com</a></td>
<td><a href="http://www.honeywellbuildingsolutions.com">www.honeywellbuildingsolutions.com</a></td>
<td></td>
</tr>
<tr>
<td>IHS Technology</td>
<td>+44 1933 408 075</td>
<td><a href="mailto:jon.cropley@ihs.com">jon.cropley@ihs.com</a></td>
<td><a href="http://www.ihs.com">www.ihs.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Impro Technologies</td>
<td>+27 (0)31 717 0700</td>
<td><a href="mailto:vikki@impro.net">vikki@impro.net</a></td>
<td><a href="http://www.impro.net">www.impro.net</a></td>
<td>40,0BC*</td>
</tr>
<tr>
<td>IndigoCube</td>
<td>+27 (0)11 759 5950</td>
<td><a href="mailto:godfrey@indigocube.co.za">godfrey@indigocube.co.za</a></td>
<td><a href="http://www.indigocube.co.za">www.indigocube.co.za</a></td>
<td>62</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>42,57*</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>15,55*</td>
</tr>
<tr>
<td>Matrix</td>
<td>+91 812 869 0106</td>
<td><a href="mailto:abhayjoshi@matrixcomsec.com">abhayjoshi@matrixcomsec.com</a></td>
<td><a href="http://www.matrixsecurcom">www.matrixsecurcom</a></td>
<td>53</td>
</tr>
<tr>
<td>MIA Telecoms</td>
<td>+27 (0)11 799 7720</td>
<td><a href="mailto:stephan@mia.co.za">stephan@mia.co.za</a></td>
<td><a href="http://www.mia.co.za">www.mia.co.za</a></td>
<td>10,64</td>
</tr>
<tr>
<td>Milestone Systems</td>
<td>+27 (0)82 377 0415</td>
<td><a href="mailto:arms@milestonesys.com">arms@milestonesys.com</a></td>
<td><a href="http://www.milestonesys.com">www.milestonesys.com</a></td>
<td>32,63</td>
</tr>
<tr>
<td>MiRO distribution</td>
<td>086 123 MIRO (6476)</td>
<td><a href="mailto:lerize@miro.co.za">lerize@miro.co.za</a></td>
<td><a href="http://www.miro.co.za">www.miro.co.za</a></td>
<td>8,38</td>
</tr>
<tr>
<td>Morpho SA</td>
<td>+27 (0)11 286 5800</td>
<td><a href="mailto:sec.san.orders@morpho.com">sec.san.orders@morpho.com</a></td>
<td><a href="http://www.morpho.com">www.morpho.com</a></td>
<td>23*</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>9*</td>
</tr>
<tr>
<td>Motorola Solutions</td>
<td>+49 172 616 1773</td>
<td><a href="mailto:susanne.stier@motorolasolutions.com">susanne.stier@motorolasolutions.com</a></td>
<td></td>
<td>61</td>
</tr>
<tr>
<td>neaMetrics</td>
<td>0861 632 638</td>
<td><a href="mailto:info@neametrics.com">info@neametrics.com</a></td>
<td><a href="http://www.neametrics.com">www.neametrics.com</a></td>
<td>21*</td>
</tr>
<tr>
<td>Powell Tronics</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>54</td>
</tr>
<tr>
<td>Progroup Manufacturing</td>
<td>+27 (0)11 493 1545</td>
<td><a href="mailto:sales@progroup.co.za">sales@progroup.co.za</a></td>
<td><a href="http://www.progroup.co.za">www.progroup.co.za</a></td>
<td>36*</td>
</tr>
<tr>
<td>PSA Africa</td>
<td>0860 543 356</td>
<td><a href="mailto:enquiries@psafrica.co.za">enquiries@psafrica.co.za</a></td>
<td><a href="http://www.psafrica.co.za">www.psafrica.co.za</a></td>
<td>35*</td>
</tr>
<tr>
<td>Radwin</td>
<td>+27 (0)11 452 1471</td>
<td><a href="mailto:salesa@radwin.com">salesa@radwin.com</a></td>
<td><a href="http://www.radwin.com">www.radwin.com</a></td>
<td>49*</td>
</tr>
<tr>
<td>RDC</td>
<td>+27 (0)11 534 849</td>
<td><a href="mailto:leean.na@radiodata.co.za">leean.na@radiodata.co.za</a></td>
