Embrace the adoption of AI
Artificial Neural Network Inside Everything
Hikvision DarkFighterX Using Dual-Sensor Imaging to Provide Full Colour Images

Hikvision has taken its DarkFighter technology up to the next level with the DarkFighterX Series PTZ and Bullet Cameras. Using single-lens, dual-sensor technology, each full HD DarkFighterX Camera mimics human eyes to render bright, full-colour images. How? By fusing two discrete light spectra: an IR sensor captures brightness, and a visible light sensor captures colour – even under 0.001 lux.

Install Hikvision’s DarkFighterX in city streets, public spaces, and critical travel nodes for the most critical protection. In colour – all day, all night.
Exploring New Depths in Oceans of Data

**Hikvision Deep Learning solution**

Deep Learning is the next step in AI. Deep Learning incorporates unsupervised or "self-learning" principles, transcending Machine Learning where classifications and patterns are still manually set into algorithms. Hikvision’s own analytics algorithms continually push Deep Learning’s development, ever enhancing its accuracy via multi-layer learning and extensive data collection. Performance in applications such as facial, vehicle, and human recognition, as well as other applications, will significantly advance as Deep Learning evolves. And Hikvision will be right there with it.
The potential for interaction and integration of a large number of things was a theme of the iLegal conference recently … one would think that all these security systems would be able to keep time.

Controlling borders is a critical task for governments the world over, both at official and unofficial entry points.

Smart cities are built on smart thinking. The smartest opening move is to create a safe environment.

SA organisations must factor natural disaster into business continuity planning.

X-ray technology is widely and safely used in commercial settings.

From the editor’s desk
Calendar
Training & education
News & events
System integrators’ profiles
Access control & identity management
Fire & safety
CCTV, surveillance & remote monitoring
IT infrastructure in security
Cybersecurity
Product news
Smart City Safe Living

“How can cities coordinate quicker and more effective emergency responses without dramatically expanding police forces?”

During the 2016 G20 Summit, Dahua Safe City Solution automatically detected 29823 vehicles behaving illegally, greatly reducing the burden on police forces, allowing them to focus on protecting key Summit areas.
Identity theft R us

There are some people in South Africa thanking whoever they see fit to thank that the government has bumbled to implementation of the PoPI Act for so long. You will have heard about the clever people who exposed personal information, including ID numbers and more of over 30 million South Africans. If PoPI was in effect (and, of course, if it was enforced) these clowns could have been facing millions in fines and perhaps even jail time.

Fortunately for them, cybersecurity at a national level can best be described as “leaves a lot to be desired”. But let’s not point fingers at the government, perhaps we should be asking how anyone with an ounce of common sense would leave such sensitive information at the mercy of criminals? Were they stupid? Were they careless? Were they naive? Were they just so greedy to make a buck off this information they got from somewhere that they couldn’t be bothered to secure it?

The “IT people” are probably going to get the blame for his/her/their incompetence, and rightly so. But how can a director of a company in this day and age not pay any attention to ensuring sensitive information is secure? The information stolen could be used for a number of criminal acts in your name, and my name.

Perhaps it’s just a case of not caring because they know there is not much that can be done in terms of legal action against them – unless some class action complaint is initiated (but what’s the chance of that)?

The only relevant question now is: what can each of us do to try to protect ourselves in light of this criminal act?

Access & Identity Management Handbook 2018

On a lighter note, the Access & Identity Management Handbook has just been published with over 100 pages of information about access control and identity management in these troubled times. Ironically, one of the focus areas of the handbook is trust. How do you determine the level of trust to assign to various identities? It also includes information on the latest technologies and trends in this market, as well as insight from a variety of access and identity experts. (Cybersecurity also gets a mention.) If you don’t get your copy in the mail, contact vivienne@technews.co.za and one will be dispatched post haste.

2018 is almost here

Finally, the Hi-Tech Security Solutions team would like to wish all our readers a safe and enjoyable holiday season. May 2018 be a year of miracles and the emergence of some political common sense.
Enter the world of Augmented Identity

OT-Morpho is now IDEMIA
augmented identity

https://www.idemia.com/  •  +27 (0)11 286 5800
EXHIBITIONS, CONFERENCES, SPECIALISED EVENTS

**Events**

**Securexpo East Africa (Date changed)**
31 January – 2 February 2018
Visa Oshwal Centre, Nairobi, Kenya
Securexpo is the largest commercial and homeland security and fire exhibition and conference in East Africa. It is the leading event in the region with hundreds of different security products on display. The 2016 event saw 2045 unique attendees and over 70 exhibiting companies. The exhibition will also be comprised of a co-located, free-to-attend conference where expert representatives from key institutions and businesses will lead compelling sessions across the three days. The programme for the conference will be announced in December 2017. For more information, go to www.securexpoeastfrica.com.

**Internet of Things Forum Africa 2018**
14 and 15 March 2018
Gallagher Convention Centre, Johannesburg
The IoT Forum Africa 2018 will tackle transformational IoT trends and explore the benefits of IoT in different industries. The conference will host over 500 delegates and 30 speakers on 14 and 15 March 2018, at the Gallagher Convention Centre in Johannesburg, South Africa. For more information visit http://iotforumafrika.com.

**Securex 2018**
22 – 24 May 2018
Gallagher Convention Centre
Securex South Africa 2017 was a great success. The feedback received from exhibitors was extremely positive. The show attracted a high quality audience with thousands of visitors attending over the three days. By the end of day two, exhibitors had already booked their stand for the 2018 show. For more information, go to www.securex.co.za.

**CAMPROSA 2018**
16 – 19 September 2018
SPIER Wine Farm, Stellenbosch
The Campus Protection Society of Southern Africa is set to host its 2018 international conference at the SPIER Wine Farm near Stellenbosch in the Western Cape. For more information on the full programme, go to www.camprosa.co.za.

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

**Axis Communications SA**

**Network Video Fundamentals**
16 – 17 January 2018
Cape Town, Western Cape

Network Video Fundamentals is a comprehensive course covering the essentials of network video. Topics such as basic camera installation, image usability, bit rate optimisation and video analytics are explored in theory lessons combined with hands-on labs.

Terri Miller, +27 (0)11 548 6791
terri.miller@axis.com

---

**Gold N’ Links Cyber**

**Executive Cyber Crisis Management Training**

**Cyber Security Awareness Training**

Various course dates. Courses delivered at client’s premises or at GNL Cyber premises in Johannesburg, Gauteng.

Dr Graham Wright
+27 (0)83 252 5727
grahamw@gnlcyber.com
www.gnlcyber.com

---

**SAIDSA**

**SAIDSA Competent Technician**

**SAIDSA Technical Certificate Courses (5 days)**

**Technical Sales Course (1 day)**

Various course dates. All courses in Johannesburg, Gauteng.

Cheryl Ogle
+27 (0)11 845 4870
saidsa@mweb.co.za
www.saidsa.co.za

---

**Eavesdropping Detection Solutions (EDS)**

**Basic Course in Technical Surveillance Countermeasures and Cyber TSCM:** 22 January – 2 February 2018, Centurion, Gauteng

**Oscor Blue/Green Spectrum Analyser Operator Course:** 26 February – 2 March 2018, Centurion, Gauteng

**Talan 3 Telephone and Line Analyser Operator Course for TSCM:** 5 – 9 March 2018, Centurion, Gauteng

Steve Whitehead, +27 (0)12 665 2109
training@tscm-za.com
www.tscm-za.com/training.html

---

**Leaderware**

**CCTV Behavioural Analysis and Incident Detection**

**Advanced CCTV Surveillance Body Language**

**CCTV Surveillance Skills and Body Language**

All courses provided in-company.

Dr Craig Donald
+27 (0)11 787 7811
sales@leaderware.com
www.leaderware.com

---

**ZKTeco South Africa**

**ZKBiosecurity Advanced**

**ZKBioSecurity Basic**

**ZKAccess 3.5**

Various course dates. All courses in Hartbeespoort, North West.

Marichen Cronje
+27 (0)12 259 1047
support@zkteco.co.za
www.zkteco.co.za

---

**Hi-Tech Security Solutions 3-in-1 training package**

For only **R4 500 excl. VAT** get your training message to:

- **5 500** readers through the listing in the print edition
- **6 022** recipients of the training news brief
- The HSS website has an average of **20 500** visits per month

Contact Vivienne on +27 (0)11 543 5800 or vivienne@technews.co.za
G4S one of the top employers in Africa 2018

For the sixth consecutive year, G4S has been certified by the Top Employer Institute as a Top Employer Africa 2018, solidifying the company’s commitment to be a responsible and sustainable employer that empowers and develops its employees to contribute towards G4S’s overall achievements.

G4S is the only private security company in Africa that has ever been awarded Top Employer certification. This is a remarkable triumph, particularly as the company has been awarded 9 certifications in 2013, 11 certifications in 2014 and 2015, 13 certifications in 2016, 2017 and now again in 2018. Independent research by the Top Employers Institute shows the company looks after its people exceptionally well, offering employees an engaging and safe working environment where their contributions are valued.

The Top Employers endorsement recognises top employers through a stringent certification process evaluating internal HR policies and procedures and is awarded to companies that achieve the highest standards of excellence in employee conditions. The annual international research, undertaken by the Top Employers Institute, acknowledges leading employers around the world.

Only organisations that achieve certification in at least five countries within the region deserve the special Top Employers Africa 2018 recognition. G4S has been certified in 13 countries, including Botswana, Cameroon, Côte d'Ivoire, DRC, Ghana, Kenya, Malawi, Mozambique, Namibia, Nigeria, South Africa, Uganda and Zambia – an accolade that makes G4S stand out in the exclusive and internationally renowned community of Top Employers in Africa.

Stanley Blyth, regional HR director, G4S Africa says: “With a staff complement of over 111 000 people in Africa, we are the largest private security employer on the continent. G4S therefore takes great pride in the creativity and diversity of our talented people and strive to create a safe and value-driven environment that provides opportunities for growth, innovation and a sustainable future for all.”

Crucial to the Top Employers process is that participating companies must meet the required high standard in the research in order to achieve the certification. The Top Employers Institute assessed G4S’s people practices on the following criteria: Talent strategy, workforce planning, on-boarding, learning and development, performance management, leadership development, career and succession management, compensation and benefits, and culture. The independent research has verified G4S’s outstanding employee conditions in all certified countries. This earned G4S Africa a coveted spot among a choice group of certified Top Employers.

For more information, contact G4S Africa, +27 (0)82 098 2666, leandi.ferreira@africa.g4s.com.

24/7 acquires SMC

24/7 Security Services has acquired Security Management Consultants (SMC). 24/7’s MD, David de Lima explains that the two companies have a long history of working together on numerous projects in the residential and education markets. Given 24/7’s focus on service delivery and the positive feedback SMC has received from clients over the years, the companies decided that joining forces was the best way forward.

The acquisition will see 24/7 establishing a new division focusing on estates and schools, which SMC’s Brian Sharkey will head. While there are many companies serving these markets, markets that are steadily growing, few of them are able to offer a holistic solution along with the drive to manage them effectively.

SMC’s operations manager, Marinda Hartenberg, will join 24/7 as operations manager to ensure the smooth running of the company’s security solutions.

With the addition of SMC’s skills and experience, De Lima says 24/7 will now be able to offer enhanced services to the estate and school markets. This will include everything from risk assessments through to integrated technology installations, and the management and running of the security operation.

While growth through acquisition is not a focus of 24/7, De Lima says if opportunities to expand the company’s market do arise, he would consider them.

The merger is already in effect and the combined companies have hit the ground running.
SABRIC encourages consumers to protect their personal information by sharing it very selectively and on a need to know basis only. Personal information includes identity documents, driver's licences, passports, addresses and contact details amongst others. In addition, confidential information, which includes usernames, password and PIN numbers should never be shared with anybody.

In order to participate in commercial activity, it has become necessary to identify yourself by providing personal information. Good identity management practices can assist in mitigating the risk of impersonation should the information be compromised.

As some personal information such as your identity number cannot be changed readily, and other personal information such as your home and work addresses are impractical to change, we recommend that you consider the following precautionary measures when you are required to provide personal information for security verification purposes:

- Do not use the information that may have been compromised. Rather use other personal information that you have not used previously in order to confirm your identity in future.
- Register a new email account.
- Implement dual authentication for all accounts and products, especially for financial services products.
- Register for SMS notifications to alert you when products and accounts are accessed.
- Conduct regular credit checks to verify whether someone has applied for credit using your personal information and if so, advise the credit grantor immediately.
- Investigate and register for credit related alerts offered by credit bureaux.
- Check your bank statements regularly.

“Whilst the compromise of personal information creates opportunities for criminals to impersonate you, it does not guarantee access to your banking profile or accounts,” says Kalyani Pillay, CEO of SABRIC. “However, the importance of never sharing confidential information in order to protect yourself cannot be overemphasised.”

**Some do’s**

- Use strong passwords for all your accounts.
- Change your password regularly and never share them with anyone else.
- Store personal and financial documentation safely. Always lock it away.
- Keep PIN numbers and passwords confidential.
- Verify all requests for personal information and only provide it when there is a legitimate reason to do so.
- To prevent your ID being used to commit fraud if it is ever lost or stolen, alert the SA Fraud Prevention Service immediately on 0860 101 248 or at www.safps.org.za.
- Ensure that you have a robust firewall and install antivirus software to prevent a computer virus sending out personal information from your computer.
- When destroying personal information, either shred or burn it (do not tear or put it in a garbage or recycling bag).
- Should your ID or driver's licence be stolen, report it to SAPS immediately.

For more information go to www.sabric.co.za.

---

**SOLID webKey is simple security**

Digital technology solutions provider Ansys Limited has announced the launch of its all-in-one online password vault and security authentication product, the SOLID webKey.

Thanks to its patented password protection technology, SOLID webKey can generate and store long, unique passwords for every site you visit, giving owners the best security while only having to remember one master password themselves.

Developed and designed in South Africa at Ansys' design and manufacturing facility, SOLID webKey helps Internet users to follow global best practices for protecting online accounts, in a simple-to-use but highly secure manner.

With SOLID webKey, you can generate passwords that comply with any policy using the maximum length accepted by the application, without having to remember it.

**How does it work?**

SOLID webKey helps to protect online accounts in two critical ways. As a portable password vault, it enables web users to create long, unique passwords for every service that they regularly sign into, which are stored in an encrypted database which in turn can only be accessed with a single master password.

Passwords are stored on Flash memory on-board the physical SOLID webKey device, which can be plugged into a USB port on any PC. Once plugged in, the SOLID webKey synchronises with the SOLID KeyPass software, which is derived from the industry-standard open source KeePass Password Safe, for access.

The product also has a unique and patented “liveliness” test as a second line of defence against loss of data, which requires a physical tap of the device before passwords can be accessed. This guards against the threat of malware which could steal passwords from the database after they have been decrypted.

Even strong passwords aren’t enough to defend against committed attackers, however, who may gain access to login credentials via phishing or other attacks.

To protect against this kind of threat, SOLID webKey’s second core feature is that it can also act as a hardware token for two-factor authentication (2FA), and is compatible with the Universal Two-Factor (U2F) standard promoted by the FIDO Alliance.

U2F is supported by popular service providers such as Google, Facebook and Dropbox. When enabled as an account setting, users will only be able to log in to these services when the SOLID webKey is physically present and the device is tapped by the user.
Physical and cyber defence centre

XON and NEC Africa launched their joint Cyber Defence Operation Centre (CDOC), the only such facility from a single service provider in Africa that offers end-to-end physical and cyber defence services, with all the underlying IT infrastructure necessary for a turnkey solution.

The key difference between this and other similar operations is the bridged physical and cybersecurity services combined into a single service, focused on safety and security for organisations ranging from state entities to individual commercial operations.

“The service we provide from our purpose-built facility in Midrand, ensures people are safe and secure in a world beset by many difficult issues,” says Vernon Fryer, who heads up NEC Africa’s African cyber business and CDOC.

NEC collaborates closely with Interpol and various other global organisations in the fight to secure the safety and wellbeing of citizens in many countries. NEC has established several cyber defence and operations centres around the globe to assist in that ongoing cause.

XON and NEC Africa’s centre differs markedly in that it provides that same world class service in Africa, from Africa, and also integrates the dependable solutions and services of XON’s enterprise-class systems integration business for the complete solution.

“Our customers get the full range of services and solutions from creating data centres to field infrastructure and services, even including alternative energy, and the networks that connect everything,” says Bertus Marais, GM of public safety and security at XON. “The CDOC unites the worlds of physical and cybersecurity and include analytics and biometrics systems. The individual services are too numerous to mention but range from access and perimeter control and surveillance to fingerprinting, iris recognition, to big data analytics to provide facial recognition at scale, crowds in public areas behaviour monitoring and control, and then the increasingly crucial cybersecurity technologies and services.”

Africa, like other parts of the world, faces several challenges from terrorism to political instability, crime, and other socio-economic-related trials.

The City of Cape Town’s recent three-phase disaster plan outlines the deployment of army and police personnel to issue rationed water in the severest scenario. The CDOC from XON and NEC Africa could provide surveillance, monitor the situation, manage the emergency resources, and facilitate a smooth and successful water distribution process. To do so it would tap into social media channels, even limited by geography, monitor conversations, establish tone of discussions among citizens for any imminent threats to public safety, combine visual and other surveillance from several sources, overlay emergency resources, and provide emergency control personnel options for dealing with several potential scenarios.

The same technology can be used elsewhere in Africa to monitor and manage terrorism threats, including scanning tens of thousands of faces at ports, facilitate electoral security, counter narcotics and other smuggling, help the fight against human trafficking, monitor and manage natural resources, key infrastructure, and much more.

“The CDOC centre is a specialised combination of technologies and skilled personnel who monitor cyber situations 24-7 on behalf of clients who don’t have the expertise to do so themselves,” says Fryer. “The reality is that this is a rapidly evolving scenario that few organisations have the resources to effectively mitigate.

“The recent Deloitte hack is still being investigated. Although, they say few customers were affected. In another case, last year November, it emerged that someone used the Mirai botnet to conduct a denial of service (DDoS) attack against Liberia. Much closer to home, an unscrupulous person used Twitter to lure unsuspecting candidates into his fake South African Defence Force enrolment scheme, charging them, and essentially keeping them prisoner at a property in Pretoria. A South African woman was also rescued from a human trafficking syndicate in Malaysia after being lured in by a fake modelling competition online that attracted women from 14 countries.”

“These examples combine the cyber world with the physical world,” says Fryer. “The borders between the two are increasingly blurred as the ramifications span from one to the other and back. The ability to reveal a wealth of personal information, from our physical locations to contacting us, anonymously and tapping our supposedy restricted personal data, means criminals and other nefarious elements have unprecedented power to corrupt and subvert our safety and security. It’s a difficult world for the authorities and emergency responders to navigate as it relies on skills and infrastructure usually foreign to them.”

For more information, contact www.xon.co.za.

Datacentrix achieves Level One B-BBEE status

Datacentrix has achieved certification as a 52.13 percent black-owned Level One Broad-Based Black Economic Empowerment (B-BBEE) Contributor, with 135 percent procurement recognition.

Completed in alignment with the amended ICT Codes gazetted in November last year, the certification was awarded through EmpowerLogic, a SANAS-accredited B-BBEE verification agency.

Datacentrix is also classified as a designated supplier, which will allow anyone purchasing from the company to gain additional 8-BBEE points on their scorecard. The organisation has both a 52.13 percent black ownership as well as a 42.67 percent black female ownership.

 Says Datacentrix CEO, Ahmed Mahomed: “Datacentrix is pleased that the strategies put in place over a number of years have enabled it to reach a Level One status. As part of our commitment to ongoing transformation, we will continue to foster an environment that will deliver substantively on empowerment objectives including skills, socio-economic and enterprise development.”

Bertus Marais, GM of Public Safety and Security at XON.

Ahmed Mahomed.
ACCESS & IDENTITY MANAGEMENT
Handbook 2018

A complete guide to access and identity management trends, technology, services and products

Published by HI-TECH SECURITY SOLUTION

To order your own copy contact Wesley on +27 (0)11 543 5800 or wesley@technews.co.za
More than 250 participants attended the two successful Milestone Open Platform of Days (MPOP) in South Africa recently. The events in Johannesburg and Cape Town brought together some of the most successful networked video systems integrators, resellers and distributors in the region. Participants exchanged information about industry trends and challenges, learned about the many applications of the Milestone Systems network video management software, and explored the solutions that are made possible through their strong partnerships.

The community received a warm welcome by Armand Steffens, country manager Africa. Christian Ringler, director Middle East, Africa & DACH, outlined Milestone’s vision: “We make the world see”, and the objective of being part of every monitoring installation with video technology worldwide. Key to reaching this is the entire Milestone community, from partners and integrators. More than 150 000 video installations have already been implemented worldwide. Since last year, the company has been focusing on its community to learn from each other, to profit from the experience of others and to grow together.

Ringler emphasised that Milestone is increasingly developing into a common platform. This means that the value proposition is no longer only Milestone’s IP video management software, but the ‘best of breed’ solutions that are offered in conjunction with the community partners. In this way, future-oriented market potentials can be recognised and utilised, for example, video management installations in the areas of Internet of Things or artificial intelligence.

Four Gold Solution Partners Axis, Netapp, Vumacam and Promise, gave testimony to the advantages of working together as a community in presentations of their innovative solutions with Milestone Systems. Roy Alves, Axis Communications, commented: “The MPOP event each year facilitates the opportunity for Axis to showcase our partnership collaboration with Milestone, highlighting our joint value proposition. Focused booth style exhibition with presentations and many open discussions with other industry players always make this style of event a huge success.”

