Professional Security for the Home
DIY consumer security kit

- Wide selection of cameras and sensors detect intrusions and fire
- View live video, play back recordings and receive alert notifications
- H.265 to optimize viewing experience
- Battery-powered Wi-Fi cameras, doorbell and baby monitor allow installation anywhere
- Save footage to the Cloud with affordable service packages
contents

From the editor’s desk .......................................................... 4

Insight and trends
Back to the future ................................................................. 6
Assessing risks in security technology systems ...................... 8
Manage your data appropriately ............................................. 10
Are IP cameras vulnerable to cyber attacks? ........................... 12
Who’s on your estate? ........................................................ 13
Are you sure you are living in a secure estate? .......................... 14

Residential Estate Security Conference 2017
Managing technology risks for effective estate security .............. 17
Residential Estate Security Conference Sponsors .................... 21

Round table
Expect the unexpected ......................................................... 26

Total cost of ownership
The total cost of ownership can hurt your security budget ............ 30

Security-as-a-service
Buy and manage or use? ...................................................... 36

Visitor management
Bin the book, evolve to electronic ........................................... 38
Islington on the Green .......................................................... 42
Effective, PoPI-compliant visitor management ....................... 43

Power management
Essential backup power equipment ........................................ 44
Five safety rules ................................................................. 46

Surveillance
Deepening the value of surveillance ....................................... 47
Cameras don’t equal surveillance ......................................... 48
Advances in video analytics ............................................... 49
Enhancing estate control rooms ......................................... 52
Surveillance on the move ................................................... 53
Biometrics
Easy, fast and secure ................................................................. 58
Selecting your biometric solution ........................................ 62

Maintenance
Remote maintenance is a reality ............................................. 64

Perimeter security
The perimeter and beyond ..................................................... 66
Thermal buffer zone ............................................................. 69
Security by radar .................................................................. 70
All-live and kicking .............................................................. 71
Securing the perimeter at Chapman’s Bay Estate .............. 72

Alarms & intruder detection
Is estate living really safer? .................................................. 73

Personnel services
Guard monitoring technologies ............................................ 74
Guarding the estate ............................................................ 76

Networking
Not cool, but critical ........................................................... 78

Home security
Simple but secure home security ........................................ 81
Home security in an estate? ................................................ 82

Integrated solutions
Integrated layers of security ................................................ 85
There’s an app for that ........................................................ 86
No sense of humour about security .................................... 87
Risk management approach to estate security ................. 88
Multi-layered estate security .............................................. 89
Enforcing security at Izinga ............................................... 90

Internet of Things
Is your water meter online? .................................................. 91
Leveraging IoT to enhance access ....................................... 92

Product focus ................................................................. 93

Directory of estate security products and service providers 101
CONVERGENT SECURITY.
Pipe dream or best-of-both?

To maximise the effectiveness of your Security Guards and to get the best out of your Security Technology investment you need a company that understands how to get these two disciplines to work together as one. Excellerate Security is that company.

With almost 40 years’ experience in the private security sector, we understand security guards. We also happen to be at the cutting edge of security technology. We have as a result developed a deep understanding of the practicalities of integrating security personnel and security technology - an understanding that we will happily share with you.

Call us, let’s talk convergence.

For further information call us today on 0860 11 00 11 or visit our website: www.excellerate.co.za
It can be secure or it can be cheap

Kicking off the Residential Estate Security Conference 2017, Rob Anderson noted an unpleasant truth about estates and their endeavour to be secure. Rob noted that estates ask for advice, request quotes to meet their specific requirements, and then choose the cheapest quote. Alternatively, someone on the HoA or body corporate knows someone “who is brilliant at this type of stuff” and the job goes to them.

Not too long after the installation is complete, the complaints start coming in about perimeter breaches, illegal and undocumented access, cameras that produce yellow (or sometimes green) images when they are working, and guards that are never where they are supposed to be (except when they’re asleep). Of course this applies to more markets than only estates, but it is an inconvenient truth many integrators, consultants, service providers and vendors deal with on a regular basis.

Even if you get someone to install the cheap stuff professionally, they won the bid on price and you will be disappointed if you think they are going to support and maintain their work just as professionally – no matter what was agreed. The budget cuts have to come from somewhere and it’s either saved during installation or in the support/maintenance phases (or both). We all know the economy is in the dumpster, but is that worth the risks involved in bad security?