<td><a href="http://www.radiodata.co.za">www.radiodata.co.za</a></td>
<td>41*,45</td>
</tr>
<tr>
<td>Reditron</td>
<td>+27 (0)87 802 CCTV (2288)</td>
<td><a href="mailto:sales@reditron.co.za">sales@reditron.co.za</a></td>
<td><a href="http://www.reditron.co.za">www.reditron.co.za</a></td>
<td>11,45*</td>
</tr>
<tr>
<td>Regal Distributors</td>
<td>+27 (0)11 553 3300</td>
<td><a href="mailto:info@regalsecure.co.za">info@regalsecure.co.za</a></td>
<td><a href="http://www.regalsecure.co.za">www.regalsecure.co.za</a></td>
<td>37*,39*,50</td>
</tr>
<tr>
<td>SALTO Systems</td>
<td>+27 (0)11 534 849</td>
<td><a href="mailto:w.dutoit@saltosystems.com">w.dutoit@saltosystems.com</a></td>
<td><a href="http://www.saltosystems.com">www.saltosystems.com</a></td>
<td>63</td>
</tr>
<tr>
<td>Security &amp; Communication Warehouse</td>
<td>+27 (0)12 653 1005</td>
<td><a href="mailto:marketing@securitywarehouse.co.za">marketing@securitywarehouse.co.za</a></td>
<td><a href="http://www.securitywarehouse.co.za">www.securitywarehouse.co.za</a></td>
<td>37</td>
</tr>
<tr>
<td>Specialised Exhibitions</td>
<td>+27 (0)10 003 3060</td>
<td><a href="mailto:leighm@specialised.com">leighm@specialised.com</a></td>
<td><a href="http://www.electraining.co.za">www.electraining.co.za</a></td>
<td>13*</td>
</tr>
<tr>
<td>Sunell SA</td>
<td>+27 (0)11 469 3598</td>
<td><a href="mailto:sales@sunellsecurity.com">sales@sunellsecurity.com</a></td>
<td><a href="http://www.sunellsecurity.com">www.sunellsecurity.com</a></td>
<td>6,33*</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>8,21*,38</td>
</tr>
<tr>
<td>Transported Asset Protection</td>
<td>083 463 2047</td>
<td><a href="mailto:andre.duvenage@securelogistics.co.za">andre.duvenage@securelogistics.co.za</a></td>
<td></td>
<td>4*</td>
</tr>
<tr>
<td>Association</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tyco Security Products</td>
<td>+27 (0)82 566 5274</td>
<td><a href="mailto:emallett@tycoint.com">emallett@tycoint.com</a></td>
<td><a href="http://www.tycosecurityproducts.com">www.tycosecurityproducts.com</a></td>
<td>37,51,53,57,64</td>
</tr>
<tr>
<td>Verifier</td>
<td>086 111 6023</td>
<td><a href="mailto:info@verifier.co.za">info@verifier.co.za</a></td>
<td><a href="http://www.verifier.co.za">www.verifier.co.za</a></td>
<td>16</td>
</tr>
<tr>
<td>VIVOTEK Inc.</td>
<td>+886 2 8245 5282</td>
<td><a href="mailto:pr@vivotek.com">pr@vivotek.com</a></td>
<td><a href="http://www.vivotek.com">www.vivotek.com</a></td>
<td>63</td>
</tr>
</tbody>
</table>

* Denotes advertiser

For more information on these and other suppliers please see www.hsbd.co.za
The future of access
CONTROL

Simple, scalable and suitable for any
SITE

Access Portal brings a world of simplicity to your access control solutions. Simple to install and easy to use, Access Portal puts the power back in your hands with intuitive design, powerful functionality and seamless integration with critical resources such as CCTV, Intrusion systems, T&A and more.

Scalability has also never been easier with Access Portal. Whether you have a small business, or are a global multi-national, the system scales quickly and easily with your growing needs. No redundancy, no hassle!

To find out more, or to request a demo, email us on info@impro.net

www.impro.net