**Milestone Systems partner awards**

In order to further emphasise the community idea, Milestone Systems awarded partner awards to thank its strong partners. The winners of the Milestone Community Days

MPOP Africa awards this year were given to:
- Promise technologies: Best Storage Solution,
- Cygnetic: Best partner,
- Camsecure: Best custom development partner,
- Axis Communications: Best MAP,
- Compass Visual Security: Fastest growing distributor,
- Pinnsec: Best distributor, and
- Mark Bense won the Milestone Passion award.

“We are very satisfied with MPOP 2017 in Africa. In addition to 12 solution partners, more than 200 resellers and customers took part. The demand for video management systems is very strong in this region, and we are seeing a particularly keen interest from the education industry,” Armand Steffens, country manager for Milestone Systems Africa concludes.

For more information contact Milestone Systems, +27 (0)82 377 0415, arms@milestonesys.com, www.milestonesys.com.
Cathexis Africa has announced the appointment of Dene Alkema as national sales manager (South Africa) with immediate effect. Alkema joined Cathexis Technologies four years ago as a senior account manager for the Gauteng region, and according to the Cathexis Technologies management team, his commitment and dedication to the company, have been instrumental in the significant growth and development of this region. As part of his new role, Alkema will be responsible for all sales and pre-sales operations for Africa.

Cathexis Technologies is on a growth path with its current expansion into various African markets, through various strategic appointments at its subsidiary, Cathexis Africa. Despite a turbulent economic environment, Cathexis Africa, is still seizing new opportunities in the market. Cathexis has identified several security challenges in the African region, which it believes its IP Video Management Software solution, CathexisVision, can easily address.

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

Sequeira joins Centurion

Centurion recently appointed Emmanuel Sequeira in the role of sliding door specialist. In this newly-created position Sequeira will be responsible for developing and maintaining relationships with prospective clients involved with sliding door automation in its different incarnations. Furthermore, he will be conducting product training at both sales and technical levels.

“I started my career as a salesperson in the information and communications technology industry,” says Sequeira, “assisting clients and organisations meet their voice and data needs. In 2017, after seven years in sales, I took up an opportunity as a product manager for an ICT distribution company where I managed brands and products related to VoIP, FTTx and surveillance.”

Asked what he will be bringing to the team, he responded by saying that he has a passion for sales and client relations, a keen willingness to learn, as well as a dedication to hard work.

For more information contact Centurion Systems, +27 (0)11 699 2400, charl.mijnhardt@centurionsystems.co.za, www.centsys.co.za.

Simply the Best
Access Control Locking Devices

GEM®

GIANNI INDUSTRIES, INC.
E-mail: inquiry1@gianni.com.tw
Website: http://www.gianni.com.tw

Download or Search 「GEM Gianni」

Download on the
App Store

Get it on
Google play
Centurion’s recent successful Access Automation Expo took place on the 21st September at the Galleria conference centre in Kramerville, and boasted exhibits by 10 regional distributors, with in the region of 600 professionals from the field of access automation and its related specialisations attending.

In recent years, access automation has seen myriad technological innovations driving it forward and becoming one of the most exciting fields to exist in the security spectrum, encompassing everything from gate motors and traffic barriers to intercom systems and GSM access control.

While the event undoubtedly acted as a springboard for Centurion’s latest product offerings, the company’s communications coordinator, Charl Mijnhardt, points out that it presented an excellent networking opportunity for professionals involved with access automation and its related fields.

“There’s never really been anything like this in South Africa, an event that focuses solely on access automation,” explains Mijnhardt. “And judging by the incredible turnout, it’s clear that it’s something that the security industry has been waiting for.”

With regards to the new Centurion products on display, Mijnhardt says, “The three new products are all geared towards providing maximum convenience and maximum functionality, both for the installer and for the end-user.” The new products are:

**G-Ultra:** The G-ULTRA is imbued with intelligence and packaged for use in a modern environment. The combination of a smart graphic user interface and a plethora of advanced features means that the G-ULTRA goes well beyond the scope of mere access automation and takes remote monitoring and control to an entirely new level. The G-ULTRA makes it possible for access holders to remotely control up to six appliances – for example a gate motor or irrigation system – via a missed call or SMS from their mobile phone.

In addition, the unit’s four channels can be individually configured as outputs, which enable learned-in users to receive notifications via missed call, SMS or email. “A typical example would be using one of the unit’s inputs to monitor the status of a Centurion gate motor, and setting it up to send you a notification when the gate is open, or opening, or both,” says Mijnhardt. “The possibilities are virtually endless.”

**G-Speak Ultra:** The G-Speak Ultra promotes the ultimate in convenience and peace of mind by combining wireless GSM technology with Centurion’s ULTRA interface. The G-Speak Ultra allows wireless communication between the user and the intercom gate station, effectively turning the user’s phone into the intercom handset.

**SDO4:** The SDO4 has been designed to automate domestic garage doors safely, quietly and reliably. The product’s chain-driven system allows for whisper-quiet operation, while a reliable battery backup ensures that the SDO4 will continue working even during lengthy power outages. In addition, the SDO4’s built-in collision sensing circuitry makes it a very safe automation solution.

For more information contact Centurion Systems, +27 (0)11 699 2400, charl.mijnhardt@centurionsystems.co.za, www.centsys.co.za.
Mastercard announced that it will be opening up access to its blockchain technology via its API published on Mastercard Developers. Mastercard's blockchain solution provides a new way for consumers, businesses and banks to transact and is key to the company's strategy to provide payment solutions that meet every need of financial institutions and their end-customers.

The company has tested and validated its blockchain and will initially implement the technology in the business-to-business (B2B) space to address challenges of speed, transparency and costs in cross-border payments. The Mastercard blockchain technology will complement the company's existing capabilities including virtual cards, Mastercard Send and Vocalink to support all types of cross-border, B2B payment flows – account-based, blockchain-based and card-based.

There are four key differentiators of the Mastercard blockchain – privacy, flexibility, scalability, and most importantly, the reach of the company's settlement network.

- **Privacy** – Mastercard blockchain provides privacy by ensuring that transaction details are shared only amongst the participants of a transaction while maintaining a fully auditable and valid ledger of transactions.
- **Flexibility** – Partners can use the blockchain APIs in conjunction with a wider suite of Mastercard APIs to create a range of powerful, new applications. Software development kits are available in six different languages to make the APIs even easier to integrate.
- **Scalability** – Mastercard blockchain is designed for commercial processing speed and extensibility by reaching consensus between a trusted network moderator and network participants.
- **Reach** – Mastercard blockchain is integrated into the company's payment network that includes 22,000 financial institutions to move funds that have been committed on the blockchain.

Dahua Technology's network video recorders (NVRs) now have a direct integration with IP-based outdoor detectors from GJD Manufacturing. This integration provides users with reliable detector-activated surveillance and monitoring.

D-TECT IP detectors and Clarius PLUS IP illuminators have been integrated with Dahua’s NVR6-4KS2 range, an enterprise-level NVR providing up to 4K resolution. Its open architecture supports multi-user access and it is compatible with ONVIF compliance, enabling interoperability when combined with third-party 4K cameras.

The NVR includes intelligent video analytics to detect people and moving objects, as well as other predetermined events, such as abandoned or missing objects, tripwire detection, people counting and facial detection.

The integration was achieved by incorporating GJD’s API on a special firmware that enables the NVR to accept alarms from the detectors and link them to the recorder’s functions. The BS8418-compliant IP detectors are suitable for intruder monitoring, CCTV surveillance and other alarm warning requirements, providing both volumetric and long-range narrow field-of-view sensing, plus remote programming.

For more information, contact Zhejiang Dahua Technology Co., +86 571 8768 8883, dahua.sa@global.dahuatech.com, www.dahuasecurity.com.

---

**Dahua and GJD partnership**

Dahua Technology’s network video recorders (NVRs) now have a direct integration with IP-based outdoor detectors from GJD Manufacturing. This integration provides users with reliable detector-activated surveillance and monitoring.

D-TECT IP detectors and Clarius PLUS IP illuminators have been integrated with Dahua’s NVR6-4KS2 range, an enterprise-level NVR providing up to 4K resolution. Its open architecture supports multi-user access and it is compatible with ONVIF compliance, enabling interoperability when combined with third-party 4K cameras.

The NVR includes intelligent video analytics to detect people and moving objects, as well as other predetermined events, such as abandoned or missing objects, tripwire detection, people counting and facial detection.

The integration was achieved by incorporating GJD’s API on a special firmware that enables the NVR to accept alarms from the detectors and link them to the recorder’s functions. The BS8418-compliant IP detectors are suitable for intruder monitoring, CCTV surveillance and other alarm warning requirements, providing both volumetric and long-range narrow field-of-view sensing, plus remote programming.

For more information, contact Zhejiang Dahua Technology Co., +86 571 8768 8883, dahua.sa@global.dahuatech.com, www.dahuasecurity.com.
The potential for interaction and integration of a large number of things was a theme of the iLegal conference recently, with the Internet of things and large system integration of security systems on sites being a prominent theme. The ability of all these things to communicate to each other is a central feature of the new age of technology. Given the status that the technology is at this stage, one would think that all these security systems would be able to keep time. Our cellphones certainly have this feature and the synchronising to local time is a particularly useful feature. I use an old Seiko chronograph watch that goes everywhere with me, including riding and occasionally falling off horses, swimming in the pool or sea, and even the shower. It occasionally runs out of battery, but once set remains remarkably accurate for a couple of years. I use my cellphone to set my time on my watch and the old grandfather clock in the lounge. However, when the power goes off for any number of reasons, there are a relatively large number of electronic appliances in the house including the microwave that lose track of time when the power resets.

One would think that with the highly advanced technology in security systems that this would not be an issue. After all, we hear a lot about smart devices. However, it is remarkable how often there is an issue with the consistency of time across different security systems or pieces of equipment. You then have a large number of security components or equipment functioning with different times at the same site. This appears to be due to a number of issues:

• The initial setting is just wrong and not enough care has been taken on it.
• When restarted after a power failure, the time is not reset and starts off from the recommencement time.
• The time on the component, including cameras, drifts, so the different components progressively become more out of sync. Depending on the system and algorithms used, the ability to maintain the correct time may be out as much as a few hours over a year if not corrected.

It means that time management becomes an element of security that is not just equated with being at meetings on time and keeping to shift schedules. While some equipment can be self-correcting where it can reference an external time server, to have all your equipment doing this is more difficult to set up. However, the security systems on site should synch with a site-based time server, which is then referenced to an external time server which can supply the correct time. Where effective
time management of your systems and components is not done, whether they are interactive or not, you have a hodgepodge of equipment showing different times and possibly in the worst scenario, even different days or years.

There are a number of implications of this time travelling within the systems.

1. Firstly, when interrogating the systems it becomes difficult to actually access correct data. A person may claim to have entered a particular area at a certain time, but you can’t find such an entry until you start going through a process of searching before and after you actually entered.

2. Secondly, when linking details on different systems or components together, your timing is going to be inconsistent. While this is similar to the first point, the complication comes in when you want to retrieve an image or video of some kind but can’t equate it with the actual time you know it happened, or the access time recorded. Take an investigator who has to put a picture together of what happened over a period of time but it appears the suspect is time travelling or is able to be in two places at once. Similarly, where you may call up multiple camera views to track somebody’s movements, you find one or more of the cameras don’t show people in an area when expected and you now have to jump around with the controls for a particular camera because they are not synched to the same time.

3. Thirdly, while the first two points may cause undue time, effort and frustration, they pale in comparison to the impact of using your systems information for evidence purposes. Whether for internal enquiries, hearings, or judicial events, incorrect and inconsistent times can compromise the evidence quality and lead directly to the failure of prosecutions. A magistrate or judge is not going to look kindly on evidence that seems to have been obtained at different times but is supposed to be of the same situation. A manager faced with a potential review by the CCMA is going to be less convinced about making a judgment against the accused if there are time discrepancies in the evidence. Explaining the intricate technical issues of time setting is not likely to get much sympathy from the person who checks his watch when starting the session.

Users need to ensure the timing of legacy or older systems, or standalone equipment and newer systems remains consistent and correct. Newer systems are dealing with these issues more effectively, but the need for accurate time servers is still just as important. What is perhaps most questionable is why your conventional retail store watch is so much more effective at keeping the right time compared to multi-million rand security systems that you are purchasing. In this sense, the security technology industry should have been paying more attention to this relatively simple issue while they have been pushing all these other ‘remarkable’ inventions and smart capabilities. The bottom line though, is if your devices are all showing different times, its time you did something about it.
Minimising maintenance
ANNIE applies learning to proactively minimise maintenance.

The idea to use a form of autonomous decision-making engine was birthed when Gerhard Furter, the creator of Naxian Systems’ ANNIE (Artificial Neural Network Inside Everything), was busy with a project for a government department in the justice sphere. It was realised that a lot of the decisions that the operators had to make were very habitual, but also based on more information than a ‘normal’ human could realistically process. These decisions could, however, be repeated by a machine if the machine could be made to understand the ‘why’ of the decision.

Furter developed suitable algorithms and ANNIE almost immediately took over 40% to 50% of the operators’ work. “She rapidly grew as clients posed a challenge based on some strange requirements, whereafter I would engineer a way for ANNIE to solve the problem, and a new set of algorithms would be spliced into ANNIE’s persona,” says Furter.

ANNIE’s purpose is very simple: to learn about and understand the environment in which she is implemented and use this knowledge to identify when something may go wrong. In ANNIE terms, a situation in which the environment is working as it should, is referred to as state 0 (zero), or zero risk.

To understand the environment, ANNIE acquires information using whatever systems she can integrate into, and attempts to identify ‘normal’ through the use of typical behaviours exhibited by the various groups or populations of assets and people. She then benchmarks and trends anything she can measure, and identifies patterns that describe habits, processes and associations between assets, people and events.

The resulting model is a real-world depiction of what her environment looks like. She uses this model to study all changes, deviations and exceptions with the intention of not only identifying problems as they evolve, but also to anticipate (predict) when something will happen that is not advantageous to the client’s operations. ANNIE will use whatever methods the client allows to try to solve the issue, or to prevent it from actually occurring, using a simple warning SMS or launching a full-blown intervention using digital or electronic devices.

To date, ANNIE’s application has facilitated a number of positive results for organisations that include:

- Increased transparency. By applying ANNIE to historic data, organisations can for the first time make sense of big data because she indicates trends, behaviours, patterns and associations that are traditionally not exposed by business intelligence resources and tools.
- Decreased risk. By applying ANNIE to real-time data in any operational environment she is able to detect anomalies that humans can never detect. This is because she looks at everything, all of the time, and then compares this to everything she has trended as ‘typical’ from past knowledge inside an environment. For anything detected outside of typical, she will raise a ‘watch dog’, which is an early indication to organisations that something suspicious may be in progress.
- Increased profits. Because of the fact that ANNIE is aware of all environments that she is connected to, at all times, she will always find the most optimal way of deploying resources. In for example the case of maintenance of systems and devices, ANNIE will ensure that the most proficient resource is sent to a faulty site, by way of the optimal route based on traffic and weather conditions, with the right tools and/or stock in hand to resolve any technical issues on site.

Where most other AI’s will implement features that are more suited to the boardroom or data science laboratory, ANNIE will roll up her sleeves and do the dirty work of not just analysing the data, but also causing physical changes in the environment entrusted to her, says Furter.

The AI development team at Naxian is engaging with Microsoft as a cloud partner to ensure that ANNIE is made available as a service through cloud platforms such as Microsoft Azure. “However, as we connect billions of things to the Internet, it is unreasonable and impractical to expect that all data and signals are sent to centralised or distributed cloud environments in order to apply the AI.

“Rather, we believe that AI should sit on the edge devices themselves. Instead of the weather station, traffic analytics service, video surveillance camera, access control device, etc. having to send data to a central point in order to collaborate and produce a result through the application of AI, these devices should have the AI embedded or attached at the edge and talk to each other. Our immediate core future focus is to ensure that we ‘port’ our intelligence onto edge devices such as Raspberry Pies and other microcomputer platforms,” says Furter.

For more information contact Naxian, +27 (0)87 820 0620, bernard@naxian.co.za, www.naxian.co.za.
THE SMART WAY TO IMPROVE PRODUCTIVITY AND DECREASE MAINTENANCE...

“If there’s one thing the world’s most valuable companies agree on, it’s that their future success hinges on artificial intelligence.”

Enrique Dans

Artificial Neural Network Inside Everything

In Gartner’s Top 10 Strategic Technology Trends in 2017, Artificial Intelligence (AI) is at the top of the list. So, if you are not acting on AI today, you will be playing catch-up. Naxian Systems’ AI – ANNIE – learns and understands her ambient environment and uses this knowledge to proactively anticipate possible problems.

The benefits?
- Increased system transparency
- Increased profitability
- Decreased downtime
- Better utilisation of resources
How to implement physical security

By Brent Cary, Genetec.

A key concern with respect to the maintenance of control centres and substations is security.

Managers of both suburban and rural power substations are faced with many challenges today, including safety, power density, right-of-way issues and cost. One of the key factors attributed to these challenges is the increasing migration activity of people from rural areas to urban homes and workplaces, which in turn, drives up the demand for municipal power distribution systems.

In essence, city dwellers – or those who have maintained residence in an urbanised setting – are recognised as higher per-capita energy consumers, which consolidates the premise of ‘more users equals more power needed’. In order to address these challenges, a new strategy should be developed and implemented, which can be enacted upon after conducting a thorough and comprehensive risk assessment process.

One key concern with respect to the maintenance of control centres and substations is security. Power utility facilities have to deal with situations like theft, vandalism and the need to comply with set international security standards. In fact, a potential attack or emergency situation on these facilities underscores the risks associated with physical security breaches and their possibly disastrous effects.

Across the region, control centres and substations utilise basic technologies like perimeter fencing, outdoor lighting and CCTV surveillance. Some are still known to be using key-based access control and previous generation analogue video systems – hindering immediate intervention or quick action should a situation come to light. The grainy analogue video feeds will possibly be able to catch an intruder on camera, but will lack the sophistication that today’s high definition (HD) IP cameras can offer, that can result in an image for positive identification.

The emergence of these challenges, combined with the need to integrate newer technologies to help further enhance security measures should prompt the utilities industry to make a transformational shift towards more modern, advanced and highly-efficient Internet protocol (IP) solutions. Regulators should implement stronger security mandates and urge power providers and operators to make the bold move of upgrading their present security systems – especially across mission critical areas.

However, operators and providers must first conduct a review and assessment of security risks and vulnerabilities of their facilities, which will give them an idea on how to execute a security strategy should any situation arise. At the same time, these companies and organisations should put their own security standards in place – effective and efficient measures designed to address physical attacks, cyber attacks and the occurrence of natural disasters.

Utility providers and operators will now have to upgrade better security systems to help tighten security. Industry experts have recommended the use of specific system features to ensure a successful upgrading of equipment and have suggested the following:

• **Implementation of network connected systems:** Having all devices connected to a singular network presents many advantages and benefits, like real-time information, the immediate detection of potential threats, on-site modification and configuration and the easy management of the system itself.

• **Utilisation of a strategic unified platform:** With multiple security systems like CCTV video surveillance, access control, automatic licence plate recognition (ALPR) and perimeter detection running at each site, it is essential to utilise an open-architecture platform that can accommodate easy customisation and integration across a diverse range of security and business systems.

• **Control and access to one central station:** If there are multiple sites and substations to secure, centralising security operations becomes highly beneficial and cost-effective. The creation of a federated architecture will give operators and providers the ability to manage all sites and systems as one global operation. All video and data is sent back to a central location, where alarms and events from various sites can be received and acknowledged.

• **Shift to open architecture:** The move towards newer and more advanced systems will need a key feature like open architecture – which can facilitate the integration with other systems and provide complete freedom in the device selection process.

• **Mapping and mobility:** Using a map-based interface simplifies system navigation, which in turn can help effect quicker responses to arising situations. Meanwhile, mobile connectivity gives essential personnel the capability to access the facility’s systems though their phones, tablets or any mobile device – a pivotal advantage especially during critical situations that happen at odd hours of the day.

In conclusion, power utility providers and operators should develop and implement a comprehensive set of security strategies to aid them in their efforts to upgrade security systems that are also in compliance with international standards and guidelines. These utility facilities should understand the need to be up to speed with today’s technological advancements, particularly across the safety and security segment, thereby guaranteeing the safety and the security of these very essential utilities’ control centres and substations.

For more information contact Brent Cary, Genetec, bcary@genetec.com, www.genetec.com.
System Integrators

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

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

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

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

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

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

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

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

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

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

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

**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
The complexity of borders

By Andrew Seldon.

Controlling borders is a critical task for governments the world over, both at official and unofficial entry points.

There are many aspects of security that governments need to be aware of and be on top of in terms of having control and insight. When a government’s resources can be wasted trying to ban a book, it would be reasonable to expect they have the time at hand because all their other security issues are well in hand. Sadly we know this is not the case.

Of all the security issues a government should be dealing with, protecting the borders of a country must be one of the prime concerns. Over the past year or two, border control has become a hot topic globally, where in places like the EU it is harder and more expensive than ever to legally gain entry, but seemingly simple to get in illegally. The same can be said, to a lesser degree, about South Africa.

To write an article covering all aspects of border control would require a book, probably many books, so in this feature we limit ourselves to two primary aspects of border control. The first is the issues faced when trying to control long borders where there are an infinite number of places to cross into a country illegally, simply putting up a fence is of limited value, but installing all manner of technology, while it would be far more effective, is far too costly.

The second area is one everyone who has travelled internationally is familiar with, that of entry to a country through the normal border controls at an airport or port, for example. Simply getting your passport stamped by a grumpy official doesn’t cut it anymore, but what else can be done to ensure those entering are who they claim and aren’t trying to get through with fake documents and malicious intent? And it would also be better to do it faster without losing control.

The higher you build your wall

Building a wall isn't always the best border control solution. If you have a limited area to protect and you can ensure you patrol that area efficiently, a wall can make a difference. However, you still need to have technology solutions in place along the wall to stop those determined to cross from coming over, under or through the barrier.