Perhaps the problem is that the people making decisions are not aware of what makes security work. Those nasty bean counters simply count beans, not the cost of lives and the trauma involved in failed security. But there again, see what cars they drive and ask them why they aren’t in a 1973 VW Beetle – that’s a cost-effective buy?

Cost of ownership was one of the presentations at this year’s Residential Estate Security Conference. You can find a brief summary of it and the other presentations in this handbook. We also have an article on the total cost of ownership as it pertains to the security market among the different editorials we include in the publication.

We also have insights from some people involved in ensuring their estate’s security who sat around a table with Hi-Tech Security Solutions to speak about the challenges they face. Money is always an issue, but it doesn’t have to mean poor security.

I would like to thank everyone who supplied information and answered questions in the process of putting the Residential Estate Security Handbook 2017 together. It’s difficult to compress everything into one publication, but with the able assistance of Rob Anderson we have managed to address many of the security issues estates today are facing.

I hope you enjoy the magazine and I welcome comments, suggestions and criticisms to andrew@technews.co.za.

Andrew
Back to the future

By Rob Anderson.

What will estate security look like in 2027?

The last 10 years has seen substantial change in the security technology world. So, what will the next 10 years bring? It is worth considering the possibilities because if you don’t, in 10 years you may not be offering the most viable solution. That would not be good for your business, or if you are a user, it could be difficult to survive the changes necessary to stay secure.

We hear so much about the ‘disrupters’ in the environment around us. For instance, the electric car could ‘disrupt’ the fuel industry. If so, the fuel industry needs to make plans to make the necessary changes for survival.

There are a few potential disruptors in the security sector, or we may just see it as technology advances. Let’s list a few (technical or otherwise):

1. The guarding industry is becoming too expensive for the average client. Not only must there be annual increases, but removing the E-grade, and at the end of this year, the D-grade, has a knock-on effect and big cost increases. So, something must happen to reduce the total cost of manpower.
2. The ever-increasing application of technical solutions, require that better ‘pilots’ or operators be employed. They need to be more skilled, trained and better paid. If we don’t, the technology spend is not a good choice and the results will be far less than required.
3. The increased computing power of electronics in the security devices has opened big opportunities. Much of the analysis is being achieved in the camera for instance.
4. Improved analytics is providing more consistent results. Some solutions even have a level of learning to improve the efficiency of the system.
5. We are starting to have a greater number of open systems, that allow for system integration to take place at low cost with high returns. The open systems allow for the interconnection of different brands and products. The days are gone when the product chosen locked you in to the brand for life.

Without listing any more ‘disruptors’, we can see a trend:

• Less people employed.
• These employed, being much higher skilled than the current deployment.
• Technology supports greater level of automated reaction to events.

If a machine (an ATM) can be good enough to hand out cash, why can’t the entrance gate have an Automated Guard Machine (AGM) to decide if you can enter? This is possible already. The use of drones in all aspects of life is already happening. So, the drone will become the first response to an alarm.

We have many on-line methods of paying for goods. It relies on making sure there is positive identification. Visitors to an estate may have to use ‘Pay System’ to register as a visitor to get access through the AGM. Of course, the AGM will be a wonderful solution to those people that shout at the guards and abuse them.

The world of robotics and artificial intelligence (AI) is making these sorts of suggestions well within our capabilities. With this scenario in front of us there are a few challenges. And they are not technical, they are people challenges:

(a) Lots of people will be out of work, a big social problem.
(b) Training and upskilling of the few left to pilot the system will become vital. This training does not exist yet.
(c) The quality of communication systems, including the internet, needs to be top class with fail-over solutions.
(d) The installer/integrator will need to be top quality. All the outcomes and results will be based on the build quality and maintenance of the system.

(e) But be careful, the AI systems monitor your actions and try to think for you. That may be the next risk we have to be aware of.

So, in the new world of less people, more technology and systems in the residential estate security space, what else can be expected? As a start:

(a) A new breed of criminal who is a technical expert. They exist already.
(b) A security manager who is a technical manager.
(c) An investigator who is skilled in the technology sector and equipment operation.
(d) Training facilities that need to have improved training courses for the new demand.
(e) Companies that offer technical audit and technical risk management services to continually evaluate the health of your system.
(f) A legal system and court procedures that will have to be able to perform in the new environment. Much of the crime may be based on technology manipulation, to the advantage of the techno-crook.

As much as we may feel this is not for us, the increasing labour costs and reducing technology costs are going to win the day. The clients will be demanding that we rise to the occasion.