So, when looking at long borders, adding technology to a wall or fence of some kind is the only real way in which a country can manage and protect the border. Fortunately, today’s advances in security systems make this somewhat easier. Charles Harrison, MD of Secu-Systems explains that the traditional security technologies we use in residential estates or mines, among other areas, while very effective in those situations, are not up to the task when it comes to long borders.

“When you have a perimeter that is hundreds or thousands of kilometres long, you can’t expect to set up a chain of surveillance cameras as this would be far too expensive. What you can do is have a physical barrier (a wall) and make use of specialised technology that can handle the long distances while still being accurate enough to guide human resources to any locations where an incursion has occurred. And of course, there are areas where there is no fence or wall for various reasons and technology is your only option.”

One way to manage the area is via military-grade thermal cameras, which can identify people moving over ranges of up to 50 km (depending on the technology and how much you can pay). While the technology is there, it is expensive and requires special licences from the country selling them as well as the buying country (for example, for an American thermal of this type one would need authorisation from the US government to export it and authorisation from the South African government to import it).

There are also solutions available that allow for the detection of friend or foe at a distance, allowing control centres or analytical software to easily determine which side detected people are on. Harrison adds that the Panoptes MTI (moving target indicator) software has been used by Secu-Systems with great success in various scenarios where distant intruders have been identified and tracked after they crossed the border line.

And tracking is important in border control. Simply recognising an intrusion and dispatching a patrol will seldom result in catching the intruders due to the distances involved. Apart from thermals, Harrison says radar is another option for border security as it allows for long-distance observation. With a ground radar system, the movement of intruders can be tracked over time to allow for effective response.

Hotpot surveillance

The one potential issue with the solutions mentioned is that of terrain. They work well...
in flat areas without too many hills and valleys. No radar or thermal technology can see through everything, however. This, according to Harrison, is where UAVs (drones) come into the picture. When fitted with thermal and visual cameras, they can offer surveillance and tracking in any lighting conditions, although the length of time they can stay in the air is an issue. Another option is mobile surveillance solutions that can be driven around to different locations, also equipped with thermal and visual cameras, as well as analytical software.

Yet even this is not enough when it comes to borders. The reality is you simply can’t be everywhere all the time, even with technology’s help. Harrison therefore suggests that intelligence is key in effective border control. “You need to know where your hotspots are. In other words, the areas where most of the intrusion happens, and then focus on those areas.”

The Kruger National Park is a South African national treasure, but it is also an area many people use to enter South Africa illegally. It is also a hotspot in terms of poaching and other criminal activities. Focusing your resources on these areas will result in more ‘successes’ in preventing crime than randomly trying to control an almost endless border.

It’s critical to note that there is no single solution to the border problem. Harrison says decisions must be made according to the location and environment under investigation, its importance in terms of the goals of the country, and then an integrated and tiered solution designed to meet those specific requirements.

He adds that there are also some quick wins to make. It’s not unheard of that people reach a border post that they won’t be allowed to cross, and simply walk a hundred metres or so down the road where there is no security and stroll across unhindered. “It’s not always a million dollar solution that can make a difference, but knowing what the problem is and designing an effective solution to deal with it.”

At the border
Of course, most people enter countries at border posts (one hopes), where they present a document such as a passport containing a visa and so forth. As noted above, even this is not a simple identity document anymore as forgers are masters of their art. Today’s border controls require more complex technology vetting both with respect to identity documents like passports and external technology (mixed with human insight).

Sanjay Dharwadker, head of the Global ID Consultancy Practice at WCC Smart Search & Match in Europe, explains that identification in these scenarios is changing. “There are two trends that are simultaneously emerging in this respect: strengthening legal identification and
“I can imagine behavioural biometrics to be a potential disruptor amongst the more widely used physiological biometrics.”

- Sanjay Dharwadker.

Sanjay Dharwadker.

physical identification as well. Both are causing additional stress on the passport issuance process as well as at border control.”

On the legal side, he says states are increasingly required to perform checks against (for example) birth and death records (civil registration). Traditionally, this involved more paperwork, but passport-issuing authorities are already making plans to do this digitally. The work in this area heavily depends on ‘biographics’ like names, dates, locations etc. This is further supplemented by what is being called ‘the social footprint’ (not to be mistaken with social media). For example, if you say you have lived in Johannesburg for twenty years, can you show educational or employment records, payslips, utility bills, etc?

“Such linkages to ‘evidence of identity’ are already postulated and are likely to become commonly deployed in the next two to five years. ICAO (the International Civil Aviation Organization, an agency of the United Nations) is already in the process of introducing the necessary policies in consultation with its 191 member states, especially during the period 2018 to 2020.”

On the physical side, the policy, standards and its legal enforcement for biometrics are already in place. Today, all travel documents are mandated to be machine readable (MRTDs). Further, there are interoperable standards for chips that might be part of such MRTDs. If a MRTD has a chip, then storage of facial biometrics is mandatory, while fingerprints and iris recognition are optional.

“In general, any MRTD chip can be read at any border crossing and an ICAO-managed public key interface ensures that the data is not tampered with,” Dharwadker adds. “Devices that do live capture of biometrics also need to conform to the standards, and thus comparison with the biometric data on an MRTD chip is already being done regularly. The automatic border control (ABC) gates are an example, and these predominantly use facial biometrics.”

Over 100 million new MRTDs are issued every year and it is estimated that at least half of them have chips with facial biometrics.

He adds that MRTDs follow the ISO biometric standards. These are formulated by diverse workgroups drawn from national standards bodies, academics, research, industry, professional bodies, UN organisations and governments. These come together under ISO/IEC JTC1/SC37 and after consolidation get incorporated (or referenced) in the ICAO Doc 9303 – the mother standard for MRTDs that is followed by its 191 member states. “ANSI and NIST do a lot of the heavy-lifting required for biometrics standards in their role as the US national standards bodies and also the SC37 hosts.”

Big brother pre-empt you

Whether we are too influenced by Hollywood visions of artificial intelligence and the ability of systems to run diagnostics on the fly, or whether we simply assume these ‘Big Brothers’ will be or are a reality, most people assume that automated biometric recognition is or will be a reality in future. The Chinese government’s multi-year project to roll out facial recognition in many large cities is an example of the future we all fear.

But is automated biometric recognition, such as facial recognition as you walk off a plane, or behavioural biometrics becoming a reality in border environments?

Dharwadker says technologies like these are in the prototyping stage and generally deployed post-facto for crisis management. “After the London subway and the Boston marathon bombing incidents, facial recognition biometrics was said to have been applied to the CCTV footage to help identify the perpetrators, and their movements were also studied.

“As I understand it, CCTV footage is regularly collected at airports. Behavioural biometrics is still in its infancy, but is fast catching up with fingerprint, face and iris due to its capability of more continuous detection in real-time and its application to both crime and fraud. As of now, I can imagine behavioural biometrics to be a potential disruptor amongst the more widely used physiological biometrics that tend to be static and do not add information on a continuous basis.

“The deployment of such technologies, he says, especially at airports, is clearly to minimise the burden on human fatigue, of officials trying to be alert and observe those curious exceptions which might prevent acts of terror.”

By the end of 2030, nearly seven billion individuals will pass through airports every year, a very large number that will mandate more technological eyes on people entering and exiting.

Electronic authorisation

With the use of modern technology and biometrics a given, it seems to be logical that having a paper book with a visa stuck inside is a bit outdated. And so it is.

One of the important components of the new air travel regime, says Dharwadker, will be the Entry and Exit System (EES). “This will go hand in hand with other measures being put in place that include: Electronic Travel Authorisation (in lieu of a paper visa), Advance Passenger Information (API), Passenger Name Record (PNR), check against watch-lists and the Interpol list of stolen and lost travel documents (SLTDs).

“The EES will come in two forms, on back-end systems and in the MRTD chip. However, it will essentially record when a person enters and leaves a country and that the entry and exists records are reconciled. An important measure that is likely to be legally enforced in as early as 2018 is that the outcome of the API can be used for a ‘board/no board’ decision for individuals on flights, thus barring individuals with doubtful credentials from travelling.”

Such measure will be enforced along with a closer look at other aspects of a travel-related profile, such as tickets purchased against cash, or short stay following long-haul flights. So the principle being applied is to take advance action as much as possible before the person reaches the border.

Complexity abounds

The reality is that border security always has and will be a critical issue for governments, and those with poor or incompetent controls are likely to be playing host to an ever increasing influx of criminals and potentially terrorists – not to mention the poor souls just looking for a better life. There is no simple solution, but by understanding the issues and addressing them head on, much of the chaos we find in border control today can be avoided and order re-established.
Government needs better technology

By Johlene Selemela, ZKTeco.

Security is central to the effective functioning of any government.

Government and related organisations are responsible for holding and managing information that is critical to a country and its citizens. Public security plays a major role in this regard and governments need to ensure the protection of citizens, organisations, and institutions against threats to their well-being and to the prosperity of their communities. In addition, the role government plays in society requires high levels of security to keep digital and physical assets safe, while making them securely accessible where required.

Now, how much can technology contribute to the overall security of government facilities, courts, power stations, prisons etc? In a time like this, it is a world-wide trend to use more technology instead of the traditional human observation and presence on site.

Today’s government departments demand what identity management solutions provide which include the following superior service experiences, person/card not present transactions, efficient workflows, elevated security and device agnostic software.

On the other hand, departments need technologies that enable them to achieve these objectives while increasing public loyalty and satisfaction. To meet the increasing challenges in the public security area, responsible public institutions and organisations can tap into their own intelligence to successfully address possible threats in advance. They can optimise their internal structures, use synergies, and carefully balance costs and benefits of their measures, by introducing cost effective security measures.

The ever-changing regulations for governmental institutions have resulted in the need for more efficient public centric processes, when it comes to identity proofing. Border management and national security concerns have expanded the need for reliable and fast methods for checking credentials at border crossings, ports, airports, courts and government institutions. These facilities need to consider systems that provide advanced technology solutions for passport and ID verification as well as increased speed of processing travellers and visitors.

This means that identity management solutions need to aid highly trained inspectors by flagging details that may not be visible or by finding recent criminal innovations in highly sophisticated fraudulent identification documents.

Prior to granting access to information, an individual who has been cleared must sign a Security Screening Certificate and Briefing Form, indicating their willingness to be bound by several Acts of Parliament during and after their appointment finishes. Today, all this can be done by means of devices that allow for fingerprint, facial recognition and palm print to capture your information and allow for one transaction to take place.

Government security is the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of South Africans.

For more information, contact ZKTeco (SA), +27 (0)12 259 1047, sales@zkteco.co.za, www.zkteco.co.za.
Integrated border management

The most important component in the deployment of a physical security solution is the integration of various security systems into one solution.

Border management is complex and multifaceted as it involves multiple government departments, including national and provincial authorities responsible for agriculture, health, revenue and tax, state security and transport services. Integrated Border Management (IBM), a concept first used by the European Union in the early 2000s, calls on the collaboration between these various key government departments to improve border management.

IBM states that individual border authorities are generally more effective when cooperation is in place. This translates to cooperation between the various departments involved in border management in the same country as well as cooperation with the border authorities of neighbouring countries.

In the SADC region, South Africa’s borders, for example, are managed by five different departments. With the Border Management Authority Bill, the government intends to establish one centralised authority to handle all matters of border management, including policing and customs. The Bill clearly states that “There is a need for integrated and coordinated border management that facilitates secure travel and legitimate trade in accordance with the Constitution, and international and domestic law.” Although the Bill was passed by the National Assembly in June this year, it has been criticised by opposition parties, who argue that setting up and operating the authority could be fraught with complexities.

While some countries have merged border agencies and others have set up formal structures for cooperation, the aim of these integrated border management systems tend to be the same: facilitating legitimate travel and commerce while preventing illegal cross-border activities.

Physical border security

With the growing threat of terrorism, syndicated crime, poaching and smuggling, and the unlawful movement of people, drugs and contraband, protecting national borders is a priority. One of the key components of border management is physical border security.

With proven experience of border protection solutions around the world, Betafence has established specialised physical security solutions that have been specifically configured for border security.

To provide effective protection against the multiple and diverse threats faced by border authorities, comprehensive border security would mirror the idea put forth by Integrated Border Management: the combination of various systems into one integrated solution. For border security, an integrated solution would ideally consist of the following components:

- Physical perimeter
- Long range surveillance systems
- Perimeter intrusion detection systems (PIDS)
- Access control
- Integration and maintenance

The physical perimeter of a border comprises the actual demarcation of the international boundary and provides a physical barrier against illegal crossing. Depending on the risk factors of each individual border area, fencing solutions can provide hardened protection against cut and climb attempts, hostile and unauthorised vehicles, and even ballistic and rocket-propelled grenade attacks.

A critical feature required from border fencing is good visibility that enables border protection officers to perform surveillance. Fence visibility is also important for camera surveillance. When integrated into a total solution, long range radar, CCTV and security lighting offer reliable detection and surveillance, which aids border officers in accurately assessing situations and responding effectively to potential threats.

A vital security system that will ensure that teams are deployed in time, is Perimeter Intrusion Detection Systems (PIDS). PIDS augments the physical perimeter to provide early warnings of breach attempts (climbing, cutting and bending of fence fabric) and triggers alarms, cameras and lighting for effective detection and inspection.

Lawful crossings

For the control and management of lawful border crossings, border authorities use access control systems at authorised border checkpoints. The physical barriers and structures employed at border checkpoints include vehicle wedges, bollards, tyre killers, turnstiles, gates and guard houses. The design of a checkpoint must include access control in such a way that: border officers are protected and supported in performing their duties; vehicle traffic and speeds are managed; unauthorised entry is prevented.

Where hostile vehicles pose a threat to security, crash-rated barriers can provide mitigation. Wherever crash-rated solutions are used, border authorities need to verify that the systems have been tested and certified according to relevant standards.

The final component in the deployment of a physical security solution is the integration of all of these systems into one solution. This ultimately enables border authorities to assess the intelligence gathered from the different components to effectively respond and report any and every security event. The purpose of an effective border security solution is not only to prevent illegal cross-border activities, but also to empower border authorities with the ability to detect and react to breach attempts and facilitate legal crossing at designated checkpoints.

As miscreants become more sophisticated, security systems must be a step ahead to anticipate, detect and mitigate against threats to protect our citizens, infrastructure and economy.

This article was supplied by Betafence. For more information contact Betafence South Africa, +27 (0)21 868 7300, www.betafence.co.za.
The mission of securing a nation’s borders is challenging for many reasons, chief among them is the sheer size of the area that needs to be effectively monitored and patrolled.

Border surveillance solutions from Secu-Systems provide Frequency Modulated Continuous Wave (FMCW) radar and multispectral imaging sensors needed to meet this demanding mission, as well as command and control software that enables the creation of a flexible, scalable border security infrastructure that can meet the demanding, ever-changing threats encountered every day.

Effective radar coupled with long-range thermal and visible light imaging systems provide advanced warning of inbound threats, as well as the visual threat assessment needed to formulate an effective response. While the initial investment in hardware may be more costly than for a lesser solution, the long-term operational cost actually results in a net savings.

By coupling long-range optical systems, the nature and threat levels of intrusions can be determined remotely in the command centre or forward observation post instead of having personnel respond to every alarm in their sector. In other words, what’s spent with the initial acquisition is saved whenever your response teams don’t have to waste time and resources visually verifying the causes of alarms. The combination of radar and long-range imaging is also more adaptable to changing threat structures, speeds and even topography.

Each technology has its strengths and weaknesses. Using them as complementary sensors allows operators to use the strengths of one to overcome the weaknesses of the other. For instance, while radar can provide persistent 360° coverage every second out to distances of more than 5 km, it can neither identify friend or foe, nor determine the intent of what it detects. Conversely, an imaging system can identify the target, but in doing so it is covering a comparatively narrow field of view.

Combining the two technologies provides a persistent coverage of multiple targets, while the camera (or cameras) can automatically slew to targets of interest and identify them. Effective radar detects threats at great distances, providing important reaction time.

Radar provides important target parameters – range, bearing, course, speed and GPS coordinates. With these parameters, and a long-range thermal imager, situational awareness is greatly increased and the appropriate response can be quickly determined and taken. But knowing that a radar/long-range thermal imager multisensory solution is the answer is only part of the decision.

For more information, contact Secu-Systems, +27 (0)11 794 7834, charles@secusystems.co.za, www.secusystems.co.za.
A thermal border

Thermals can cover an extended border more efficiently in all lighting conditions.

Like many cutting-edge technologies, thermal imaging was first developed for military use in the 1950s and 1960s when the US successfully introduced cooled infrared detectors onto missiles. Infrared detectors eventually evolved into thermal imaging technology, which has made its way into non-military applications and is now widely used in various areas such as industrial inspections, medical diagnoses, and in satellites.

An important milestone in the advancement of this technology was the invention of uncooled infrared detectors, which enabled cheaper and easier to maintain thermal imaging products to make their way to the general market for use in applications including security surveillance, forest fire prevention, and power plant monitoring.

Dahua Technology has developed thermal imaging devices with innovative functions that balance visible light with infrared, enabling the ability to effectively monitor an area under all lighting conditions. In addition, these functions include advanced capabilities such as intelligent temperature measurement, which further extends the scope of surveillance applications such as in detecting forest fires or quickly checking for passengers with high fevers at international airports.

Border security

Border security concerns not only the security of the country, but also the safety of citizens and their property. Traditional border monitoring systems still face many imperfections:

First, a relatively small amount of patrols are employed to guard large areas, leading to gaps in coverage. In areas where cameras are used, there are often blind spots in their line of sight, such as tall grass or brush, or places beyond their range. Finally, when emergencies occur, responses can be slow and inefficient due to the scattered nature of guards and the need for manually sounding alarms.

Dahua has created a solution to tackle the challenges of border surveillance. For example, take a 100 km section of essentially unlit, wild border terrain. A thermal dome camera (TPC-SD8320) with 30x zoom can be installed every 1 km. It can quickly detect objects using thermal imaging and then confirm threats using visible light images. In this way, night monitoring difficulties can be completely overcome with infrared light. In total, just 100 cameras alternately placed on both sides of the border are necessary to provide full coverage.

Now, instead of a number of patrols working alone outside over a large area, a small team of workers can manage the border from a command centre, which features advanced automated functions. The centre is outfitted with an e-map, which shows the location and current sight line of each camera, allowing border workers to assess surveillance coverage in realtime.

When a camera detects someone entering a restricted area, it will automatically trigger an alarm while continuing to track the target. Staff can then alert the intruder and warn them with sirens.

New HD video solution

The Holis HD video recorders combine with new HD analogue cameras to offer affordable alternative to IP for SMB market.

Johnson Controls has introduced its HD Video Solution, a new value-based solution that provides video quality while supporting analogue infrastructure. The Holis HD Trbrid Video Recorders support SD analogue cameras, Illustra Essentials IP cameras, and a new line of HD cameras.

Available in 4, 8, and 16-channel models, the recorders feature search, record, zoom and export functions, as well as all channel synchronous real-time playback for simplified post-event forensics. With support for H.264 dual-stream video compression, the recorders feature up to 12 TB of storage and 1080P real-time-recording across all channels.

Combined with the new American Dynamics HD camera portfolio which includes fixed and varifocal bullet and dome cameras, the HD video solution provides an alternative to IP cameras and allows users to upgrade their system over time while protecting their CCTV investment.

The new fixed HD bullet and mini-dome cameras boast 3.6 mm fixed lenses and provide up to 1080p video resolution (1920 x 1080) in an uncompressed format over the same standard coaxial cable that is used for standard CCTV cameras. Where most dome cameras operate on two axes, the fixed mini-dome’s 3-axis feature has a much wider field of view.

The varifocal HD bullet and dome cameras include a 2.7-12 mm motorised lens, and feature Smart Infrared for recording over 50 metres away in total darkness. The cameras are waterproof, rated IP67, and feature WDR, making them an ideal solution for applications with volatile weather or lighting conditions.

For more information, visit http://www.holisnvr.com/.
Smart cities are built on smart thinking

By Brett van den Bosch.

The phrase ‘smart city’ tends to conjure up images of glistening, Utopian sprawls where people can live untroubled by the dangers and mundane inconveniences that are an unavoidable part of any real, modern cityscape. Perhaps that should be the ideal, but even the wealthiest nations have a long way to go before achieving it, let alone South Africa with its particular set of problems.

The world’s leading smart city exponents, like Dubai and Singapore, can feel very far away from us here at the southern tip of Africa, but there is much that can and should be done to work towards, if not Paradise City, then at least smarter and safer metropolises for the country’s denizens to create a better future. If one embraces the wisdom that within every challenge lies an opportunity, then it could even be said that the almost ubiquitous sprouting up of residential estates in South Africa creates an ideal breeding ground to develop and perfect the elements of smart city creation on a smaller, more manageable scale before scaling up to our cities.

Although South Africa should and will forge its own path in this, as it does in all things, there is no harm in learning lessons from what the rest of the world is doing, and many experts the world over are hard at work advancing the fundamentals of smart cities. Hi-Tech Security Solutions consulted three of them to help piece together the building blocks upon which a modern, forward-thinking city is built.

First safe, then smart

So what is the first step, when there is so much to do? In the experience of Edwin Diender, Huawei’s global vice president for the government and public utilities sector, the smartest opening move is to create a safe environment. ‘Public safety is such a broad issue that it touches every individual, community and organisation,’ he clarifies. ‘If a person feels safe where they live and work, they enjoy being there and aspire to create a life there for themselves and their families. As this sense of safety spreads throughout a community, a desire grows for all sorts of public services to make life easier, and in fact this can be considered a KPI of a smart city. Once a solid foundation of safety is established, a smart city can branch out into other domains like traffic, energy, city efficiency and information sharing across different spheres.’

His experience working in various roles with several industry leading vendors, together with his personal history working on southern African programmes and initiatives, gives Diender valuable insights into local issues. Given South Africa’s high unemployment rates, he is adamant that the point of making a city smarter should never be about replacing people’s jobs with machines. ‘The goal is to improve efficiency at the city level through integration and holistic thinking,’ he elaborates. ‘As an extension of our respect for communities, Huawei works to establish initiatives for the youth to better understand these concepts, and possibly even inspire them to a career in smart city management. To this end, we work together with local stakeholders to establish schemes for students to use these programmes and initiatives as a sort of internship, and we are also involved in nurturing the next generation of graduates by collaborating on establishing education curricula.’

Diender explains that Huawei has developed a strategy that looks at smart city developments as a journey, and aims to establish not so much a roadmap as a

www.securitysa.com November 2017 29
SECTOR FOCUS: SAFE/SMART CITIES

today, but no cities have been planned with an IT infrastructure in mind – cities have transportation, water and energy infrastructures. This means we need to add a new infrastructure utilising whatever existing bits of IT infrastructure are present. Depending on the size and age of the urban areas, this can be a daunting task.”

Steffens points out that one of the major benefits of smart cities is the wealth of data and data sources, and Milestone is well positioned to facilitate this. “Video systems like Milestone XProtect, with rich integration of data sources and metadata, can combine and aggregate information from multiple data sources for true, holistic situational awareness. This paves the way for combining video management and cognitive systems, in turn leading to predictive systems, augmented reality displays and interpretive functions and moving the use of video systems beyond security. These are all areas Milestone is looking into.”

Smart is an evolution

First and foremost, it is important to define what a safe and smart city is, and to have a holistic view of how one evolves, according to Eugene Le Roux, MD and president of NEC Africa. “Cities transform from initial construction to introduce facilities that enrich people’s lives, then growth accelerates and that brings new challenges. Cities continuously grow, mature and reconstruct around infrastructure, transport, energy and citizen lifestyles. It is important that they be able to do so flexibly so they can cater for unknown future demands,” he says.

As in any sphere of life, data and the intelligence it enables are vital to the success of a modern smart city. “At each stage cities must be able to collect and share information more effectively and link those layers that support urban life,” explains Le Roux. “ICT can bring people together, can strengthen the fabric of society. Encapsulating that information in an intelligent platform means it can be monitored in real-time and transmitted anywhere it’s required, for plain old everyday needs or for special needs that arise during disasters and other emergencies.”

Since the communications infrastructure is so essential, Le Roux says the first thing that is needed is a network that links to every area of the city, at the centre of which is an intelligent platform that collects and collates data from multiple sources that range from Internet of Things (IoT) to social media channels. It must analyse the streams automatically – overseen by humans where

Integration

The smart city makes an ideal candidate for this type of approach, as integration at various levels is at the heart of any successful rollout. “It is vital to link together the various information systems into a unified platform,” he says. “As a practical example, this can enable a live police investigation to automatically bring together the initial emergency call made by a person with CCTV footage of the incident’s location, and bring it together on a geographical information system (GIS) map. These elements are all available in South Africa but are currently disconnected – all that remains is to bring them together. The efficiencies that result from such integration facilitate taking the next step along the journey and progressing the concept further, and faster.”

The nuts and bolts of a smart city initiative are inextricably tied to the availability of a reliable communications infrastructure, and Huawei has extensive expertise in this regard, explains Diender: “LTE (long term evolution) mobile technology, which is already broadly deployed across South Africa’s major cities, is a key enabler as it not only provides for the needs of today but also for tomorrow as we move from the current fourth generation (4G) to 5G and beyond.

Another invaluable tool is cloud technology, which allows several information services to be brought into a back-end infrastructure where it is easier to be maintained and serviced; but also, from where it is easier to be made available and shared across agencies and departments. And with communities and people across the city. For example, Huawei’s technology is able to create a layered segment specifically for public safety, and employ bandwidth optimisation so that a drastic forklift upgrade is not always necessary. We also have the capability to put in place an integrated platform that can function as the heart for bridging diverse communication channels such as landline, voice, video, data, mobile and two-way radio, to name a few, and to use these capabilities across a wide range of different terminals and devices, including apps to facilitate services to the community.”

No matter the extent of the programmes and initiatives, Diender asserts that it must be underpinned by ambition, coupled with a clear and realistic vision. “In this context a smart city could be viewed as a platform, or a system of different functions, that is able to bridge all the initiatives and programmes to help move the community higher up the value chain. As a starting point, the key ‘pain’ points of the city in question must first be identified before they can be addressed. This is different for every city – each will have a different approach for achieving its goals, but it always starts with an ambition and a vision,” he concludes.

Smart does not equal safe

While it can be tempting to use the terms safe city and smart city interchangeably, Armand Steffens, Milestone Systems’ country manager for the African continent (except Northwest Africa), believes a distinction should be made at the outset. “A smart city is not necessarily safe, nor is a safe city smart in the sense of intelligence,” he opines. “For us, a smart city is an urban area that uses diverse types of electronic data collection and sensors to supply information used to manage assets and resources efficiently.

“The smart city concept integrates information and communication technology (ICT), and various physical devices connected to the network (the Internet of things or IoT) to optimise the efficiency of city operations and services and connect to citizens. Smart city technology allows city officials to interact directly with both community and city infrastructure and to monitor what is happening in the city and how it is evolving.”

By contrast, he describes a safe city as an urban area where the citizens experience a low to zero number of safety incidents. “If a smart city can reduce the number of incidents, then this is a positive effect of an intelligent infrastructure,” he says.

Digging deeper into the communication fundamentals required, Steffens describes a smart city as “basically a very large IT infrastructure – and an IT infrastructure is an IT infrastructure, no matter the size of it. The same principles of connectivity, interoperability, security and scalability apply no matter the size. Then there is data flow, where strict governance rules have to be in place to ensure that the needed data is available for performing each different task within a secure context. Cybersecurity has to be an important part of any smart city project, as well as privacy and data governance.”

“We have all the technology needed to be made available and shared across agencies and departments. And with communities and people across the city. For example, Huawei’s technology is able to create a layered segment specifically for public safety, and employ bandwidth optimisation so that a drastic forklift upgrade is not always necessary. We also have the capability to put in place an integrated platform that can function as the heart for bridging diverse communication channels such as landline, voice, video, data, mobile and two-way radio, to name a few, and to use these capabilities across a wide range of different terminals and devices, including apps to facilitate services to the community.”

No matter the extent of the programmes and initiatives, Diender asserts that it must be underpinned by ambition, coupled with a clear and realistic vision. “In this context a smart city could be viewed as a platform, or a system of different functions, that is able to bridge all the initiatives and programmes to help move the community higher up the value chain. As a starting point, the key ‘pain’ points of the city in question must first be identified before they can be addressed. This is different for every city – each will have a different approach for achieving its goals, but it always starts with an ambition and a vision,” he concludes.

Smart does not equal safe

While it can be tempting to use the terms safe city and smart city interchangeably, Armand Steffens, Milestone Systems’ country manager for the African continent (except Northwest Africa), believes a distinction should be made at the outset. “A smart city is not necessarily safe, nor is a safe city smart in the sense of intelligence,” he opines. “For us, a smart city is an urban area that uses diverse types of electronic data collection and sensors to supply information used to manage assets and resources efficiently.

“The smart city concept integrates information and communication technology (ICT), and various physical devices connected to the network (the Internet of things or IoT) to optimise the efficiency of city operations and services and connect to citizens. Smart city technology allows city officials to interact directly with both community and city infrastructure and to monitor what is happening in the city and how it is evolving.”

By contrast, he describes a safe city as an urban area where the citizens experience a low to zero number of safety incidents. “If a smart city can reduce the number of incidents, then this is a positive effect of an intelligent infrastructure,” he says.

Digging deeper into the communication fundamentals required, Steffens describes a smart city as “basically a very large IT infrastructure – and an IT infrastructure is an IT infrastructure, no matter the size of it. The same principles of connectivity, interoperability, security and scalability apply no matter the size. Then there is data flow, where strict governance rules have to be in place to ensure that the needed data is available for performing each different task within a secure context. Cybersecurity has to be an important part of any smart city project, as well as privacy and data governance.”

“We have all the technology needed to be made available and shared across agencies and departments. And with communities and people across the city. For example, Huawei’s technology is able to create a layered segment specifically for public safety, and employ bandwidth optimisation so that a drastic forklift upgrade is not always necessary. We also have the capability to put in place an integrated platform that can function as the heart for bridging diverse communication channels such as landline, voice, video, data, mobile and two-way radio, to name a few, and to use these capabilities across a wide range of different terminals and devices, including apps to facilitate services to the community.”

No matter the extent of the programmes and initiatives, Diender asserts that it must

travel guide. Part of this strategy requires the company to look beyond the conventional framework of vertical markets like healthcare and education and the information silos that inevitably result, and rather think horizontally to optimise synergies across application areas.
SECTOR FOCUS: SAFE/SMART CITIES

appropriate – and be connected to city resources such as emergency services and safety and security personnel.

“Five layers of technology culminate in smart cities,” he elaborates. “Sensing and video authentication use radio frequency identification (RFID) and wireless sensor networks across land, sea, air and outer space to provide data concerning all aspects of urban life for advanced authentication. The central platform effectively visualises data, accumulated and used in many scenarios, such as for early detection of earthquakes or bad weather, for example, to enable preparedness throughout the city. Or it can be used to monitor freeways over optical cable sensors and for advanced biometric recognition in which video data is also used. Data acquired through sensing is continuously authenticated by location and condition validity checks.”

It is important that data can be analysed and information reported in real-time when anomalies are detected. Any relevant data, such as video, is relayed along with the anomaly notification where it is needed, in such a way that police will receive security-related data, fire services fire-related data and so on. “This helps prevent crime, prepare first responders for emergency situations so they bring the right equipment, and prevent accidents, among other benefits,” Le Roux says.

“What is more, air conditioning can be monitored and precisely controlled, dustbins can be monitored and removal crews despatched only when necessary, water pipes and taps can be monitored and plumbers alerted when there are leaks, lights can be automatically switched on and off, and bulbs replaced by crews when necessary. Added to this, the cloud can provide backup solutions and widespread geographical and system integration.”

When it comes to the actual communication layers required for such an endeavour, the latest and fastest technologies might be desirable, but reliability is arguably even more important. “Communication layer infrastructures need to be in tune with throughput demands,” says Le Roux. “Existing CCTV can be used, in many cases, for automated, reliable facial recognition by simply adding an intelligent software layer to the central platform, as long as the cameras achieve a certain minimum resolution.

“The same principle is true of all systems, and the networks that connect them all only need to have the throughput capacity to transmit the amount of data they’re being asked to convey. Wi-Fi is a useful endpoint communications technology for all the services, but the more services you layer onto the network and the more IoT devices you connect and the more personnel and their personal devices that are connected, the more bandwidth the backbone will need.”

Examples of smart cities that tend to grab headlines are those with broad CCTV rollouts, but there are many other elements that distinguish a smart city from a ‘dumb’ one. Due to the scale and complexity, there is truly no one-size-fits-all bundle of must-have services, but some of the many components that fall under the smart city umbrella include the likes of fire-fighting command and control systems, smoke detectors, biometrics for public safety access control, video monitoring, citizen IDs, medical services e-records and local healthcare facilities.

They also extend into lifestyles services such as e-learning, hotel bookings, point of sale and e-money, and include infrastructural services such as power storage systems, waste water purification plant information, management and operation, location and availability of rapid charging electric vehicle stations, traffic congestion information systems and telematics. Furthermore, they drill into check-ins at airports, flight information displays, weather predictions, and train monitoring and e-ticketing systems.

A smart city rollout relies on input and expertise across the public and private sectors, but to ensure a consistent vision, Le Roux believes it is important that the city mayor drives the initiative with the view of using technology to make cities safer. “We see this process as a public-private partnership that aims to achieve the goals which the mayor wishes to achieve. It becomes clearer how to resource the project once the mandate is in place,” he states.

To summarise how a city like Johannesburg, Cape Town and others that have aspirations to get on the smart bandwagon should approach such a project, Le Roux advises: “The network is the base step because it links all locations and ultimately services. That’s coupled to the intelligent platform at the centre, to which all systems will connect. Thereafter you roll out services as required, and as budgets allow, based on the city’s most pressing concerns. These are usually focused around safety and security services, monitoring and managing crime, response resources and associated activities and infrastructure. Thereafter additional emergency services are usually added and the full range is rounded out with citizen services and finally additional lifestyle services that improve the standard of living even further.”
Managing future cities

Something new and strange is happening in our cities. The question is: are we ready for it?

Walk through Cape Town’s central business district toward the world-famous V&A Waterfront, and you’ll notice how the lines between city and seashore, residential and commercial, are rapidly blurring. A similar transformation is happening in Jo’burg’s oft-neglected CBD, in the suddenly revitalised districts of Newtown and Maboneng.

Further afield, the trend is shaping how we live, work and play in a new generation of integrated estates and so-called central improvement districts. A visit to Cape Town’s Century City, for example, mixes a hybrid of residential complexes within a fabric of business and commercial premises and one of the largest shopping malls in Africa. Likewise, Johannesburg’s Waterfall Estate is picking up where the sprawl and congestion of Sandton, the city’s ‘unofficial CBD’, left off, bringing together all the amenities the estate’s well-heeled residents could ever need and want without ever leaving the precinct.

Indeed, the mall is becoming somewhat of a dinosaur, an isolated island of commercial activity. Instead, it’s shifting – Transformers-like – to our inner cities, where people traditionally work and increasingly live. With firm policies that seek to reverse apartheid-style town planning in cities like Cape Town, people from all walks of life and income brackets are finding new opportunities to move closer to the cities in which they work, and with that shift comes the need to better manage these communities at every level.

As is often the case, every solution breeds a new problem. Tiaan Janse van Rensburg, commercial director of Cape Town-based software and solutions developer Solution House, says the positives of urban regeneration far outweigh the negatives, especially for previously disadvantaged communities forced to live far from their places of work, but the negatives can’t just be glossed over on the hope that they’ll work themselves out.

“We’re not used to managing our cities in the same way we manage our shopping malls or security estates,” says Janse van Rensburg. “A mall is a closed environment where every aspect of public safety, access, transport, parking, security and maintenance is managed centrally, often by one company. In a city or city district, this multiplicity of services is often managed separately, by different companies, groups and both public and private authorities, each using their own system or software, few of which acknowledge let alone collaborate with each other.

“So typically we end up with a mashup of different services that fail to take advantage of the very real and very present synergies that already exist between them.”

While this is all new to us, South Africa’s future cities lag somewhere behind more developed cities when it comes to urban reintegration.

You wouldn’t expect to find a shopping mall at the heart of New York’s 9-11 memorial district, for example, but in the Oculus – developed by one of the world’s largest shopping mall groups, Westfield – that’s exactly what you’ll see; dozens of stores that function as a hub connecting offices in Brookfield Place and One World Trade Centre with subway lines and trains that serve 50 000 commuters every day. London’s Boxpark and Beijing’s San Li Tun district are similar – albeit structurally very different – concepts.

Ironically, while they might be further down the path of urban enlightenment, they lack the elements of integrated management software like Solution House’s home-grown Incident Desk. Developed specifically to address the needs of integrated communities, Incident Desk merges information from multiple systems into a cohesive, geospatial, real-time management platform that can scale up from one room in one building to entire districts and cities.

“Tiaan Janse van Rensburg, commercial director of Cape Town-based software and solutions developer Solution House, says the positives of urban regeneration far outweigh the negatives, especially for previously disadvantaged communities forced to live far from their places of work, but the negatives can’t just be glossed over on the hope that they’ll work themselves out. We’re not used to managing our cities in the same way we manage our shopping malls or security estates,” says Janse van Rensburg. “A mall is a closed environment where every aspect of public safety, access, transport, parking, security and maintenance is managed centrally, often by one company. In a city or city district, this multiplicity of services is often managed separately, by different companies, groups and both public and private authorities, each using their own system or software, few of which acknowledge let alone collaborate with each other.

“So typically we end up with a mashup of different services that fail to take advantage of the very real and very present synergies that already exist between them.”

While this is all new to us, South Africa’s future cities lag somewhere behind more developed cities when it comes to urban reintegration.

You wouldn’t expect to find a shopping mall at the heart of New York’s 9-11 memorial district, for example, but in the Oculus – developed by one of the world’s largest shopping mall groups, Westfield – that’s exactly what you’ll see; dozens of stores that function as a hub connecting offices in Brookfield Place and One World Trade Centre with subway lines and trains that serve 50 000 commuters every day. London’s Boxpark and Beijing’s San Li Tun district are similar – albeit structurally very different – concepts.

Ironically, while they might be further down the path of urban enlightenment, they lack the elements of integrated management software like Solution House’s home-grown Incident Desk. Developed specifically to address the needs of integrated communities, Incident Desk merges information from multiple systems into a cohesive, geospatial, real-time management platform that can scale up from one room in one building to entire districts and cities.

“If we’re going to push forward and build the cities of the future in South Africa, our services need to match and keep up,” says Janse van Rensburg. “Multi-services – metros, maintenance, buildings, security, crime prevention, vehicle checks – currently exist as separate entities, while our lives do not, which makes it very hard to provide a seamless service in these seamless environments. Service providers simply haven’t adapted as quickly as these multi-tenant environments have developed. If there’s an incident in a public walkway, is that managed by the metro or the private security firm hired to protect the space? Or when a suspect vehicle enters a private space in a public estate, who gets the call?”

Janse van Rensburg believes there needs to be a cultural shift in the vendor environment for integrated urban spaces to really thrive, especially in developing countries like South Africa where communication and collaboration are so often weighed down by bureaucracy. This would necessarily entail keeping data from different vendors safe and hidden behind walls, as prescribed by the Data Protection and Copy Act and the PoPi Act, for example. Management solutions must be able to deal with a certain level of complexity and security, while remaining flexible enough to facilitate the sharing of critical information.

“Much like the residents of our future cities, every service supplier must be able to have their ‘own space’ but also know which of their spaces and activities are shared for the benefit of the community.

“Another aspect we’re actively working on is the ‘third dimension’ of spatial planning and management. Most city districts are managed in a two-dimensional ‘map’ space, but an integrated management system needs to account for the physical structures in the managed district as well – the buildings, for instance. Any solution should therefore be able to move seamlessly from a 2D spatial view to a 3D structural view, without having to switch systems or platforms. It’s a technical challenge we’ve already overcome at many of our client sites in South Africa and the UK, but something that needs more development if it’s going to work on a much larger scale.”

Something new and strange is happening in our cities. Are we ready for it?
Developing a safe city is a major task, especially when one has to build on older infrastructure that was not designed for the communications and interactivity we are capable of today. There is therefore no easy approach to the project, but Gino de Oliviera, Kedacom representative at Forbatt SA advises there are three phases one must deal with on the surveillance front if one wants the project as a whole to succeed over the long term.

Basic infrastructure
De Oliviera says the first step has to be ensuring you have the basic infrastructure in place to support the demands of all the technical components of your safe city. South Africa is generally behind in this area, although we are seeing modern communications technologies like fibre being installed in major cities.

As yet, however, there is a lack of surveillance technology to cover the roads and other public areas in cities. In places where there is good surveillance coverage, many of the cameras and storage solutions are owned and operated by private companies, making it a challenge to centralise information in one place where it can be used to support police and emergency services.

De Oliviera recommends that cameras, no matter who owns them, are linked to a central communications backbone in a grid structure to ensure there is no single point of failure, and to allow for easier management and maintenance.

This could include all the cameras deployed, whether stationary or mobile, and whether linked via wired or wireless communications.

The Kedacom camera range supports a variety of uses, from Starlight bullet or dome cameras for road monitoring, through to the company’s 3 km and 5 km Laser PTZ cameras. These devices can be installed on high points, such as the top of buildings, to allow operators to zoom into areas of interest up to 5 km away with a 60x optical zoom.

The surveillance company also has a tracking system which can be used to identify and track people in open public areas. The solution allows operators to monitor large areas with a limited number of cameras, while the intelligent software allows them to track the movement of a person or vehicle at the same time.

In the mobile space, Kedacom also provides complete solutions, from vehicle PTZ cameras, mobile NVRs, and mobile network options. It also provides body-worn cameras for police and guards patrolling on foot.

Resource integration
Integrating the front end and back end of the safe city seamlessly is critical to the success of the project – including the integration of privately owned cameras. Kedacom’s VMS (video management system) is able to integrate and manage up to 100 000 cameras by cascading and stacking the VMS and storage solutions.

Importantly, De Oliviera notes that the whole system is managed as one platform.

Compatibility issues are dealt with via ONVIF compliance and the company’s analogue-to-IP converter. There is also a third-party gateway that allows for the inclusion of additional products from other manufacturers, as well as a software development kit (SDK) that other companies can use to integrate their products into the Kedacom platform with ease.

Deep application
Once you have your surveillance solution in place, the question arises as to how one is going to deal with all the data collected and ensure operators are only presented with useful information to act on. Kedacom has created dedicated intelligent software and has a range of analytical solutions that have been proven in safe cities around the world. It also has more than 1 600 active developers.

De Oliviera also notes that the company has worked on more than 700 safe cities projects in China. One of these was a project with 100 000 cameras for a province with more than 50 million inhabitants. Another is the Nanning safe city, where cameras are located at 100 metre intervals on the roads.

For more information, contact Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co.
Disaster recovery as a service?

By Johan Scheepers, Commvault systems engineering director for MESAT.

Johan Scheepers talks about the emergence and benefits of disaster recovery as a service (DRaaS).

In the last few years, organisations have started replacing traditional disaster recovery (DR) services with disaster recovery as a service (DRaaS), why?