It’s not the badly trained guard that is going to fail. It’s going to be the badly designed/installed/maintained technology that is going to fail. How are we going to manage that risk?

As I have been told many times, “The future is not what it used to be.”

For more information, contact Adamastor Consulting, 086 099 5269, rob@adamastor.co.za, www.adamastor.co.za.
STOP SEARCHING.

We strive to provide you with every solution possible. You found us for a reason.
The process of risk assessment and implementing mitigating actions is well known to us all. In the business world, the risk assessment process is often undertaken following the PESTEL format. PESTEL refers to the components that need to be evaluated, i.e. PESTEL stands for Political, Economic, Social, Technology, Environmental, Legal.

To a large extent, this approach does carry over to the methods used when doing a security risk assessment. It is, however, unusual for the security risk assessment to evaluate the risks ‘embedded’ in the technology solutions, be they existing or new technology. Even more interesting is that the technology solution was probably implemented because of a physical risk assessment. The technology was used to mitigate the physical risk, and much to the surprise of all, it comes with its own risks.

One of the challenges is that the technical risk assessment needs to be undertaken by a technically competent person who understands the risk assessment process. Do these individuals exist? Probably, yes, but they are few and far between.

**Common risks**

Let’s look at some of the technology risks that are most common, easy to assess and resolve. At present, the biggest risk must be the sudden rush of ransomware and virus infections. If these get into your security system you will remember it for a long while. The problem is that almost 100% of security systems are connected to the Internet. The security ‘guru’ will tell you this is vital for:

(a) Software upgrades
(b) Remote maintenance
(c) Cloud-based security systems

Before the digital age, we had ‘closed’ systems, now it seems that this is not possible. The solution, employ a specialist who puts actions and processes in place to reduce the risk, and provide a recovery solution for when your systems are attacked by a cyber criminal. True to form, most organisations take action after the first infection.

Moving on to the other risks seen on many sites:

**Camera systems**

Have you checked that the camera is still recording? If the camera has been set up with analytics, is it still functioning as planned? What happens when the power fails? Is there a backup power system (that works)? Is the camera still showing the view intended and does it provide a good picture 24/7?

And of course, in the IP camera world the threat of the camera being ‘hacked’ has become real.

**Power backup systems**

- How often are the batteries checked to see if they are at the end of their life?
- Does the standby generator support the UPS correctly, or does the UPS see the generator as a ‘bad supply’ and runs on batteries?
- Are cables sized correctly so that voltage drops are not excessive?

**Lightning and surge damage**

- Are the power as well as data systems backed up with surge protection?
- Does the earth system comply with the surge protection equipment requirements?
- Surge protectors fail and need to be checked regularly. Is that being done?

**Data backup**

We have all learnt the hard way, so in most cases this is being done. The most common problems are:

- The system fault or virus migrates to the backup as well. Then there is no backup other than an accurate copy of the problem.
- Has anyone ever tried to recover the system from the backup to see if it works?

**Access control systems**

The access control systems are just as good as the current database of valid users and the way the system is used. In most cases (hopefully), the access control is synchronised with the CCTV to create a visual image of the person gaining access and egress. The most common failures here are:

- The security guard gives access and there is no visual or data record of the transaction.
- The database is years old. People still have access that should not.
- The database backup method is incorrect. This is most often the case with the SQL database.
- Who has the system setup access codes? Have they been shared? Or worse, if the maintenance chap is gone, how do you get into the system? But don’t worry, in most cases the systems are run on the default access codes…

**Installation defects**

This is probably the most common area of concern.
• Are there drawings and network diagrams of the systems? If not, what happens when service providers change?
• Are cables numbered and installed neatly so that it’s possible to trace faults?
• Have the correct cable types been used? Solid core, braided core, current carrying capacity etc.
• Is the electric fence energiser installed well away from the other components?
• Is there fuse or circuit breaker protection on the power circuits?
• Has the surge protection been by-passed?
• Are there tamper switches, power fail and low battery notification systems?
• Have all the system clocks been synced to one time?

Interlinkages and dependences
The above risks are often linked: e.g. if the power fails then your other systems go down. Some interlinkages and dependencies will be obvious, but others less so. Does anyone consider mapping these and trying to work out how robust the whole system is?

This is a situation that we have all found ourselves in, with systems failing and we can’t believe so much can go wrong at the same time. Well, maybe it was one of those ‘lurking’ risks we need to be aware of.

And so, we can go on evaluating possible risks in the technology and putting actions in place to reduce the chance of a risk showing its potential. For the security technology sector to mature and play a positive part in this industry, much needs to be done to manage these risks.