There are a few benefits that DRaaS offers. Firstly, it assists organisations to reduce costs and relinquish the responsibility of their DR data centre and infrastructure to a service provider. They don’t need to ‘double’ their infrastructure costs in order to replicate a DR site for their data centre. There is no outlay for hardware or software. However, there are other indirect cost benefits such as no cooling, floor space, power costs etc.

Furthermore, DRaaS provides organisations with the flexibility of IT as a utility. For example, if you require more store/compute almost instantly, DRaaS enables this flexibility. With regards to Recovery Time Objective (the time required to restore data or a service after a disaster or disruption) and Recovery Point Objective (how much data am I willing to lose?), this is now determined by the SLA with the service provider, making the process far simpler for the business.

What are the key benefits of DRaaS?

The cost benefit is obvious as well as the fact that they no long require their own infrastructure along with the management responsibilities for the data centre. It must be noted that support staff are still required, but DRaaS takes a lot of the complexity out of DR by having a specialist take care of their DR infrastructure and SLA requirements.

What are some of the features that DRaaS has that traditional DR does not?

DRaaS features a utility model of cloud computing that has a significant impact on a business. It enables companies to scale their store/compute with ease and speed. If we have a look at an in-house data centre scenario, it is far more difficult to quickly increase or decrease store/compute. Servers need to be commissioned, routed through procurement etc. It can sometimes take months to install the server. DRaaS is essentially a ‘pay-as-you-use’ model which is far more economical, not to mention simpler.

You have highlighted the pros to DRaaS however, what are some of the pitfalls in switching to a DRaaS service?

Physical accessibility is the most apparent downside to DRaaS. Your DR resides in a remote data centre, which means a company won’t have access to it. If a particular component needs to be physically accessed, this needs to be routed through the service provider. However, it must be mentioned that this issue is the same for any type of cloud service where data centres are located all over the world. It is also important to conduct due diligence when selecting a service provider as not all are equal. It is vital to ensure they are compliant with data regulations and have security built into the platform. It will serve a company well to establish the classification of the data centre and to read the ‘fine print’.

Do you predict an uptake in DRaaS in the coming year?

Adoption is taking place far more rapidly with smaller and mid-sized businesses. They are more agile and ready to move to a DRaaS model as their IT budgets are far more constrained than those of their larger counterparts and they realise the benefits very quickly.

On the flip side, we are seeing large organisations and groups consolidating their data centres which indicates they may continue to make use of their own DR infrastructure for some time or even indefinitely. In addition, larger organisations and certain verticals such as financial services are more heavily regulated and often have stringent requirements which compel them to retain their own DR sites rather than making use of the DRaaS model.

There are some organisations, however, that are and will consider the hybrid model whereby certain elements of their data for DR purposes will be stored in country and on premise, such as financial data. This is required by SARS. However, other data that is not sensitive may make use of the DRaaS model such as production systems/data.

We will also see Applications as a Service (AaaS) driving the uptake of DRaaS. Companies that offer AaaS will naturally have to offer DRaaS as part of their AaaS offering. In general, we will see an uptake in 2018 of DRaaS.

For more information contact Commvault, www.commvault.com.
Mining and manufacturing sectors are becoming increasingly vulnerable to cyber attack. This is highlighted in Dimension Data’s Global Threat Intelligence Report for 2017, where it was revealed that the manufacturing sector was second only to the finance industry on the list of most attacked sectors in the Middle East and Africa region in 2016.

In fact, manufacturing featured amongst the top three targets for five out of the six global regions. Sectors like mining and manufacturing are fast becoming a favourite with cyber criminals and it’s not difficult to see why. Most manufacturing systems today were made to be productive, with funds traditionally spent on upgrades for productivity rather than cybersecurity.

OT environments are at risk
Taking a closer look, mining and manufacturing plants are run by operational technology (OT) which controls the physical devices within the plant. These environments are generally operated by the engineering function, independent of the enterprise network run by IT in the organisation. This is problematic because historically manufacturers have not been security focused. To complicate matters further, most operational technology was introduced 20 or 30 years ago when there was little risk of a cyber attack.

The result is that the necessary IT systems to prevent cyber attacks simply weren’t put in place. This includes failing to introduce measures to authenticate the traffic between the various devices contained in the plant and the logical security application of segmenting networks. This threat to the OT environment is being exacerbated by the proliferation of the Internet of Things (IoT). With digital transformation on the rise, organisations are deploying applications and devices that interact with business operations to enhance business outcomes.

For mining and manufacturing this means connecting IT and OT systems securely into one enterprise network to enable boundless information flow for real-time, informed decisions. The move from isolated devices to Internet-enabled platforms that can communicate with each other creates entirely new cybersecurity risks. Critical systems are now exposed and vulnerable to information attacks and Denial of Service (DDoS) attacks.

The consequences can be devastating
It is estimated that by 2020 there will be more than 40 billion devices connected to the Internet. And particularly concerning for South Africa is that 21% of all IoT attacks originated in the MEA region in 2016, according to the Global Threat.

When connecting the digital and physical worlds, new data sources need to be considered as both a source and target of an attack. While in the past cyber attacks have been largely focused on targeting confidentiality of information, we are now seeing a shift towards the availability and security aspect of IT.

This is particularly relevant in the OT environment, where an attack on the technology can bring an organisation to a standstill. Critical services are all controlled via automation and operational technologies, and the impact on their availability has an adverse effect on consumers of these services. For example, if the power grid should be made unavailable because of a cyber attack, electricity would become unavailable to all consumers, ultimately impacting the economy of the country.

This requires a new approach to securing OT environments. A consultation process is needed to understand what the impact on the business would be should its OT environment come under attack as well as the cybersecurity requirements to prevent attacks. These requirements include the discovery of elements that form part of the OT network, build and design based on security principles, controls for segregation, monitoring, access control and endpoint protection.

Penetration tests should also be run to uncover cybersecurity gaps, allowing for advice on technical solutions to cover those gaps, and assisting manufacturers to implement controls to manage their entire IT security. It is critical that OT form part of an overall enterprise cybersecurity strategy. This will enable manufacturing organisations to take advantage of the benefits of the digital era, while still ensuring that they have invested in the required measures to protect their OT environment from becoming the soft target of a cybersecurity attack.
Availability in the age of security risk

By Claude Schuck, regional manager for Africa at Veeam.

Six out of seven organisations lack a high level of confidence in their ability to reliably protect and recover data within their virtual environments.

With ransomware attacks becoming increasingly prevalent, companies are more aware than ever for the need for effective cybersecurity measures. But despite this, not enough is being done to ensure the availability of data in the event of systems being compromised.

Enterprises are spending millions on disaster recovery (DR) and business continuity (BC) strategies but they do not invoke them nearly enough for the investment to be measured accurately. In fact, the 2017 Veeam Availability Report makes for sobering reading around the impact that security risks could have on availability.

The report has found that six out of seven organisations lack a high level of confidence in their ability to reliably protect and recover data within their virtual environments. To make matters worse, 85% of respondents rated themselves less than very confident in the current capabilities of their organisations regarding virtual machine backup and recovery. With virtualisation being part of the foundation of every modern IT environment, including on-premise and cloud-hosted, any response other than ‘very confident’ is unacceptable.

Think differently

Clearly, the old way of looking at DR and BC is still too complex. It needs to be simplified if organisations have any chance of effectively implementing these plans in the event of a disaster. One of the best ways to ensure that this happens is by conducting regular tests. This will provide real insight into how easy it is to manage (and recover) data in times of crisis and what the impact of non-availability could potentially be.

It will also show executives in a realistic manner, the amount of downtime the business can tolerate from its high-priority applications compared to those that are not as time-sensitive. According to the report, the median tolerable downtime among high-priority applications is 7.5 minutes. For normal applications this window opens to 90 minutes. So, ask yourself just how quickly you can access your mission-critical data. Realistically, anything longer than 20 minutes could spell potential disaster for the enterprise.

In this environment, it is still crucial to ensure good cybersecurity measures are put in place to mitigate the risk of any potential attacks. The problem is that many decision-makers equate this to simply installing the latest anti-virus software. Unfortunately, viruses and malicious software have evolved and need to be addressed differently. As with any security concern, the biggest threat often comes from the employees of a company. From disgruntled users to unsuspecting people clicking on suspicious links, a company must make sure that it provides the right level of data access to the various employees in the business.

Addressing security concerns

This is not only something that happens amongst private sector organisations. Governments must be aware of the risks that not effectively securing their data and testing their DR and BC strategies could have on operations. The impact could be significant not only in the running of a department, but also the operations of a country.

In South Africa, most public sector departments still store their data on legacy applications. In recent years, the government has started migrating to more centralised systems in an effort to improve accessibility of data and minimise the ‘sprawl’ occurring in their server architecture and information systems. However, they still need to ensure that availability remains the priority during the shift (just as with private sector organisations). Ultimately, DR, BC and cybersecurity policies should not just be about a tick box approach. Instead, these need to be regularly tested (more than just once or twice per year). Many of these availability tests happen in either a simulated environment, over weekends or at night when there is not a peak load on the systems.

Disaster can strike at any time. It is therefore imperative to conduct testing during peak load times to experience first-hand what will happen in the event of a disaster. This requires a different way of thinking and one that executives in the digital world need to start embracing.

As is evident by the report, the significance of not having access to data when it matters most could potentially result in a company having to close its doors.

For more information, contact Veeam, www.veeam.com.
Planning for the unexpected

SA organisations must factor natural disaster into business continuity planning.

The recent floods highlight the fact that South Africa is vulnerable to its own set of natural disasters with the potential to disrupt businesses quite substantially. Flooding is a periodic danger in many parts of the country, including Gauteng and the Western Cape, while other natural disasters like water shortages owing to drought, wind and hail damage must be factored into sustainability planning, says Cindy Bodenstein, marketing manager of ContinuitySA.

“Compared to many other parts of the world, South Africa does have a relatively benign climate, but disasters do occur and can have devastating effects on businesses, as the recent floods have reminded us,” she says. “Even a fairly localised climatic event can put an unprepared company out of business; responsible companies and their boards must factor natural disasters into their scenario planning to ensure staff safety in the event of a natural disaster, but also to ensure that the business has robust contingency plans to recover as quickly as possible.”

Bodenstein also says that local companies must not forget that they are increasingly part of global supply chains, and so are affected by the impact of natural disasters elsewhere. For example, the tsunami that hit Japan in 2011 did not only devastate that country, it meant that many Japanese factories could not supply components needed in international supply chains, automotive and electronics companies were particularly hard hit. The massive hurricanes in the United States this year have affected certain supply chains as well.

Planning an emergency response to a flood, hurricane or similar event is obviously critical, but it is even more important that companies factor natural disasters into a comprehensive business continuity management plan.

“Business continuity management is a much more comprehensive process that aims to identify and prioritise risks in terms of their potential impact on business processes, and put mitigation and recovery strategies in place,” she says. “Coping with the disaster is just the start, you have to know how to get the business back up and running in the shortest time possible, and only business continuity management can do that.”

For more information contact ContinuitySA, +27 (0) 11 554 8050, cindy.bodenstein@continuitysa.co.za, www.continuitysa.co.za.
Many fears abound around the use of X-ray technology and similar body scanning equipment used to enhance security in high-risk areas. Hi-Tech Security Solutions discusses the truth behind the technology and how it can minimise theft and security risks.

It is important to differentiate between medical X-rays and X-ray technology used to scan people in airports, ports and in the workplace. Medical X-rays are high-frequency (beyond ultraviolet) radiation, typically on a wavelength of a few ångströms, allowing them to penetrate just about anything but bone/minerals and metals. (Source: biology.stackexchange.com)

Security scanners, on the other hand, emit terahertz radiation, which has a wavelength between microwave and infrared. This is a very low level of energy per photon. Terahertz radiation will not penetrate more than a centimetre of light material, allowing one to find hidden metal objects which reflect terawaves. The intensity of the radiation is relatively low since these scans are also detected by digital cameras, which are quite sensitive. According to the American Association of Physicists in Medicine, the radiation exposure from full body airport scanners is equivalent to what an individual receives every 1.8 minutes on the ground from natural background radiation or equivalent to every 12 seconds during an aeroplane flight. (Source: biology.stackexchange.com)

Security scanners, on the other hand, emit terahertz radiation, which has a wavelength between microwave and infrared. This is a very low level of energy per photon. Terahertz radiation will not penetrate more than a centimetre of light material, allowing one to find hidden metal objects which reflect terawaves. The intensity of the radiation is relatively low since these scans are also detected by digital cameras, which are quite sensitive. According to the American Association of Physicists in Medicine, the radiation exposure from full body airport scanners is equivalent to what an individual receives every 1.8 minutes on the ground from natural background radiation or equivalent to every 12 seconds during an aeroplane flight. (Source: biology.stackexchange.com)

Neil Cameron of Johnson Controls says that while the risks of radiation exposure are greatly reduced in people passing through security scanners, it is necessary that users adhere to the Public Health Amendment Act, 1971 (Act 42 OF 1971) published by the National Department of Health.

X-ray scanners, he says are ideal to allow organisations to control, maintain and access validated data of the people passing through the scanner.

He cautions that the provider of X-ray scanning technology needs to be certified to measure dosage of radiation and is required to keep a secure database of each person’s transactions through the system as well as their dosage exposure. Sensors inside the X-ray cabinet measure radiation for each person as they pass through the scanner and the machine maintains a cumulative record of this data.

Maximum exposure

“The Johnson Controls’ system carefully analyses the frequency at which the person is passing through in order to ensure that they do not reach the maximum dosage exposure. In a number of instances, employees have tried to beat the system by repeatedly passing through the machine in a short space of time. In this way, they force the machine to issue an alert that results in the person not having to pass through the machine on their next entry or exit at the premises.

“The machines are now configured in such a way that employees will pass through the scanner during a randomly selected dummy scan operation. In other words, the X-rays are deactivated for that particular pass, without the employee having any knowledge of this. In this way, they do not exceed the upper limit of exposure, but they believe that they are being reviewed on each pass through the scanner,” says Cameron.

Security X-ray scanners are able to detect any substance that is harder than skin, with a definable shape, such as weapons, platinum, diamonds and other high-value, small quantity products. The scanner takes an initial sample scan of a person, which is stored in the system for future comparison against subsequent scans. Future scans will highlight areas of change, allowing security personnel to further investigate and, for instance, order a more thorough body search in a closed environment.

Continued on page 40
INNOVATIVE X-RAY SECURITY SCREENING

CONPASS MIP
MOBILE SCREENING AT ANY DESIRED LOCATION

CONPASS
PERSONAL INSPECTION SOLUTIONS

PARCELS, BAGGAGE AND PALLETIZED CARGO INSPECTION
50X30 • 60X45 • 60X80 • 100X100 • 160X165 • 160X180

OCCUPIED VEHICLES AND CARGO INSPECTION
DTP 200LV • DTP 7500LVR

info@adanisystems.com
www.adanisystems.com
Johnson’s low-dosage scatter scan is able to provide a high-definition digital format image of very small particles, making it ideal for use in the mining environment as well as in prisons. The X-ray system identifies areas of difference on people passing through the scanner but the machine does require human intervention when differences are detected. The person is then placed in a holding room until the operator has reviewed the scan to identify whether a search is required and on which body part the foreign object is suspected to be.

“To put employees at ease, male employees are viewed on the X-ray machine and searched, if necessary, only by male security officers, while female employees are scanned/searched by female security officers,” Cameron points out.

Wave goodbye to X-ray
Jayne Nel of Vantage MDT says that the Milliwave Full Body Security Scanner they provide employs millimetre wave technology that enables quick and automatic detection of potentially dangerous items in a non-invasive and sensitive manner. The technology, which originated for the aviation industry, was developed specifically to bypass the privacy and health issues around X-rays.

Millimetre wave (mmw) scanners produce detailed full-body images of people, using ultrahigh-frequency millimeter wave radiation rather than X-rays. Millimetre wave scanners produce a special type of microwave with wavelengths that fall in a range exactly between 0.001 metres (1 millimetre) and 0.01 metres (10 millimetres). In other words, the waves emitted by mmw scanners are much larger and therefore have less impact on small structures, such as human proteins and nucleic acids. (Source: science.howstuffworks.com)

The Milliwave Full Body Security Scanner uses automated target recognition (ATR) software that renders every subject as a generic outline, with suspicious areas highlighted. It will display the words ‘pass’, ‘inadequate’ or ‘fail’, depending on whether it detects a foreign object or not. Operators are necessary to physically operate the machine but they do not become involved in the actual detection process.

For privacy reasons, the operator sees a generic body shape (avatar) on the screen which is highlighted with a red mark on a specific body area that requires further investigation by security officers.

Subject to the stringent health regulations of the TSA (USA) and ECAC (Europe), these scanners work on the following principle:

Continued from page 38

the machine sends millimetre waves in short succession which reflect off the skin surface. The detection software uses machine-trained algorithms to search for anomalies that would indicate unusual objects of all material types, rather than looking for specific items.

“Because it passes aviation standards, it has been through rigorous testing and is therefore an attractive option for other sectors including mining, manufacturing and distribution. Due to the fact that it does not pose a health risk, it can be used to scan staff on a daily basis. A further benefit is that scans take only 32 milliseconds, meaning that high throughputs of personnel are quickly achieved, resulting in minimal disruption,” Nel points out.
X-RAY SCANNING & BODY & ASSET SCANNING SYSTEMS

Dual energy X-ray inspection system

Inspection control evolved much over the past few years. ZKTeco has sold numerous access control, entrance control and inspection control solutions that catered for standalone and small to medium-size installations.

The beginning of 2017 saw the launch of the dual energy X-ray inspection system which now offers ZKTeco the opportunity to compete head-to-head with some of the big names in the global market, but at a much lower price point. The ZKX6550 X-ray inspection system increases the operator’s ability to identify potential threats. The device is designed to scan briefcases, carry-on baggage, small cargo parcels. It uses a reliable high-quality dual energy X-ray generator that produces an image that allows operators to identify potential threat items visually.

The ZKX6550 has innovative biometric identify function for operators, improving the security of system and preventing operators from forgetting passwords. With an ergonomic modern design, the system could help operators to identify suspicious items fast and accurately. It offers higher wire resolution with a Hamamatsu X-ray detector, true-colour scanning image, fingerprint identification and is widely usable for carry-on baggage.

A standard inspection system comes with fingerprint console board, console desk and bidirectional scan. The product also sports an energy saving mode, a video surveillance system and an electrical weighing system.

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

Xscann Technologies is an innovative company that has been operating within South Africa for several years and is responsible for the development of state-of-the-art body scanner solutions that are in operation throughout Africa and the rest of the world. By utilising the cutting-edge technology offered by Xscann, companies eliminate the usual problems associated with conventional body searching methods and send a message of zero tolerance to potential smugglers. For customers who place importance on the prevention of smuggling of precious metals and gems, the Full Body Scanner is an essential security tool.

The new machine offers outstanding image quality of the entire body with high image resolution and a flicker free display making it an effective tool for the detection of:
1. Precious stones – including diamonds
2. Precious metals
3. Objects concealed Internally or externally
4. Contraband and threat detection (weapons, explosives, narcotics, etc.)

Dual view X-ray Body scanner (BS16HR-DV)

Contact details:
6 Guernsey Drive, Longmeadow East; Edenvale
Tel: +27 011 608 1504
Fax: +27 011 608 1570
Email: info@xscann.com
charl@xrdscreening.com
rudzani@xscann.com
Web: www.xscann.com
www.xrdscreening.com
www.smithsdetection.com

Major Installations (Over 30 completed projects):
- Diamonds industry: Petra diamonds – 2 units, Letseng diamonds mine (Lesotho) – 1 unit, Koe diamonds mine (Lesotho) – 1 unit, Limpopo diamonds mine (Lesotho) – 1 unit, Alexkor – 2 units
- Gold Industry: Sibanye Gold – 2 units, Rand Refinery – 2 units, Harmony Gold – 2 units
- Platinum industry: Impala Platinum – 5 units, Anglo American (PMP) – 5 units, Lonmin – 6 units, Heineus SA – 1 unit, Tafanani one (Tanzania) – 2 units
Danish scanning customs

Danish customs choose Adani CONPASS MIP mobile body screening solution.

Adani has been chosen as a supplier of the mobile X-ray body screening solution for the Danish Customs Service, SKAT. Adani working together with NORAD A/S, Denmark and Hartmann GmbH, Germany have been awarded a contract to design, develop and supply the CONPASS MIP mobile full body security screening system to cover the needs of the Danish Customs Service in screening of potential drug smugglers, attempting to import illicit substances into Denmark.

Leonid Zelenkevich, international sales and marketing director of Adani says, “We have worked with the technical and commercial teams at NORAD A/S and Hartmann GmbH to develop a fully custom-made mobile X-ray body scanning solution that will satisfy the end user need and provide them with another effective and extremely flexible tool for prevention of illegal drug import into the country.”

The demand for more complete personnel screening systems is increasing in many key markets as a result of a mixture of events and the realisation by the enforcement agencies that the technology exists to safely screen for a wide range of banned and dangerous items. The Adani CONPASS product line has demonstrated that its robust design, high performance and flexibility has proven popular with an increasing range of international customers.

Hardy Vinter, senior customs adviser of NORAD A/S adds, “The key to winning this contract is a combination of the knowledge NORAD has to the Danish end user operations, effective cooperation with Adani during the tendering process and not least a quality product that provides the best image quality in the market.”

Patrick Keller, sales manager of Hartmann GmbH says, “With the excellent knowledge of our engineers, we combine high-quality scanning-equipment with long-term vehicle integration technology into a specified mobile scanner solution – we are sure this product creates new opportunities for the mobile security market.”

For more information, contact Adani, +375 17 349 0039, info@adanisystems.com, www.adanisystems.com.

Head to toe scanned image

For customers who place importance on the prevention of smuggling of precious metals and gems, the full body scanner is an essential security tool. Xscann Technologies' system offers image quality of the entire body with high image resolution and a flicker free display making it an effective tool for the detection of:

1. Precious stones – including diamonds,
2. Precious metals,
3. Objects concealed internally or externally, and
4. Contraband and threat detection (weapons, explosives, narcotics, etc).

Xscann Technologies boasts an in-house developed X-ray Management Software (XMS) solution that includes: once-off software licensing, matrix configuration for gender segregation, various access control integration (e.g. Babylon, Impro, Opto, etc.), algorithm to ensure that personnel will not be subject to radiation exceeding 1mSv per annum, logging of personnel radiation data for archiving, and a reports generator.

XMS reporting includes X-ray totals by radiation, X-ray totals by name, over-quota individuals, excessive entries, excessive dummy scans, excessive holds, scan logs, search logs, etc.

For more information contact Xscann Technologies, 0861 972 266, info@xscann.com, www.xscann.com.
ExSite enhanced cameras

Engineered and designed to survive harsh conditions, Pelco’s ExSite Enhanced Cameras are a comprehensive solution for the oil and gas industry. The Pelco ExSite Series is comprised of fixed and PTZ, explosion-proof IP cameras designed to meet the rigorous requirements for the hazardous locations such as the oil and gas industry.

Pelco ExSite cameras are virtually indestructible with a robotically welded housing, and a direct drive positioning system devoid of belts, gears and pulleys for use in extreme weather conditions. This minimises ongoing maintenance, thus reducing maintenance costs. The direct drive positioning system is extremely fast and accurate and can hold position in high winds up to a category 3 hurricane.

In recent years, real-time video surveillance solutions have become the standard for securing oil and gas facilities, chemical plants, manufacturing and marine facilities and numerous other demanding environments. The ExSite cameras feature a 1080p, 30X integrated optics package, multiple compression formats, and both upright and inverted operation to improve image quality and reliability with variable lighting conditions.

From their indestructible design and low-light technology to their multiple compression formats, ExSite Enhanced HD cameras improve overall safety, operations, and security by ensuring high-quality video across the enterprise.

For more information contact Yvette Venter, Pelco by Schneider Electric, +27 (0)11 254 6400, yvette.venter@schneider-electric.com.

Avigilon Appearance Search

Avigilon Appearance Search video analytics technology is a sophisticated deep learning artificial intelligence (AI) search engine for video. It sorts through hours of footage with ease, to quickly locate a specific person or vehicle of interest across an entire site.

Avigilon Appearance Search technology can dramatically improve incident response time and enhance forensic investigations by allowing operators to build robust video evidence and create a powerful narrative of events.

Its search capabilities now incorporate the characteristics of a person’s face, as well as shape, size, texture, colour, clothing and accessories when searching for a person. Adding faces to Avigilon Appearance Search technology increases speed and accuracy by using the unique combined features of a face based on hair colour, texture and other facial features and accessories, enabling the technology to understand that it is searching for the same person, even if items such as their clothing change over time.

The quick search capabilities of Avigilon Appearance Search technology enable operators to scan vast amounts of recorded footage, efficiently grouping video data to help track a person’s or vehicle’s route, identify a previous and last-known location, and assist investigations.

Avigilon Appearance Search technology works with Avigilon video analytics cameras to generate, record and classify video data for effective searches. Integration with ACC software provides advanced video search capabilities to enhance the user experience of the entire Avigilon solution.

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

Suprema FaceStation 2

FaceStation 2 is Suprema’s flagship face recognition device for access control and time and attendance. It accommodates up to 30 000 users on a single device, so it easily caters for sites large or small, and it’s loaded with Suprema’s latest face recognition technology, so you can expect fast matching speeds of up to 3 000 matches per second with accuracy, including built-in countermeasures for fake face threats.

In FaceStation 2 Suprema has combined cutting-edge technology with its advanced proprietary algorithms. A dual camera system is used to capture both visible and IR images which are then processed using advanced image analysis techniques and intelligent machine learning based classifiers, allowing a fake face to be detected by estimating specific features and their distribution compared with reference models of real faces.

One of the highlights of FaceStation 2 is its ability to overcome interference from dynamic lighting conditions, including sunlight and ambient light, enabling it to operate in lighting conditions between zero lux to 25 000 lux which covers day and night and basically includes total darkness to bright light, but excludes direct sunlight.

An optional tilt-bracket, which allows for a greater height range of 145 cm to 210 cm, is available for sites that provide for wheelchair users and children.

In terms of usability, near-zero training is required, for both users and system administrators, to operate the FaceStation 2. Using the latest Android 5.0 OS and featuring visual elements of material design concept, FaceStation 2’s wide touchscreen LCD delivers an intuitive graphic user interface that is extremely easy to use.

For RF card support, FaceStation 2 incorporates dual-frequency, multi-card reading technology. The device features both LF (125 kHz) and HF (13.56 MHz) RFID and reads most types of RFID card standards with a single device including MIFARE, HID iCLASS, DESFire, FeliCa, HID Prox, EM and NFC. For the first time in face terminals, FaceStation 2 also supports authentication by BLE (Bluetooth Low Energy) which makes it a future-proof investment for today’s evolving credential technology.

For more information contact Suprema +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za.
Fingerprint recognition has been around for quite a while and is used for many different reasons, but security and identity confirmation are technology’s main purpose. Using biometric systems such as fingerprint readers can greatly increase the security of your electronic devices, including your personal computer, company computers and the priceless data on your devices. If you are concerned about the security of your company, a fingerprint reader may provide the secure, convenient protection you need.

The FV18 is a multi-biometric reader capable of capturing and processing finger vein and fingerprint biometric data at the same time. The new hardware platform uses ZMM220 core-board with 1.2 GHz CPU. With optimisation of both hardware platform and algorithm, FV18 is one of high recognition rate, high security and high-speed terminal. The device offers flexibility of both standalone installation and installation with any thirdparty access control panels which support standard Wiegand signal.

It features a webserver (optional), anti-pass back, access control interface for third-party electric locks, door sensors, exit button, alarm and doorbell, highly accurate finger vein recognition technology and new firmware.

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

Solar LED lanterns

Magnet now distributes new portable Mobiya solar LED lanterns, which have been designed by Schneider Electric as a convenient, safe and reliable source of energy-efficient lighting.

Mobiya TS 170S off-grid portable solar LED lanterns consist of a solar panel and an integrated mobile phone charging facility, with a USB cable with five adaptors.

“This compact, user friendly lighting system is particularly well suited for use in off-grid households, small shops and for street vendors. Mobiya solar lanterns are also effective in power outages, emergency situations, vehicle or machine breakdowns, as well as for outdoor activities, like camping, fishing and entertaining,” says Brian Howarth, managing director, the Magnet Group. “Apart from the convenience of having uniform lighting available exactly where and when its needed, these lamps are equipped with a handy mobile phone charger, with USB ports, enabling users to charge mobile phones any time, at no cost.

“These environmentally friendly lanterns do not generate noise or emissions and can be hand carried, even by children. Robust Mobiya lanterns are drop impact resistant from a height of 1.5 m and water resistant up to 0.5 m for 1 hour.”

The Mobiya LED TS170S lantern has three level settings which provide 48 hours of light at 20 Lumens output, 12 hours of light at 85 Lumens and six hours of light at maximum 170 Lumens.

An advanced Lithium Ferro Phosphate (LiFePO4) battery, with a 1 500 cycle, three-year life span, is charged efficiently through the solar panel, with micro-controller based charge control to prevent over charge and deep discharge.

For more information, contact Magnet, +27 (0)31 274 1998, samantham@magnetgroup.co.za, www.magnetgroup.co.za.

4 MP network camera

The M31 4 MP video surveillance with built-in IR illumination, is an affordable, discreet fixed mini dome with a flat-faced design that suppresses reflections. Using WDR technology and IR illumination, it provides compact HDTV surveillance even in challenging light conditions or total darkness. The M31 provides users with multiple, individually configurable streams in H.264, H.265 and Motion JPEG.

The smart design allows for easy repainting, or using the optional black accessory casing to blend the camera into its environment. Axis Zipstream technology reduces bandwidth and storage requirements. It is also IP42 water and dust resistant. A variety of accessories are available for flexible and easy installation.

For more information contact Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com.
Penta-brid video from Dahua

Dahua Technology has released the XVR. Equipped with the intelligent functions of IVS and face detection, XVR records and analyses tripwire, intrusion and disappearance from images. In addition, these intelligent functions meet with the application requirements of high efficiency and intelligence. XVR combines the simplicity of analogue systems and rich camera selections to achieve simple installation and easy operation. Significant saving in total cost of system is achieved by ease of installation and reuse of existing coaxial cabling. Therefore, it is ideal for a wide range of applications such as public safety, retail store, transportation, stadium, recreation centre, home surveillance and education, etc.

There are various models available:
- XVR41/4200 Series 720p: 720p real-time recording, HDCVI/AHD/TVI/CVBS self-adaptive plug and play, up to 6 TB capacity for each SATA drive.

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

BioStar 2 Mobile Card

Suprema BioStar 2 Mobile Card is an application for storing Personally Identifiable Information (PII) in the user's own smartphone, enabling organisations to support the needs of mobile credential solutions for access control.

Imagine you need to issue access cards to hundreds or thousands of employees and manage your access cards for visitors. Taking all of the cost of buying raw cards, the cost of printing access cards, and the cost of managing them together will be time consuming and costly. Imagine, however, using BioStar 2 and the BioStar 2 Mobile app to issue mobile cards that store biometric information and access privileges to employees and issue mobile cards for visitors to use for a specified period of time. You will be able to operate the system at a much more convenient and economical cost.

BioStar 2 Mobile Card supports BLE (Bluetooth Low Energy) and NFC (Near Field Communication) and therefore works with almost every smartphone today. There is no need for third-party portal services and readers.

Suprema's BioStar 2 mobile card can be issued directly from BioStar 2 or BioStar 2 Mobile app without using portal services like other systems do. In addition, the BioStar 2 Mobile app, which allows you to directly control the functions of BioStar 2 or monitor system logs, is used together to provide users with a unified user experience (UX).

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

XProtect Professional

XProtect Professional+ is the newest video management software offering from Milestone that provides enterprise features at a price point that is mid-market friendly. It provides operators with a long list of features:
- Support for unrestricted number of cameras including H.265 compression, 4K, UHD, and edge storage recording redundancy.
- Management of multiple site locations, centrally or locally via three user interfaces: XProtect Smart Client, Remote Client and Milestone Mobile with Video Push.
- Integration with analytics, access control, laser scanners, geospatial locators, and more.
- Multi-layered maps, full alarm management, and 2-way audio support.

When Milestone works with our technology partners for fully integrated solutions, we provide a detailed software development kit (SDK) with information on our Application Programming Interface (API) so the partners can tie their solutions into ours. This means that the Milestone open architecture, video management software (VMS)

can deliver to end users unique, optimal systems that look and feel like end-to-end solutions – yet offer way more flexibility to change and expand in future.

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

Suprema BioStar 2 Mobile Card

Suprema BioStar 2 Mobile Card is an application for storing Personally Identifiable Information (PII) in the user's own smartphone, enabling organisations to support the needs of mobile credential solutions for access control.

Imagine you need to issue access cards to hundreds or thousands of employees and manage your access cards for visitors. Taking all of the cost of buying raw cards, the cost of printing access cards, and the cost of managing them together will be time consuming and costly. Imagine, however, using BioStar 2 and the BioStar 2 Mobile app to issue mobile cards that store biometric information and access privileges to employees and issue mobile cards for visitors to use for a specified period of time. You will be able to operate the system at a much more convenient and economical cost.

BioStar 2 Mobile Card supports BLE (Bluetooth Low Energy) and NFC (Near Field Communication) and therefore works with almost every smartphone today. There is no need for third-party portal services and readers.

Suprema’s BioStar 2 mobile card can be issued directly from BioStar 2 or BioStar 2 Mobile app without using portal services like other systems do. In addition, the BioStar 2 Mobile app, which allows you to directly control the functions of BioStar 2 or monitor system logs, is used together to provide users with a unified user experience (UX).

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

One of the more eagerly anticipated and most widely welcomed security offering to be included in the 2017 Duxbury Networking portfolio is Sophos Intercept-X, a new-generation, signatureless anti-exploit and anti-ransomware software solution.

According to Ross Anderson, Sophos product development manager at Duxbury Networking, “The Sophos-engineered technology underpinning Intercept-X includes root-cause analytics and advanced malware clean up together with advanced anti-exploit features that block zero-day threats without the need for traditional file scanning. In addition, automated forensic reporting is included in the solution, providing a 360-degree visual analysis of attack events while tracing them back to their origins. It also pinpoints additional infection points, provides advanced clean-up of malware.”

Anderson says a key feature of Sophos’ Intercept-X technology is its ability to hunt for – and eliminate – deeply embedded spyware and lingering malware that have been missed by conventional cybersecurity software and anti-virus systems.

“We expect Sophos and its Intercept-X technology to remain at the forefront of the security industry in 2018 as it clearly understands the threat landscape, changing business needs and customer challenges faced today,” he adds.

For more information contact Duxbury Networking, +27 (0)11 351 9800, llira@duxnet.co.za, www.duxbury.co.za

Portable biometric solutions

There has been an increasing demand for a variety of bespoke portable solutions in most sectors, but in particular for employee and contractor time and attendance (T&A), student rollcall, mustering and visitor management.

A number of software solutions developed by Powell Tronics, used together with recognised portable biometric devices on a wireless network backbone, have provided estates and educational facilities alike with flexible remote-use options. One upside is that installations do not require extensive infrastructure.

The PT-Rollcall application allows for exam management flexibility by using one biometric device for multiple venues. Each session is opened and closed then the device is moved to the next exam venue for opening and closing sessions. The software will only allow students enrolled for that specific exam into the venue; all other non-enrolled people will be disallowed entry. Web reports are available for authorised personnel on request.

Powell Tronics’ ATOM Mobile time and attendance (T&A) application is similarly ideal for remote offline employee enrolments and attendance transactions. The device is connected to the main database via Wi-Fi on return to the main office and then remotely captured data is downloaded for perusal.

Another Powell Tronics portable software development is the mustering application, which is ideal for use during emergency evacuation procedures. The application provides management with a tool that indicates who has entered the premises and if anyone is missing at mustering points. Exact identification of a person’s location on the premises, allows security personnel to search for them and ensure that they are quickly brought to safety.

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

Net2 Entry Touch Panel

Launched in March 2017, the Net2 Entry Touch Panel is the latest addition to Paxton’s video door entry range, Net2 Entry.

Available in three design options, flush mount, surface mount and rain hood, the panel comes with a host of features, including a quality 7-inch colour touch screen and personalisation options, making it suitable for more sites than ever before.

The panel has an IK7 impact protection rating with an easy-to-read anti-glare screen for optimal daytime viewing. The new user interface is simple and straightforward to navigate, offering dynamic search functionality alongside customisable branding options. The touch panel also includes a versatile grouping feature enabling smarter management of multi-tenant buildings and gated perimeter sites, plus SIP compatibility allowing more sites to enjoy the flexibility of answering their door via a SIP-enabled smart device or handset.

For more information, contact Paxton, +27 (0)21 427 6691, support@paxtonaccess.co.za, www.paxtonaccess.co.za.
Forget your keys with Smart Lock

Have you ever forgotten to bring your keys? It is quite a problem if you have no housemate in this situation. No worries, TL400B can help you to solve this problem. ZKTeco’s smart lock TL400B provides various access methods for your convenience, including password, smart card, key and smartphone. For a smartphone, a dedicated APP can be downloaded, thus you can manage and unlock the TL400B without any difficulty. You can also keep track of who enters your home and when it happens. For enhanced security, random passwords for code access are available.

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

Bosch IP Cameras

In today’s dynamic world there is no one-size-fits-all video security solution. There are many situations that call for different types of video security capabilities. With a selection of form factors and features, IP 4000i, 5000i and 6000 cameras are designed to suit many needs. The fixed dome bullet and box cameras offer up to 5 megapixel resolutions, up to 60 frames per second and high dynamic ranges of up to 134 dB, plus Bosch’s starlight technology for low-light scenarios on selected models.

All IP 4000i, IP 5000i and IP 6000 cameras now have Essential Video Analytics on board as standard. This means valuable data can be retrieved quickly from hours of stored video and you are alerted whenever it’s needed, providing improved levels of security 24/7. In addition to advanced intrusion and automatic detection with timely alerts, it enables users to go beyond security and use video data to make more informed business decisions.

For example, gathering business statistics such as counting the number of people entering or leaving the store while securing the main entrance or using video data to help enforce health and safety regulations. Triggering automatic alerts in case the number of people in a queue exceed a certain level to improve service levels, or identifying patterns in customer activity to optimise store layout and improve customer experience and sales.

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

Multi-biometric terminal

PFace202 multi-biometric time & attendance and access control terminal supports up to 600 palm templates, 1 200 face templates, 2 000 fingerprint templates and 10 000 cards (optional). With ZKTeco’s latest hardware platform and ZKFace, ZKFinger, ZKPalmVein algorithm, it offers a new UI and user-friendly operation interface to provide smooth user experience. With advanced palm and face algorithm and multi-biometric verification technology, the terminal’s security level of verification is significantly enhanced. High verification speed. Advanced access control function. Optional built-in battery backup, providing approximately 3 hours of continuous operation.

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

Outdoor camera with IR

The AXIS M2025-LE is a small, bullet-style camera delivering high-quality images in HDTV resolution. It has built-in IR illumination that enables surveillance up to 15 m. The outdoor-ready camera is resistant to rough weather and the integrated sunshield protects against sun and rain.

With a 115° field of view, a single camera gives full surveillance at low cost, and Axis Corridor Format provides efficient monitoring of corridors and shopping aisles. WDR – Forensic Capture increases forensic usability by highlighting details in both dark and well-lit areas. It is IP66 as well as NEMA 4X-rated for reliable outdoor use. The back box enables secure cable management and easy installation.

For more information contact Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com
Intelligent touch screen access terminal

Intuitive touch screen terminal provides intrusion control, legacy/smart modes for backward compatibility.

Johnson Controls has introduced its multi-functional Software House TST-100 Touchscreen Terminal, providing an enhanced end-user experience at the door. With an intuitive touch screen user interface, native intrusion functionality and compatibility with both legacy and IP-based door controllers from Software House, the TST-100 Touchscreen Terminal adds value to the access control system by allowing users to have more flexibility and control at the reader level.

The TST-100 features a large, 4.3-inch graphical LCD touch screen that displays a range of colourful icons and custom command menus, providing end users with quick and easy feedback of the access control operation, and allows guards and other individuals the ability to easily arm and disarm intrusion zones and issue custom commands directly at the door.

Built using the HID Global 5127 Mini multi-technology read head, the Touchscreen Terminal supports a range of highly secure smartcard technologies, including HID iCLASS SE and iCLASS Seos. It uses high-speed encrypted RS-485 for secure communications to an IP controller, making it ideal for healthcare facilities, educational facilities, airports and other critical security environments where network connectivity directly to a reader on the unsecure side is not allowed.

“The TST-100 Touchscreen Terminal hits several targets of multi-functionality, advanced security and ultimate usability all within a sleek, user-friendly touch screen interface,” said Rafael Schrijvers, access control product marketing manager, EMEA, Building Technologies & Solutions, Johnson Controls.

The TST-100 also offers intrusion functionality at the door without the addition of an intrusion interface, allowing end users to view arm/disarm intrusion zones on the device. A command menu provides end users with the ability to issue custom key commands to the intrusion system as well. The reader’s programming includes Johnson Controls’ Reliable Messaging (RM) protocol that facilitates compatibility with any iSTAR door controller.

The Touchscreen Terminal can be added to any Software House platform, including the C•CURE 9000 Security + Event Management system, and can also be integrated with the victor Unified Client. The TST-100 includes the IP-based Ethernet Access Control Door Module (IP-ACM), which when installed near the doors it controls, establishes secure IP, network-based communications with iSTAR door controllers using cyber-secure AES encryption. The Touchscreen Reader’s IP-ACM door module also includes Power-over-Ethernet (POE) capability, helping to lower installation costs.

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

Low voltage circuit breakers

EasyPact CVS is the easy choice for most common electrical distribution applications in medium sized commercial and industrial buildings. This range is both fast to install and easy to use, as well as offering operational safety. Engineered to match common electrical distribution applications, the range delivers exacting design and a focus on scrupulous manufacturing quality to ensure it remains cost-effective over the long run.

Schneider Electric offers the EasyPact CVS range of Class II, moulded case circuit breakers, which are precision engineered to help make installations safer and more reliable. Manufactured from premium materials in ISO 9001 and ISO 14000 certified production plants, the range of circuit breakers are fully tested and certified by national, international and third-party organisations to all relevant safety standards.

EasyPact CVS is the easy choice for most common electrical distribution applications in medium-sized commercial and industrial buildings. This range is both fast to install and easy to use, as well as offering operational safety. Engineered to match common electrical distribution applications, the range delivers exacting design and a focus on scrupulous manufacturing quality to ensure it remains cost-effective over the long run.

The robust circuit breakers are suitable for isolation, guaranteed to the IEC 60947-2 standard, and provide a highly visible and lockable contact position indicator to ensure operator confidence. Earth leakage protection can be added by installing a Vigi CVS option module. In the event of a circuit fault, simple visual indicators help maintenance personnel quickly locate the tripped breaker and take steps to correct the problem.
New Suprema access reader

BioEntry P2 is suitable for both enterprise level access control systems and SMBs.

The latest edition to Suprema’s range, BioEntry P2, packs a full list of features into a slim design to offer a comprehensive access control solution. High matching performance and multi-card reading, this mullion-type fingerprint access control device brings a versatile biometric access solution to the African market, regardless of RFID standards and the size of the projects it covers.