Being aware of them is the first step.

Taking action is the most important next step to provide reliable solutions, and it has to be a client and integrator/service provider joint action.

Let’s reduce our technology risks in the security sector.

For more information, contact Adamastor Consulting, 086 099 5269, rob@adamastor.co.za, www.adamastor.co.za.

The maintenance contract and procedures
So, the systems are all well managed and kept as risk free as possible. And then the monthly maintenance crew arrived and switched some equipment off for repairs and maintenance. As luck will have it, there is an incident while the equipment is off. We usually call it bad luck, but actually it is a real risk and there must be procedures to be able maintain a minimum level of security.
Manage your data appropriately

By Andrew Seldon.

Home is where one relaxes and forgets about the stresses and demands of day-to-day life, except if your job is managing an estate and the security of its residents.

Nobody thinks twice about providing personal information to organisations tasked with managing an estate. One assumes the people employed will automatically treat sensitive information with care and not let it fall into the wrong hands.

Unfortunately, as people and businesses across South Africa have discovered, this is not the case. Whether through carelessness, ignorance or malicious intent, personal information seems to be easy to obtain and use in criminal endeavours. When it comes to an estate, the information collected by managing agents, body corporates and home owners’ associations (HoA) is the very essence of ‘personal’ information and seeing it fall into the wrong hands can have far reaching consequences.

Businesses across South Africa know they have a limited time to comply with the stipulations of the Protection of Personal Information Act (PoPI) and many have started the process of understanding what data they possess and what they need to do with it. Residential estates may think they have secured the sensitive information on their servers or held by their cloud service providers, but PoPI may be a rude awakening for estate managers.

John Cato, a director of IACT-Africa warns that PoPI is a general law that applies to any organisation or person that collects personal information. So from an estate’s point of view, this means the data collected at the gate when visitors or contractors arrive, to the personal data of its residents, such as addresses, phone numbers, email addresses, and even banking details qualify as data that PoPI wants protected.

Even those estates that still rely on the old visitor’s book will find themselves in contravention of the law once PoPI is enforced – which is expected to be somewhere towards the end of 2018. The visitor’s book simply doesn’t make the grade and storing them in a drawer somewhere is even more of a failure in terms of PoPI.

That’s not to say that simply because you have a biometric access system at the gate, or an access control solution that sends an SMS with an entry code that you are in the clear. PoPI doesn’t really care how information is collected, it focuses on why you are collecting it, obtaining consent for collecting it, what you plan to do with it in terms of lawful processing, how you will destroy it, and how you store it in the meantime.

Data handling processes

Cato explains that PoPI expects every organisation or person to handle personal information with appropriate and reasonable organisational and technical safeguards. This means the “secure and lawful processing of personal information”, according to Cato.

In preparing to meet the requirements of PoPI, he says every organisation needs to identify where personal information is collected, held and processed, and ensure the rules governing how the information is handled are set in stone. And while personal information applies to people, it also applies to businesses (juristic persons). If you collect sensitive information about a service provider, for example, that information also needs to be governed by the same processes.

It’s also important not to collect information you don’t need to have as any individual can ask why you want to collect the information requested, what you will use it for and how long you will keep it. So when an unexpected visitor arrives at the gate, the guards must be able to provide this information, which can be printed on a large sign outside the access control area, or on a leaflet which is presented to the visitor. These should be backed up with a formal privacy policy. In a business environment, the CEO would normally be the person responsible for PoPI compliance as the information officer. He/ she would then appoint a deputy to handle the compliance on behalf of the CEO’s office. In an estate things aren’t so clear. Would the chair or the HoA or the estate manager be the responsible party? Cato advises every estate to appoint one individual to handle compliance to ensure there is accountability for information management.

Where to start?

Assuming compliance because your vendor or service provider says you are compliant is not a good idea. Cato suggests each estate starts by assessing what data they have and what data they collect on an ongoing basis. Then ascertain if the storage and processing of that data is in line with the Act – that you have taken “appropriate and reasonable” measures in line with industry practices to secure and manage the data.

A simple example would be whether access to the database in which your residents’ personal information is stored is controlled so that only certain people can access the information. When it comes to access control at the gate, the same principles apply.

Estates often outsource their access control to third parties, which Cato says is basically a standard practice. However, the estate needs to have a written agreement with the service provider that defines responsibilities for the estate and the service provider for the collection, processing and destruction of data. He adds that the law does not allow you to abdicate responsibility. The estate will be held accountable, but will have legal recourse against the service provider if the latter has contravened the Act.

Similar rules apply to all service providers used by the estate. The company running the resident portal, for example, also needs
to have a written contract with the estate setting out the terms under which information is processed. And this even goes as far as procurement. The estate needs to be sure its procurement providers are compliant and handle personal data correctly.

The reach of PoPI even stretches to the golf club. Golf estates, for example, will also have to have a set of processes managing how data about members and guests is handled. And what about the bowls team?

** Destruction is mandated**

This article has referred to the destruction of data as part of the stipulations of PoPI. There is more than one story about finding visitor’s books under a table or simply thrown away into the garbage. Such an act is irresponsible at a minimum and will be illegal under PoPI (as will the visitor’s book). The concept of processing information not only covers what data is collected and how, as well as how it is stored and used, it also covers its destruction.

Firstly, the estate needs to determine how long it will store information. For residents the storage term is not set while they are living on the estate, but what happens to their data when they leave? How long does the estate keep visitor or contractor information? Cato says there is an argument to be made for keeping this information available to make it easier for people to gain access in future, but how long will data remain on the system without being accessed? This is another issue estates need to sort out when they assess their PoPI readiness. They should clearly define their retention practices in an appropriate policy to protect themselves against their practices being mistakenly interpreted in the event of a compromise or breach.

Then, when it is determined that data must be destroyed, how do you do it? Cato explains that for paper records, a consumer-grade shredder is not compliant. Information must be destroyed so that it cannot be reconstructed and a person identified, meaning you need a more expensive shredder that slices and dices paper finely.

For electronic data, pressing the delete key is not acceptable either as it is not a difficult job for someone with a bit of technical knowhow to recover files or parts of a file. Estates will need to wipe their data properly, especially in the case of upgrading computers. A hardware shredder or technology such as disk degaussing should be used.

** Cyber security and estates**

Hi-Tech Security Solutions knows of at least one estate in South Africa that has had its data encrypted by ransomware. The estate in question could not recover its data from backups because the backups were also encrypted. Good fortune prevailed and one of the estate’s service providers was able to resolve the issue (in a manner that would be illegal under PoPI), but the cyber security question is as pertinent to an estate as it is to any business.

Estate’s computerised systems must be protected by anti-virus software and firewalls, and a reliable backup process must be in place. This means a backup that is made to media that is stored offsite – not simple a Dropbox copy. For estates that can afford it and have the technical capabilities, Cato says they could even look at encrypting their data to ensure that it is safe even if some malicious actors get their hands on it.

It’s also worth noting that using cloud services such as Dropbox and the many others also raises a concern as PoPI compliance means the laws of the country where the service is hosted must be equal to or better than PoPI’s stipulations.

Similarly, the new General Data Protection Regulation (GDPR) regulations in Europe will also be causing a headache in South Africa. Cato explains these regulations govern the collection and use of EU residents’ personal data globally. That means collecting personal information from your German summer-time resident will be governed by PoPI and GDPR rules.

And, Cato warns, let’s not forget about the cyber security implications. It’s also worth noting that using cloud services such as Dropbox and the many others also raises a concern as PoPI compliance means the laws of the country where the service is hosted must be equal to or better than PoPI’s stipulations.

**Appropriate and reasonable**

When looking at all the implications PoPI can have on an estate’s collection and management of data, one can go on forever about what should or should not be done. However, Cato advises that it need not be such a complicated task as long as the efforts by the estate are seen as appropriate and reasonable, and are formally documented.

With the correct advice and assessment assistance, there should be no reason for an estate to fall foul of the law. There is still enough time to ensure PoPI compliance, although not too much time when considering the scope of the project. But in short, as long as the estate can show its efforts to comply were reasonable and appropriate, the HoA will probably not have a jailbird on the committee.

For more information, contact John Cato, IACT-Africa, +27 (0)10 500 1038, johnc@iact-africa.com, www.popisolutions.co.za.
The Internet of Things (IoT) is currently on the rise and with the expansion of digitisation, the separation between physical security and network security is no longer clear.

Previously, intrusion detection, access control, video surveillance and other physical security technologies operated primarily on analogue infrastructure, while networks, servers, computers, tablet and smartphones operated separately on IP-based infrastructure. The introduction of IP-based infrastructure has changed this and has revolutionised physical security by delivering the benefits of high-capacity, low-latency performance efficiencies and operational cost-effectiveness.