BioEntry P2 is suitable for both enterprise level access control systems and SMBs. It has a large 8 GB memory and can accommodate up to 10 000 users and 1 000 000 event logs. Fast access through doors is reinforced with a powerful 1.0 GHz CPU, allowing BioEntry P2 to achieve matching speeds of up 10 000 matches per second.

The most secure device in its class, BioEntry P2 offers accuracy and significantly reduced false rejection rates. These benefits are achieved by combining the new OP5 fingerprint sensor with Suprema’s enhanced fingerprint algorithm, which compensates for unsatisfactory fingerprint captures such as direct sunlight conditions or distorted fingerprint images.

Dual-frequency, multi-card reading technology enhances the P2’s versatility and flexibility in system design by allowing users to effectively integrate BioEntry P2 into legacy systems as well as to provide users with the capability of adopting new authentication methods into their existing system including RFID, mobile and biometrics. P2 supports all HID multiCLASS compatible RFID standards, it features both LF (125 KHz) and HF (13.56 MHz) RFID and reads most types of RFID card standards with a single device including MIFARE, HID iCLASS, DESFire, FeliCa, HID Prox, EM and NFC.

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

Whether you employ staff or rely on outsourcing, the question is the same: “am I paying for real hours worked?”

While various controls can be employed to regulate attendance, they are often simple to manipulate. Signing on and off duty on behalf of a colleague and recording inflated working hours are two methods which can lead to a loss of profits, excessive overtime pay-outs and reduced productivity.

This widespread problem can be addressed by the simple implementation of an FPX10 biometric device. Historically, the fingerprint recognition of many biometric devices could not consistently positively identify staff members. This resulted in confusion and an often inaccurate recording of time and attendance. This shortfall has been overcome by the FPX10’s advanced 21-point fingerprint recognition, which identifies staff, and records their clocking on and off duty, in real time.

The data is recorded and accessible in real time, owing to the GPS and GSM functionality of the FPX10. The user can access the data remotely, from the dedicated online support platform, at any time of day. From the online portal, the user can control the movements of its staff. Depending on the intended application and site, the user can limit access to various areas to select personnel, and can alter permissions to clock on and off duty between sites – where multiple devices are used across a number of sites.

The technology has been designed to integrate into almost any payroll management system, with the aim to ensure that one only pays for actual hours worked. Additional benefits of this function are that it provides an objective record of attendance, which can be used to resolve disputes regarding pay and as a key document in disciplinary proceedings; and acts as a tool to improve overall staff performance.

The functionality of the FPX10 can be extended by implementing site-specific parameters and alarm conditions. This allows for automated notifications to be sent to the user when a parameter is breached or an alarm event is triggered. These events could include the failure to report for duty, or the late arrival by a staff member. In addition to being brought to the attention of the user in real time, these events are automatically recorded in the user’s payroll management system, ensuring that the employee in question is not paid for the period of his/her absence.

While the benefit of improved control over staff is clear, the FPX10 provides a support and safety element in the form of emergency, medical and fire panic buttons. The panic buttons can be activated by staff at any time, which will notify the user of the distress situation and trigger the necessary assistance.

The device has been designed to suit a vast range of industries. It boasts a rugged casing to withstand the conditions of labour-intensive industries, but is sleek enough to suit to an office environment. The FPX10 is portable, owing to it battery life of up to 72 hours, and can consequently be used in locations without dedicated power supplies.

For more information contact Active Track, +27 (0)11 551 1687, info@activetrack.co.za, www.activetrack.co.za
Network door controller

Scalable IP architecture for smaller security deployments.

Johnson Controls has introduced the iSTAR Ultra LT door controller from Software House, a special edition iSTAR Ultra door controller that provides a full IP architecture and enterprise level features for small to mid-sized access control deployments.

iSTAR Ultra LT centralises all access control decision processing and secures network communications while allowing end users to use existing infrastructure and Power over Ethernet capabilities to reduce costs. With a scalable architecture that includes support for up to eight card readers and 500,000 cardholders, iSTAR Ultra LT is ideal for businesses seeking a flexible, future-proof access control system that can be expanded as needed.

iSTAR Ultra LT’s control module maintains the local access control database and makes all access decisions, centralising access control management for operators. It can be shared with several Ethernet door modules, providing added costs savings. Its advanced encryption and authentication ensure that communications between access controllers and doors are cyber secure, and it also includes a Bluetooth Low Energy (BLE) smartphone application that allows operators to easily configure and manage controllers and locks, lowering commissioning, and saving time and effort.

Said Rafael Schrijvers, access control product marketing manager, EMEA, Building Technologies & Solutions, Johnson Controls, “iSTAR Ultra LT’s enhanced cybersecurity, IP architecture and generous scalability provide our customers with the building blocks they need for the future.”

Similar to iSTAR Ultra, iSTAR Ultra LT combines support for traditional hard-wired access control doors with support for wireless lock sets, all in the same controller. Ultra LT supports both ASSA ABLOY Aperio and Schlage NDE, AD300 and AD400 wireless locks for added flexibility and installation savings and use of the controller’s PoE Plus capabilities lowers installation costs further. It includes two gigabits of memory and 16 gigabits of storage, as well as a single host/database connection for every eight doors.

End users can use iSTAR Ultra LT with the C•CURE 9000 Security and Event Management platform from Software House.

For more information contact Johnson Controls Security Products, +27 (0)82 566 5274, emallett@tycoint.com, www.tycosecurityproducts.com
Documentation for fire systems

By Charles Thiongo, FDIA.

A fire detection system is not considered complete until there is adequate and necessary documentation about the system.

A fire detection system is not considered complete until there is adequate and necessary documentation about the system. Certificates for a system are issued to show compliance and make note of any variations to the standard. The end user, clients representative or purchaser of the system will rely on the certificates to show compliance to regulation and for any insurance requirements.

Before a contractor starts to install a fire detection system there should be an approved design to show where the devices are to be installed, what type of system is to be installed and what interfaces, if any, are to be incorporated into the system. The design should also specify what actions should be taken by the system when a fire is detected to ensure safe evacuation of the people. A design certificate is the first document that needs to be produced before any fire detection system is installed, and accompanying this should be drawings and a document giving details on the system.

After the installation is complete, the installer needs to produce a certificate showing that the system has been installed as per the approved design with regard to the relevant standard, which in South Africa is the current SANS 10139:2012. The installer also needs to produce an as-built drawing and a wiring diagram showing cable routes and where all the devices have been installed. The as-built drawings from the installer also make it easier for the maintenance team when they are carrying out fault finding or maintenance and for future additions or modifications to the system.

A commissioner needs to check and test the system thoroughly before issuing a commissioning certificate. The commissioner needs to confirm that the installation is of an acceptable standard, it has been carried as per the approved design and it complies to the national standard.

The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

When a fire is detected to ensure safe evacuation of the people. A design certificate is the first document that needs to be produced before any fire detection system is installed, and accompanying this should be drawings and a document giving details on the system.

A commissioner needs to check and test the system thoroughly before issuing a commissioning certificate. The commissioner needs to confirm that the installation is of an acceptable standard, it has been carried as per the approved design and it complies to the national standard.

The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.

The following are the other documents that need to be handed to the end user together with the above-mentioned certificates:

• Operation and maintenance manual for the installed system.
• Data sheets for the major devices/equipment in the system.
• As-built and schematic drawings.
• A written record of any deviations or variations from the original design.
• A record of tests that were carried out on the system.
• A log book.

Some end users may require an independent organisation to verify compliance with the recommendations of the SANS 10139 standard in respect of design, installation and commissioning. The organisation that does the verification will issue a verification certificate or a compliance certificate if the installation satisfies the requirements of the standard.

It is possible that one organisation can issue false alarms. The commissioner will test the devices to confirm the correct operation of the system and inspect the installation to ensure there is no obvious potential for an unacceptable rate of false alarms. The commissioner, having inspected and tested the system, assures the end user that the system will function as intended. He also becomes responsible to ensure the correct documentation is handed over to the client.
New Fire Orbs in South Africa

A simple-to-use, cost-effective new fire-extinguishing device is being introduced to the local market by Fire & Security Techniques of Centurion. The FST Fire Orb is a self-activating, portable fire-extinguishing device that activates automatically when in contact with open flames.

The FST Fire Orb is effective for use against all types and classes of fires, from electrical shortages to fat, oil, and paraffin stove fires, vehicle fires, and workshop and factory fires. The FST Fire Orbs can be wall-mounted for maximum effectiveness, explains Fire & Security Techniques’ CEO, Neil Hughes.

Each FST Fire Orb weighs only 1.3 kg, making it lightweight and easy to handle and operate. It consists of a lightweight case of frangible material, with a protective exterior sheathing. The internal cavity contains a pyrotechnic detonator at or near the centre of mass.

It is activated by fuse cords extending to the surface. The device is filled with mono ammonium phosphate, a non-conductive dry chemical powder, which means it can be used on any electrical product without resultant damage. The detonator incorporated in the FST Fire Orb is a small, non-lethal explosive mechanism.

The force of the bursting device is non-harmful to humans, animals, or property, and the effect is minimised further by the use of low-density, low-mass components. This means no part of the device has sufficient mass or density to constitute a ballistic hazard or result in concussive shock.

The FST Fire Orb activates automatically upon direct contact with open flames and not heat. Upon activation, it emits a loud bang of between 119 dB to 138 dB as a warning signal, and disperses the dry chemical powder in order to extinguish the fire. The device is simply rolled or thrown into the fire, whereupon it activates within three to seven seconds.

The FST Fire Orbs have passed tests conducted by the PSB Corporation and Sirim Qas International for Class A, B, and C fires. Additional tests carried out include thermal resistance, burst effect, sound level, compression resistance, and drop tests. The devices are regulated and certified in accordance with ISO 9001:2001. They have also been approved and classified by the South African Police Service.

“We offer a free risk-assessment service for all clients interested in the product, whereby our risk-assessment manager advises suitable installation requirements pertaining to customer specifications,” Hughes highlights.

“The product is far more effective than traditional fire extinguishers, which must be operated manually in order to be effective. In addition, fire extinguishers have no fire-alert activation to warn any bystanders and are bulky devices that weigh 10 kg to 15 kg on average.”

Fire & Security Techniques demonstrated the Fire Orbs at the City of Tshwane’s Winter Awareness Day in the Kopanong Informal Settlement on 14 June. “One of the many applications of the new technology is fire prevention in informal settlements,” Hughes points out.

These not only have a high risk of fires, especially in the cold and dry winter months, but often lack the necessary firefighting equipment and skills. In this regard, the company is also championing its own Fire Heroes programme to promote fire-prevention awareness, and to assist in generating employment opportunities in local communities.

Alarm signal innovation

The QWCD series LED strobe signal light and electronic siren combination is set to make an impact in the market place as a ‘sound with sight’ alarm.

“This is a new concept where a traditional electronic siren is now available with a flashing enclosure. The siren cover lights up like a light globe by using ultra bright LED lights” says Don Smith, technical director of Mimic Components. Not only is it affordable, the many features available on the QWCD series are very useful.

“For example, the MP3/SD card option allows you to create, record and play personalised instructions such evacuation plans or assembly points during an emergency. These messages not only act as powerful instructions during a time of crisis but can also install a sense of calm to workers who could otherwise be panic ridden.”

In operations where noise is an everyday factor and ear-plugs worn to deafen sound, the flashing light is a visual warning solution. The QWCD horn covers are made with a polycarbonate (PC) material, making it highly durable and weather resistant. They are ideal for offshore rigs where machines and waves compete to be heard, and can be used in arctic conditions where temperatures reach -50°C.

The QWCD series is available as emergency vehicle light bars and aviation obstruction lights, in colours red, yellow, green or blue.

For more information contact Mimic Components, +27 (0)11 689 5700, sales@mimic.co.za.
Reducing fire risk

FireClass fire detection selected for three major projects.

After recent successes on tertiary educational facility installations, Sentry Fire and Security in consultation with the technical team at Elvey selected 118 FireClass fire detection systems in various models for three major projects.

The first project was for the factory of a large international tobacco products manufacturer. In this instance, Sentry Fire and Security was appointed to replace the previous technology supplier and determined that faults on the panels were a major cause of concern.

“Just imagine the catastrophic scenario if the threat of a fire was not timeously detected in a tobacco plant. The building would literally go up in smoke in a very short space of time, resulting in huge financial losses and posing a major threat to human life,” says Edward Preston of Sentry Fire and Security.

The client had expressed a need to install a panel that would work with their current devices, so a conventional panel was selected. Apart from the obvious need to protect its assets, proactive fire detection meant that the company could drastically reduce the time taken for the evacuation of personnel.

Two separate projects for the same national retailer involved the upgrading of an existing system as well as the installation of new FireClass technology at a further three stores. In the pre-existing installation, the retailer was becoming increasingly frustrated with an extensive number of false alarms and the inability to silence the alarm once it had been activated. Both of these issues resulted in unnecessary callouts, which were both costly and of irritation to all concerned.

In the new installations, not only was the guarantee of minimal false alarms a major factor, but the client required a system that was user friendly, to ensure that operational staff could respond quickly to issues. Accuracy of identification of actual emergencies is critical and forms the core of the customer’s specifications for a satisfactory fire detection panel installation.

Preston says that the company selected a multi-criteria sensor to detect smoke and heat at one of the new stores. This was necessary because the store makes use of a number of air-conditioning units located in the ceiling void as well as backup generators, which produce smoke in advance of producing heat. The remaining stores were supplied with addressable panels while the tobacco factory selected a conventional panel to replace the previous conventional panel. By retaining the existing conventional devices, together with the new conventional panel, the tobacco products manufacturer is able to conserve capital outlay.

All FireClass panels are linked to the Sentry Fire and Security control room and Preston is personally alerted via SMS of fault conditions and alarms, after which the client is updated. The company performs a two week soak test then shares certificates with the client subsequent to installations being completed. Thereafter, service maintenance is conducted every six months and the client is issued with a service certificate.

Re-evaluating existing fire detection systems forms a critical part of any risk assessment. According to Weslee Davey, fire detection product specialist at Elvey, ensuring that fire detection technology is suited to the application and exhibits reliability and durability over time, forms the crux of fire damage mitigation or elimination.

Preston says that all parameters outlined in the company’s original brief were completely achieved and as a result of the success of the retail projects, further shops will be upgraded to FireClass products. “FireClass products are extremely reliable and this, together with the unparalleled round-the-clock technical support we receive from Elvey, means that our relationship with Elvey and choice of FireClass products as our first option is cemented.”

He adds: “We have used a number of other fire detection products over the years but they have generally been plagued by false alarms, a lack of user friendliness and faults on the panels. We made a shift to the FireClass range of products in 2017 after conducting a careful review of their specifications and capabilities. Our relationship with Elvey is a long-standing one and they were able to advise on the optimal model for each project on which we have deployed the FireClass fire detection technology.”

For more information contact Elvey, +27 (0)11 401 6700, info@elvey.co.za, www.elvey.co.za
Easy-to-use intelligence

TVT’s Intelligent Video Analysis (IVA) provides a set of analytical functions that raise the alarm when certain conditions are met.

The TVT brand of surveillance products is known for its ease of installation and use, but the brand also offers intelligent solutions designed to ensure your surveillance operations deliver reliable service 24x7, even when you’re not watching.

TVT’s Intelligent Video Analysis (IVA) provides a set of analytical functions that raise the alarm when certain conditions are met, alerting users via the NVMS 9000 recording platform, or on TVT’s mobile apps. Vaughn Tempelhoff, from local TVT importer Forbatt SA, explains that when a TVT solution is installed, including the NVMS, recorders and IP cameras, users are able to implement a black-screen approach to surveillance operations, allowing the technology to alert them when an event occurs.

In line with its focus on keeping things simple, TVT offers four basic IVA options for users to choose from.

Object Removal: This intelligent algorithm warns users of missing or abandoned objects. The operator chooses up to four areas on their screen that they want to monitor, for example, a painting on the wall or a computer on a desk. If the monitored object is removed from the stipulated area, an alarm is sounded.

Similarly, the operator can also monitor an area for abandoned objects. If the system detects that something has been left in a monitored area for more than a certain time, it also raises the alarm. This feature could be used to check for illegal parking or for suspicious abandoned packages, for example.

Exception: This algorithm monitors a video stream for changes in the image, such as blurring, colour changes or scene changes, and warns the users as soon as something unexpected is detected.

Line Crossing: Each camera can have up to four ‘lines’ assigned to its image, such as the perimeter of a property. Whenever something crosses a line (a person or a car), the user is alerted and can take action. One can also specify which direction the line must be crossed in order to raise the alarm.

Intrusion: Similar to Line Crossing, this application allows the user to specify an area under observation. Whenever something intrudes into this area, an alert is issued. A shop, for example, could use this to warn if a customer goes behind a counter or into an area where valuable goods are stored.

In all these cases, the alarm is sounded on the NVMS9000 as well as on the user’s mobile. Users can view the footage of the exception on their mobiles from anywhere in the world, as long as they have an Internet connection and the TVT app.

Mobile apps and megapixels

Users who want to keep an eye on their surveillance system while on the move can download TVT’s mobile apps and easily connect them to their NVR. Superlive Pro is the app for iPhone and Android smartphones, while Superlive HD is designed for iPad and Android tablets.

The latest versions of these mobile apps allows users to view their cameras, take snapshots of events of interest, initiate remote playback of events and even control their PTZ cameras. You can even display a multi-channel preview of more than one camera if all you need is to keep an eye on your assets.

Depending on what you want your surveillance solution to watch over, TVT has a range of IP cameras starting at 2 MP resolution and rising to over 5 MP. It also supplies a range of analogue HD cameras, again ranging from two to 5 MP.

For more information, contact Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co
Johnson Controls introduced the VideoEdge 1U network video recorder from American Dynamics, a camera management solution for when simple, low-cost installation and scalable video storage capacity is a priority. The VideoEdge 1U NVR’s 16 embedded software configurable Power-over-Ethernet ports make it ideal for small to medium-sized businesses seeking a quick-to-install, cost-effective video recording option.

The VideoEdge NVR supports as many as 32 IP cameras and stores up to 24 TB of recorded video in a small 1U form factor, enabling small to medium-sized businesses to meet their network growth requirements. With embedded PoE switches, users can expect faster installation times as well as reduced hardware requirements and downtime.

Embedded intelligence allows users to receive multiple video streams for live and recorded video, alarm, and meta-data collection, all tailored to different viewing conditions. The end result is superior video with significantly reduced network bandwidth, CPU resources and memory usage. Multicast video streams further reduce the bandwidth required for streaming high-quality video.

Additionally, users can set up analytics on Illustra cameras and other cameras directly from VideoEdge 1U. The system’s analytics capabilities can gather information for countless business and security needs. When used in retail settings, additional point of sale text integration can be used to identify fraud or track cashier competence as well.

“The value gained by leveraging data from VideoEdge 1U NVR’s analytics not only enhances security applications by tracking behaviours but also by capturing consumer metrics and using it to shape business-critical plans and functions,” said Stuart Bettle, video product marketing manager, EMEA, Building Technologies & Solutions, Johnson Controls. “These benefits come in a unit designed with the smaller user’s need for easy installation and unique requirements in mind.”

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

Reinforcing the benefits of security technology collaboration, Hikvision has announced a Multiple Fisheye Dewarping Solution for Milestone Systems XProtect with Device Pack 9.0 (and later).

The dewarping solution allows Hikvision’s fisheye network cameras to be seamlessly integrated with Milestone’s network video management software, enabling the Milestone Smart Client to display the dewarped images captured by Hikvision fisheye cameras in real-time with no distortion. Recorded video can be retrieved and played back dewarped as well.

With this new solution, Milestone customers will be able to use just a single camera to provide 360° wide-area surveillance coverage without visual blind spots. The solution delivers effective situational awareness and decreases the overall cost of cameras, installation and maintenance.

The dewarping solution further enables access to camera viewing modes such as 180°, 360°, PTZ, PTZ-quad, and horizontal panoramic. Up to 12 different views can be created in the Milestone Smart Client, with the intelligent PTZ view allowing security operators to pan, tilt and zoom through an entire scene.

“As businesses continue to increase situational awareness, 360° cameras stand as one of the strongest areas of growth in the surveillance industry. The integration with Milestone’s XProtect is significant for the market and for our mutual customers to obtain another high performance dewarping solution, tailored to a number of vertical markets, including retail, parking lots, transportation, gaming, campuses and interior building space applications,” said Adler Wu, global technology partner programme manager at Hikvision.

Hikvision fisheye network cameras boast functions such as high-resolution imaging, Ultra WDR, IR illumination, and alarm activation. They offer flexible installation including versatile ceiling, wall and pendant mount options.

For more information contact Janis Roux, Hikvision South Africa, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com
Software defined surveillance

By Franck Martinaux.

Fighting the economic recession by enhancing existing servers and storage.

It is now public information that for any players of the surveillance industry in South Africa (SI, distributors, vendors, etc.), 2017 has been a difficult year. Since the end of the first quarter of the year, the country officially entered an economic recession. An important chunk of the market relies on projects of significant sizes and many of them have been delayed or cancelled. Unfortunately, projections for 2018 and 2019 are not promising at all.

Does that mean the need for security decreases? Not at all, and quite the opposite since statistically crime rates rise in periods of recession, therefore security is more important than ever.

Simply put for the end-users, regardless of their activities, recession means that budgets must be revised, reshuffled to focus on core activities as companies try to limit the damage incurred on their growth. Obviously, security is rarely seen as a productivity tool but more as an optional insurance to increase business resilience. Security related budgets are therefore embedded as part of any business operational routine.

Given that context, and as a member of the surveillance industry, we surely need to approach the problem of budget restriction for security using a disruptive approach.