Now, nearly every security camera or sensor technology sold today operates on an Ethernet-based wired or wireless network which means that physical security solutions, like video surveillance systems, are prone to the same types of attacks and exploitations that have inundated data networks for decades. So, how do organisations secure their physical security network to ensure that the very infrastructure that is meant to be protecting business assets isn’t used against them?

It starts with treating the physical security infrastructure and devices in the same manner as network infrastructure and devices. Therefore, protecting everything, right down to switch level.

**Analogue vs. IP**

Cameras on a modern analogue CCTV system send their video footage in base band format over cabling back to a digital video recorder (DVR) where it is digitised and stored on hard drives. On the other hand, IP cameras broadcast their video as a digital stream over an IP network, and because the video is an IP stream straight from the camera, the DVR is replaced by a network video recorder (NVR) which determines how and where footage is stored.

The analogue system is traditionally more secure given that it is usually physically separated from other network components, but the benefits that can be gained from using an IP-based system mean that the risks thereof need to be properly considered and mitigated.

**A single IP device is all it takes**

Considering how important a CCTV surveillance system is in protecting everything, from private medical research facilities, to military bases and power generation facilities, the protection of the physical security solution itself has become a concern. Whereas analogue physical security implementations benefited from a certain degree of protection simply by not being connected to other systems, an IP-based CCTV system generally uses the same network infrastructure as the rest of the company.

This means that an attacker no longer needs direct, on-site access to equipment or infrastructure in order to take the system offline, monitor video footage without authorisation, steal or destroy recordings, or modify content. In fact, a single device is all it takes, as an attacker only needs access to one IP-based device (like an IP camera) to potentially gain access to the company’s entire network and digital assets.

**Protecting the physical security network**

The typical CCTV deployment connects servers and management consoles to IP-enabled cameras and NVRs. Because these systems also need to interact with broader security measures, such as access control systems, alarms and security incident management software – each of these connections is thus a vulnerability.

So how can businesses protect their IP-based CCTV systems from intruders given the ever-expanding nature of the Internet of Things? There are a number of common-sense methods that bear repetition. An IP-based surveillance system needs network protection and it is advisable to use a dedicated network for clients and servers and to separate surveillance from these networks in addition to establishing a secure perimeter with a strong firewall.

There are also specific network access control solutions that have been created to help protect IP devices, like cameras against the threat of viruses and other malicious software, sealing hardware and software devices off from outside attacks and isolating them from the corporate network should they become infected. To tighten up any perimeter weakness, organisations should use port protection to set up switches within their networks and restrict user access to certain parts of the network.

These are available as pre-staged servers that are available as pre-configured 8-port or 24-port switches that make for an easy setup. By placing protection at a port level, it becomes possible to add switches and quickly allow or block devices. These protective appliances usually have display panels that provide information on the network, such as the device IP and MAC addresses, port number the devices are connected to on the switch and authentication status.

In the event of an unauthenticated device, an alarm will be triggered in the video management system, even if the appliance is turned off. These alarms provide information about the detected device and its connected network port, allowing the security operator to take immediate informed action. By placing intelligent security at switch level, it is possible to effectively cover the vulnerabilities presented by the IoT in that it is now possible to protect a company’s network from an unknown device gaining unauthorised access, automatically. If an unknown device attempts to log on to a network, it is blocked from the rest of the network, quarantined and reported, before the intruder has a chance to do any harm.

It’s important for businesses to remember that an IP-camera, just like any IP-device, is no longer just a product or a device – it is a vulnerability and it is time to start treating everything on the physical security network in the same vein.

For more information contact Graphic Image Technologies, +27 (0)11 483 0333, laurence@git.co.za, www.git.co.za.
Who’s on your estate?

Estate employees must be screened and verified.

Among the abundant lifestyle incentives and quality amenities, one of the key attractions of residential estates is the level of security they provide to homeowners. In South Africa, a country with one of the highest crime rates in the world, citizens who can afford the luxury of estate living find comfort in knowing that their properties and loved ones are protected from criminal activity.

With security being a top draw card, it is important to ensure that not only is the property well secured, but also that the estate employees pose no risk.

Rudi Kruger, general manager of risk management at LexisNexis Data Services says that it is for this reason that priority should be placed on screening estate security employees. “Background screening helps management make informed decisions by improving transparency and disclosure. It is imperative that estate security management run verification checks on all employees to protect residents from criminals in disguise, who could potentially use their positions to invade the personal space of unsuspecting residents.”

Nobody can predict the future but an evaluation of a candidate’s history will quickly give you an idea of their integrity and credibility.

Kruger added that the following checks could be included to form a complete picture of the candidate:

- ID verification
- Criminal checks
- Qualification checks
- Fraud listing
- Employment history
- Fit and proper screening
- Professional association membership
- Driver’s licence
- Bank verification
- Rapid personality questionnaires
- Business background search
- Professional driving permit
- Consumer Goods Council verification
- Citizenship verification
- Director/member confirmation

With the assistance of Lexis RefCheck, a hiring manager is in a more knowledgeable position when it comes to the hiring of estate employees, thereby limiting risk. Lexis RefCheck services include verification of tertiary and secondary academic qualifications held by the individual from registered local and international institutions, identity and South African citizenship validation, fraud history checks via the South African Fraud Prevention Services, credit history checks through detailed TransUnion and Experian credit bureau reports, criminal history check via AFISwitch (electronic fingerprint collection and processing), verification of local and international employment history and professional association membership, and matching of bank account against an identity number or registration number.

For more information, visit: http://www.lexisnexis.co.za/our-solutions/private-sector/risk-management/refcheck.aspx
Are you sure you are living in a secure estate?

SAIDSA developed a short questionnaire to help you decide if you are living in a secure estate or not.

The difference in house prices between houses in the suburbs and those in secure estates is enormous. The latest statistics show you can pay double or more for the same house if it is perceived to be located in a secure estate. But what is a secure estate? Simply having an electric fence and a guard at the gate does not make it secure.

SAIDSA developed the questionnaire below to help estates discover how secure they really are. Go through the questions below, and give yourself one point for every ‘yes’ answer to discover if you are really living in a secure estate.

1. Does the body corporate/homeowners’ association always buy security solutions based on proven quality, reliability and effectiveness for your environment?
   SAIDSA comment: If your answer is no, make sure that somebody investigates alternative options. It will only take one homeowner to take on the trustees/body corporate for failure to fulfill their fiduciary duty on providing security at the estate.
2. Does your electric fence have zones to allow for easy identification of exactly where the alarm is?
   SAIDSA comment: Make sure that your fence is zoned in not more than 100 m sections and you have at least a mimic panel at the main entrance gate indicating the section of trouble/intrusion.
3. Do you only use certified installers (certified by SAIDSA and with the appropriate vendor certifications)?
   SAIDSA comment: Make sure that the installers/maintenance teams are at least PSIRA registered.
4. Do you have visual verification on the perimeter?
   SAIDSA comment: See (5).
5. Do security personnel have full access to the perimeter all the time?
   SAIDSA comment: If not, then visual verification on the perimeter is a must.
6. Do you have a maintenance programme in place to ensure the optimal functioning of your security equipment?
   SAIDSA comment: Make sure somebody on the body corporate or homeowners’ association takes ownership of this task.
7. Is the movement of people in and out of your estate electronically recorded and backed up?
8. Do you verify the identities of people renting or buying on the estate?
9. Is there regular, open and constructive communication between the estate’s residents and committee, and the security service provider(s)?
   SAIDSA comment: Communication is the most important part of the chain of security.
10. Do you verify that the products you install are certified for local use? Are they quality products with a local representative and warranty for backup and support?
   SAIDSA comment: This is a difficult one as there is currently no organisation that certifies electronic security products besides products that need to be ICASA approved. SAIDSA suggests you make sure that the supplier of products you select is a member of ESDA. If you scored less than 7, you are not living in a secure estate.

Johan Booyzen, SAIDSA’s chairman, comments: “Security isn’t something you can buy. It should be a way of living. Security should start within our own attitude and at your own home. From there you should form partnerships with neighbours, your security company, CPF and SAPS.

“Even if you are in a security estate you still have open common areas that are unprotected and potentially dangerous areas. My suggestion would be that even if you reside in a security estate, act as if you are still in a normal suburb. This would give you the extra layer of security provided by your estate/body corporate as well as your own security system where you have full control.

“I’m of the opinion that visual verification is the future of security, even if you are in a security estate. You can recommend that the estate implements this, or do it on your own for your own safety and peace of mind.”

Who is SAIDSA?
The South African Intruder Detection Services Association (SAIDSA) is an association of service providers of security systems, ranging from basic alarms to sophisticated electronic intruder detection systems and CCTV, incorporating signal monitoring as well as the provision of armed reaction services. SAIDSA is regarded as the watchdog of this segment of the industry and has the interests of both its members and the public at heart.