In a surveillance project, the common rule is that the share for IT equipment (servers and storage) is between 20% to 30% of the investment, if not more. What is less known is that server-class equipment is designed to last between 6 to 10 years where the actual warranty proposed by vendors is usually three years extendable to five years. According to a leading analyst firm’s report, the potential life-span of servers is between 7-10 years (typically 6 years for rack servers and up to 10 years for integrated systems). This is “up to three times longer than the typical replacement cycle for servers and storage arrays.”

Limiting the warranty (and consequently the real life span) to a certain duration is a way to fuel the planned obsolescence and to force end-users to refresh their existing equipment. It is great when the budget to replace out-of-warranty equipment is compatible with the economic context, it becomes more problematic when a chief financial officer (CFO) decides rightly to suspend investment in a surveillance project.

Some economic pioneers are rightly preaching for a circular economy which is an alternative to the traditional linear economy (make, use, dispose) in which resources are kept in use for as long as possible, extracting the maximum value from them whilst in use, then recover and regenerate products and materials at the end of each service life. Such a circular economy is seen as our next economic model in an expected resource scarce world where integrated service-based IT companies will ensure products perform and last longer with an increased customer relationship, thus increased satisfaction.

How can it be implemented for a surveillance project?

There is a very good chance that customers already have a surveillance infrastructure with existing servers and storage in place. These servers could have been stamped as obsolete by VMS (video management system) calculators for lack of CPU power or storage capacity. However, they are an excellent base for building blocks in a hyper-converged infrastructure.

A hyper-converged, or software defined infrastructure focused on surveillance, such as CAPS-OS by Capsule Software, thanks to optimisation of the I/O flow for video streams, offers a gain of performance of between 30% to 40% compared to a native implementation on the same server hardware configuration.

It allows organisations to re-purpose a server by partitioning it into multiple virtual machines with dedicated roles such as access control, asset tracking, LPR and so on. Where storage is concerned, even a 10-year-old storage array either using SAS or SATA drives is still compatible with the latest SATA drives of 8, 10 or 12 terabytes. Coupled with a software-defined storage layer, this legacy storage will perfectly fulfill the needs of the modern surveillance infrastructure in term of performance and data security.

Software-defined storage has been proven to be much more efficient than native hardware storage, and it reduces the number of hardware storage units you need to maintain and replace. Nowadays, the idea of re-purposing an existing IT infrastructure is extremely seducing, completely seamless and possible thanks to software defined infrastructure. Adopting such strategy will increase any business’s resilience, strengthen equipment performance and enable decision-makers to enhance their investments. Entering the circular economy presents many advantages to the surveillance market.

For more information, contact Franck Martinaux, Capsule Technologies, franck@capsule-sa.co.za, www.capsule-sa.co.za
South Africa is a target for cyber attacks

South Africa is currently a magnet for cyberattacks, with hackers set on stealing data.

Following the announcement by large South African data centre operator and website hosting service provider Hetzner, that a key database had been hacked, Maeson Maherry, chief solutions officer for LAWtrust, Africa’s leading cybersecurity firm, says numerous data breaches over the past few weeks show South Africa is a “focus area for cyber attacks”.

The Hetzner breach – which was discovered on Wednesday 1 November, follows the revelation two weeks ago that over 30-million South Africans’ personal information (including property ownership, income and employment history) had been exposed online, in what is considered South Africa’s biggest data breach.

“We are effectively in a Cold War where the goal has become less about disruption and more about stealing data,” Maherry says. He says it is imperative that South African businesses act to protect their data and their brand, and retain customer confidence.

“Businesses have to provide multilayered defences to protect the data and this has to be done in such a way that the information services are still accessible and convenient to customers.”

This means businesses need to put in place strong authentication for all administrators, employees and customers in light of the breaches. Companies also have to encrypt everything, including data in databases, file servers and data in the cloud.

Sophos has announced the latest version of its next-generation Sophos XG Firewall that delivers a breakthrough in network traffic visibility. Using Synchronised Security to obtain information from the endpoint, XG Firewall can identify, classify and allow the control of all previously unknown applications active on the network, such as those which don’t have signatures or are using generic HTTP or HTTPS connections.

Synchronised app control can reduce the security risks associated with unidentified traffic by allowing administrators to see exactly what is on their network.

Synchronised app control will automatically associate discovered applications with appropriate categories where possible and administrators can assign unknown apps to categories that will block or prioritise them as desired. Interactive application reporting provides deep insight into daily traffic activity.

“In a recent study, IT professionals admitted that about 60 percent of network traffic is unknown, and the security risks associated with this tops their list of concerns,” commented Dan Schiappa, senior vice president and general manager of enduser and network security groups at Sophos. “Sophos can identify this traffic because the endpoint knows exactly what applications are running and it can share this data with the firewall through the Sophos Security Heartbeat.”

Sophos XG Firewall is available for on-premise and cloud deployment, on all the major virtualisation platforms as well as through the Microsoft Azure marketplace. Both Sophos Endpoint Protection and the next-generation anti-ransomware solution Intercept X will provide the XG Firewall with the Synchronised Security data required for this new level of traffic identification.

In addition, Sophos has introduced new XG Series hardware appliances that provide a modular system for connectivity with a wide variety of integrated connectivity and FleXi Port modules. The addition of two fail-safe bypass port pairs on-board every 1U appliance and an optional bypass FleXi Port module for all 1U and 2U XG Series models, plus optional Power over Ethernet (PoE) modules make it easy to enable Synchronised Security in any environment.
Ransomware defined 2017

No platform immune from ransomware, according to SophosLabs 2018 Malware Forecast.

Sophos has released its SophosLabs 2018 Malware Forecast, a report that recaps ransomware and other cybersecurity trends based on data collected from Sophos customer computers worldwide during 1 April to 3 October 2017. One key finding shows that while ransomware predominately attacked Windows systems in the last six months, Android, Linux and MacOS platforms were not immune.

“Ransomware has become platform-agnostic. Ransomware mostly targets Windows computers, but this year, SophosLabs saw an increased amount of crypto-attacks on different devices and operating systems used by our customers worldwide,” said Dorka Palotay, SophosLabs security researcher.

The report also tracks ransomware growth patterns, indicating that WannaCry, unleashed in May 2017, was the number one ransomware intercepted from customer computers, dethroning long-time ransomware leader Cerber, which first appeared in early 2016. WannaCry accounted for 45.3 percent of all ransomware tracked through SophosLabs with Cerber accounting for 44.2 percent.

“For the first time we saw ransomware with worm-like characteristics, which contributed to the rapid expansion of WannaCry. This ransomware took advantage of a known Windows vulnerability to infect and spread to computers, making it hard to control,” said Palotay. “Even though our customers are protected against it and WannaCry has tapered off, we still see the threat because of its inherent nature to keep scanning and attacking computers. We’re expecting cyber criminals to build upon this ability to replicate seen in WannaCry and NotPetya, and this is already evident with Bad Rabbit ransomware, which shows many similarities to NotPetya.”

The SophosLabs 2018 Malware Forecast reports on the acute rise and fall of NotPetya, ransomware that wreaked havoc in June 2017. NotPetya was initially distributed through a Ukrainian accounting software package, limiting its geographic impact. It was able to spread via the EternalBlue exploit, just like WannaCry, but because WannaCry had already infected most exposed machines there were few left unpatched and vulnerable. The motive behind NotPetya is still unclear because there were many missteps, cracks and faults with this attack. For instance, the email account that victims needed to contact attackers didn’t work and victims could not decrypt and recover their data.

“NotPetya spiked fast and furiously, and did hurt businesses because it permanently destroyed data on the computers it hit. Luckily, NotPetya stopped almost as fast as it started,” said Palotay. “We suspect the cyber criminals were experimenting or their goal was not ransomware, but something more destructive like a data wiper. Regardless of intention, Sophos strongly advises against paying for ransomware and recommends best practices instead, including backing up data and keeping patches up to date.”

Cerber, sold as a ransomware kit on the Dark Web, remains a dangerous threat. The creators of Cerber continuously update the code and they charge a percentage of the ransom that the “middle-men” attackers receive from victims. Regular new features make Cerber not only an effective attack tool, but perniciously available to cyber criminals. “This Dark Web business model is unfortunately working and similar to a legitimate company is likely funding the ongoing development of Cerber. We can assume the profits are motivating the authors to maintain the code,” said Palotay.

Android ransomware is also attracting cyber criminals. According to SophosLabs analysis, the number of attacks on Sophos customers using Android devices increased almost every month in 2017.

“In September alone, 30.4 percent of malicious Android malware processed by SophosLabs was ransomware. We’re expecting this to jump to approximately 45 percent in October,” said Rowland Yu, a SophosLabs security researcher. “One reason we believe ransomware on Android is taking off is because it’s an easy way for cyber criminals to make money instead of stealing contacts and SMS, popping ups ads or bank phishing which requires sophisticated hacking techniques. It’s important to note that Android ransomware is mainly discovered in non-Google Play markets — another reason for users to be very cautious about where and what kinds of apps they download.”

The SophosLabs report further indicates two types of Android attack methods emerged: locking the phone without encrypting data, and locking the phone while encrypting the data. Most ransomware on Android doesn’t encrypt user data, but the sheer act of locking a screen in exchange for money is enough to cause people grief, especially considering how many times in a single day information is accessed on a personal device. “Sophos recommends backing up phones on a regular schedule, similar to a computer, to preserve data and avoid paying ransom just to regain access. We expect ransomware for Android to continue to increase and dominate as the leading type of malware on this mobile platform in the coming year,” said Yu.

IndigoVision has launched its new BX thermal bullet camera. The BX thermal has a VOx uncooled thermal sensor and athermalised focus-free lens and provides an all-in-one intelligence-driven solution for extreme outdoor and indoor thermal security. High thermal sensitivity (<40 mK) captures more image details and accurate temperature measurements over long distances, providing various installation possibilities, from perimeter detection to process or machinery monitoring. It is combined with built-in intelligent video and thermal analytics which can detect a maximum, minimum or temperature difference, alerting users when an abnormality is detected.

The BX thermal bullet camera offers many features:
- Multiple resolution options – 336 x 256 or 640 x 512 VOx uncooled thermal sensors.
- High thermal sensitivity – <40 mK with an athermalised focus-free lens delivers accurate temperature measurements over long distances.
- Thermal analytics – temperature measurement -40°C to +550°C, hot trace and fire warning.

For more information contact Alex Penhaligon, IndigoVision, +27 (0)72 496 8570, a.penhaligon@indigovision.com.
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Track</td>
<td>+27 (0)11 551 1687</td>
<td><a href="mailto:info@activetrack.co.za">info@activetrack.co.za</a></td>
<td><a href="http://www.activetrack.co.za">www.activetrack.co.za</a></td>
<td>50</td>
</tr>
<tr>
<td>Adani Systems</td>
<td>+375 173 490 039</td>
<td>info@adani systems.com</td>
<td><a href="http://www.adani">www.adani</a> systems.com</td>
<td>39*</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>44,47</td>
</tr>
<tr>
<td>Betafence South Africa</td>
<td>+27 (0)21 868 7300</td>
<td></td>
<td><a href="http://www.betafence.co.za">www.betafence.co.za</a></td>
<td>26</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://africa.boschsecurity.com">http://africa.boschsecurity.com</a></td>
<td>47</td>
</tr>
<tr>
<td>South Africa &amp; sub-Saharan Africa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capsule Technologies</td>
<td></td>
<td><a href="mailto:franck@capsule-sa.co.za">franck@capsule-sa.co.za</a></td>
<td><a href="http://www.capsule-sa.co.za">www.capsule-sa.co.za</a></td>
<td>57</td>
</tr>
<tr>
<td>Cathexis Africa</td>
<td>+27 (0)31 240 0800</td>
<td><a href="mailto:sales@catafrica.co.za">sales@catafrica.co.za</a></td>
<td><a href="http://www.cathexisvideo.com">www.cathexisvideo.com</a></td>
<td>13</td>
</tr>
<tr>
<td>Centurion Systems</td>
<td>+27 (0)11 699 2400</td>
<td>charl.mijnhardt@</td>
<td><a href="http://www.centsys.co.za">www.centsys.co.za</a></td>
<td>13,14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ContinuitySA</td>
<td>+27 (0)11 554 8000</td>
<td><a href="mailto:info@continuitysa.co.za">info@continuitysa.co.za</a></td>
<td><a href="http://www.continuitysa.com">www.continuitysa.com</a></td>
<td>37*</td>
</tr>
<tr>
<td>Duxbury Networking</td>
<td>+27 (0)11 351 9800</td>
<td><a href="mailto:lliara@duxbury.co.za">lliara@duxbury.co.za</a></td>
<td><a href="http://www.duxbury.co.za">www.duxbury.co.za</a></td>
<td>46</td>
</tr>
<tr>
<td>ElectroMechanica</td>
<td>+27 (0)11 249 5000</td>
<td><a href="mailto:lizannes@em.co.za">lizannes@em.co.za</a></td>
<td><a href="http://www.em.co.za">www.em.co.za</a></td>
<td>60</td>
</tr>
<tr>
<td>Elvey</td>
<td>+27 (0)11 401 6700</td>
<td><a href="mailto:info@elvey.co.za">info@elvey.co.za</a></td>
<td><a href="http://www.elvey.co.za">www.elvey.co.za</a></td>
<td>17*,54</td>
</tr>
<tr>
<td>Forbatt SA</td>
<td>+27 (0)11 469 3598</td>
<td><a href="mailto:sales@forbatt.co">sales@forbatt.co</a></td>
<td><a href="http://www.forbatt.co">www.forbatt.co</a></td>
<td>33,55</td>
</tr>
<tr>
<td>G4S Africa</td>
<td>+27 (0)82 098 2666</td>
<td><a href="mailto:leandi.ferreira@za.g4s.com">leandi.ferreira@za.g4s.com</a></td>
<td><a href="http://www.g4s.co.za">www.g4s.co.za</a></td>
<td>8</td>
</tr>
<tr>
<td>Genetec</td>
<td></td>
<td><a href="mailto:bcary@genetec.com">bcary@genetec.com</a></td>
<td><a href="http://www.genetec.com">www.genetec.com</a></td>
<td>20</td>
</tr>
<tr>
<td>Gianni Industries</td>
<td>+886 222 677 986</td>
<td><a href="mailto:inquiry1@gianni.com.tw">inquiry1@gianni.com.tw</a></td>
<td><a href="http://www.gianni.com.tw">www.gianni.com.tw</a></td>
<td>13*</td>
</tr>
<tr>
<td>Hikvision South Africa</td>
<td>+27 (0)10 035 1172</td>
<td><a href="mailto:support.africa@hikvision.com">support.africa@hikvision.com</a></td>
<td><a href="http://www.hikvision.com">www.hikvision.com</a></td>
<td>IFC*,1*,56</td>
</tr>
<tr>
<td>Hi-Tech Security Solutions</td>
<td>+27 (0)11 543 5800</td>
<td><a href="mailto:welsey@technews.co.za">welsey@technews.co.za</a></td>
<td><a href="http://www.technews.co.za">www.technews.co.za</a></td>
<td>11*</td>
</tr>
<tr>
<td>Hitek Security Distributors</td>
<td>+27 (0)21 946 3344</td>
<td><a href="mailto:sales@hitsecuirty.net">sales@hitsecuirty.net</a></td>
<td><a href="http://www.hiteksecurity.net">www.hiteksecurity.net</a></td>
<td>15*</td>
</tr>
<tr>
<td>IndigoVision</td>
<td>+27 (0)72 496 8570</td>
<td><a href="mailto:a.penhaligon@indigovision.com">a.penhaligon@indigovision.com</a></td>
<td><a href="http://www.indigovision.com">www.indigovision.com</a></td>
<td>60</td>
</tr>
<tr>
<td>Johnson Controls Security Products</td>
<td>+27 (0)82 566 5274</td>
<td><a href="mailto:emallett@tycoon.com">emallett@tycoon.com</a></td>
<td><a href="http://www.tycosecurityproducts.com">www.tycosecurityproducts.com</a></td>
<td>48,51,56</td>
</tr>
<tr>
<td>LAWtrust</td>
<td>+27 (0)11 731 8238</td>
<td><a href="mailto:robyn@lawholdings.co.za">robyn@lawholdings.co.za</a></td>
<td><a href="http://www.lawholdings.co.za">www.lawholdings.co.za</a></td>
<td>58</td>
</tr>
<tr>
<td>Leaderware</td>
<td>+27 (0)11 787 7811</td>
<td><a href="mailto:sales@leaderware.com">sales@leaderware.com</a></td>
<td><a href="http://www.leaderware.com">www.leaderware.com</a></td>
<td>16,17</td>
</tr>
<tr>
<td>Magnet</td>
<td>+27 (0)31 274 1998</td>
<td><a href="mailto:samantham@magnetgroup.co.za">samantham@magnetgroup.co.za</a></td>
<td><a href="http://www.magnetgroup.co.za">www.magnetgroup.co.za</a></td>
<td>44</td>
</tr>
<tr>
<td>MASS</td>
<td>+27 (0)12 142 0000</td>
<td><a href="mailto:info@mass-solutions.co.za">info@mass-solutions.co.za</a></td>
<td><a href="http://www.mass-solutions.co.za">www.mass-solutions.co.za</a></td>
<td>51*</td>
</tr>
<tr>
<td>Milestone Systems</td>
<td>+27 (0)82 377 0415</td>
<td><a href="mailto:arms@milestoneys.com">arms@milestoneys.com</a></td>
<td><a href="http://www.milestoneys.com">www.milestoneys.com</a></td>
<td>12,45</td>
</tr>
<tr>
<td>Mimic Components</td>
<td>+27 (0)11 689 5700</td>
<td><a href="mailto:sales@mimic.co.za">sales@mimic.co.za</a></td>
<td><a href="http://www.mimic.co.za">www.mimic.co.za</a></td>
<td>53</td>
</tr>
<tr>
<td>Naxian</td>
<td>+27 (0)87 820 0620</td>
<td><a href="mailto:bernard@naxian.co.za">bernard@naxian.co.za</a></td>
<td><a href="http://www.naxian.co.za">www.naxian.co.za</a></td>
<td>OFC*,18,19*</td>
</tr>
<tr>
<td>neaMetrics</td>
<td>0861 632 638</td>
<td><a href="mailto:info@neaometrics.com">info@neaometrics.com</a></td>
<td><a href="http://www.neaometrics.com">www.neaometrics.com</a></td>
<td>49*</td>
</tr>
<tr>
<td>OT-Morpho is now IDEMIA</td>
<td>+27 (0)11 286 5800</td>
<td><a href="mailto:sec.san.contact@morpho.com">sec.san.contact@morpho.com</a></td>
<td><a href="http://www.idemia.com">www.idemia.com</a></td>
<td>5*</td>
</tr>
<tr>
<td>Paxton</td>
<td>+27 (0)21 427 6691</td>
<td><a href="mailto:support@paxtonaccess.co.za">support@paxtonaccess.co.za</a></td>
<td><a href="http://www.paxtonaccess.co.za">www.paxtonaccess.co.za</a></td>
<td>46</td>
</tr>
<tr>
<td>Pelco by Schneider Electric</td>
<td>+27 (0)11 254 6400</td>
<td><a href="mailto:yvette.venter@schneider-electric.com">yvette.venter@schneider-electric.com</a></td>
<td></td>
<td>43</td>
</tr>
<tr>
<td>Powelltronics</td>
<td>0861 787 2537</td>
<td><a href="mailto:marketing@powelltronics.com">marketing@powelltronics.com</a></td>
<td><a href="http://www.p-tron.com">www.p-tron.com</a></td>
<td>23*,46</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>6*</td>
</tr>
<tr>
<td>Reditron</td>
<td>+27 (0)87 802 CCTV (2288)</td>
<td><a href="mailto:marketing@reditron.co.za">marketing@reditron.co.za</a></td>
<td><a href="http://www.reditron.co.za">www.reditron.co.za</a></td>
<td>43,45</td>
</tr>
<tr>
<td>Secu-Systems</td>
<td>+27 (0)11 794 7834</td>
<td><a href="mailto:charles@secusystems.co.za">charles@secusystems.co.za</a></td>
<td><a href="http://www.secusystems.co.za">www.secusystems.co.za</a></td>
<td>27*</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>43,45,49*</td>
</tr>
<tr>
<td>TeleEye (South Africa)</td>
<td>+27 (0)11 557 9200</td>
<td><a href="mailto:info@teleyee.co.za">info@teleyee.co.za</a></td>
<td><a href="http://www.teleyee.com">www.teleyee.com</a></td>
<td>60</td>
</tr>
<tr>
<td>Xscann Technologies</td>
<td>+27 (0)11 608 1504</td>
<td><a href="mailto:info@xscann.com">info@xscann.com</a></td>
<td><a href="http://www.xscann.com">www.xscann.com</a></td>
<td>41*,42</td>
</tr>
<tr>
<td>Zhejiang Dahua Technology Co.</td>
<td>+86 571 8768 8883</td>
<td><a href="mailto:dahua.sa@global.dahuatech.com">dahua.sa@global.dahuatech.com</a></td>
<td><a href="http://www.dahuasecurity.com">www.dahuasecurity.com</a></td>
<td>3*,15,28</td>
</tr>
<tr>
<td>ZKTeco (SA)</td>
<td>+27 (0)12 259 1047</td>
<td><a href="mailto:sales@zkteco.co.za">sales@zkteco.co.za</a></td>
<td><a href="http://www.zkteco.co.za">www.zkteco.co.za</a></td>
<td>25*,41,44,47</td>
</tr>
</tbody>
</table>

For more information on these and other suppliers please see www.hsbd.co.za
research, development and innovation

Making the difference

When it comes to surveillance technology today, there are many cameras to choose from, but not all brands offer the added value the end user appreciates and that makes our technology and products best sellers for the distribution channel.

FORBATT SA

We import exclusively for our network of distributors.

www.forbatt.co
sales@forbatt.co
Forbattsa
011 469 3598