It is the representative employer body for the industry in South Africa. The objectives of the association include a continuous evaluation of the development and the adequacy of skills in the industry, to upgrade the quality and standards of electronic security in South Africa, and to protect the public from unscrupulous, fly-by-night operators.

All companies listed on SAIDSA’s Approved Register have complied in every way with stringent standards that have been laid down by SAIDSA in regard to control rooms, installations and reaction services and are continuously inspected to ensure continued compliance. A complaint against an approved service provider will be investigated by the Executive Committee of SAIDSA and, if not satisfactorily resolved, the member may be removed from the register.

SAIDSA appeals to all members of the public, commerce and industry to consider the importance of selecting a reputable company. This Register of Service Providers has been compiled to assist in making the right choice and is available to all interested parties.

For more information contact SAIDSA, +27 (0)11 845 4870, saidsa@mweb.co.za, www.saidsa.co.za.
Did you know?

- RDC are the local pioneers of VHF security communication systems specifically designed to meet local needs.
- RDC equipment is locally designed and manufactured in Edenvale South Africa.
- RDC’s technology has been adopted globally in over 48 countries.
- RDC has supplied over 2,000,000 communication devices which are present on every continent.
- RDC have the most experienced and specialised team to answer all your estate security communication questions.
- RDC offer a range of technologies to answer the most important local needs in estate security communication.

Do you think?

You need to talk to RDC about your estate security communication infrastructure? Also see our article question and answer piece in this publication by industry specialist Terry van Zyl.

Gert Venter | +27 11 452 1471/2
Email: gert.v@radiodata.co.za | www.radiodata.co.za
Managing technology risks for effective estate security

By Andrew Seldon.

Hi-Tech Security Solutions and Rob Anderson hosted the Residential Estate Security Conference 2017 in Johannesburg earlier this year.

Security is all about mitigating risk and the main risk mitigation tool in estates is technology-based. Today’s technical solutions not only provide better security, but can also, if planned correctly, save money.

But what about six months or a year after the installation? What risk management processes do you have in place to ensure your security technology is running optimally and delivering the services you require all the time? Are the systems being regularly assessed and evaluated according to a plan? What are the typical risks lurking in the technology that should be evaluated, measured and maintained for enduring security?

Hi-Tech Security Solutions and Rob Anderson hosted the Residential Estate Security Conference 2017 in Johannesburg earlier this year to address these questions and more. This year’s conference was focused on the technology risks that can take a well-designed and functional solution and turn it into an underperforming and inherently insecure risk if not maintained and managed correctly. The event looked at various security technologies, highlighted the risks they face and advised attendees on how to extract maximum value and longevity from their security investment.

Delegates were able to hear from a number of experts in various fields, covering different areas of risk that estates today are dealing with. In addition, 10 sponsors occupied the exhibition area where delegates could wander around and network with vendors and other people worried about security on estates. Just before the lunch break, the five gold sponsors were represented in a panel discussion where they answered questions about their products and solutions aimed at the residential market.

The sponsors were:

- Betafence
- Elf Rentals
- Elve (gold sponsor)
- Enforce Security
- Forbatt SA (gold sponsor)
- MiRO (gold sponsor)
- OT Morpho (gold sponsor)
- Paxton
- Powell Tronics (gold sponsor)
- ZKTeco
Continued from page 17

Risk assessments in security technology

The conference was kicked off with Rob Anderson introducing the topic and the focus of the day: identifying, understanding and mitigating your security technology risks. Anderson introduced the conference attendees to the PESTLE (Political, Economic, Social, Technical, Legal, and Environment) model of analysis, and the conference’s specific focus on the technical side of things.

The reason for his focus on technology is that while physical risk is easy to see, technical risk is not always apparent until something happens. As far as estates are concerned, the technical risks start at the initial quotation.

Anderson says quotations for the same project can be as much as 400% apart in price, which is confusing and detrimental as estates often choose the cheapest option without any thought to why it is cheap. There are also no drawings or data sheets and other necessities included in the quote that the estate would need to make a rational decision. The risk then moves onto the installation, which can lead to many headaches later if not done correctly.

Anderson then briefly touched on other technical risk areas which subsequent speakers would expand on in their presentations. These included lightning protection, power management, cybersecurity, access control, surveillance, total cost of ownership and more. He noted that the topics presented at the conference were only a few of the primary risks estates face today, mentioning a few others this conference did not have time to cover.

Keep your access controlled

Starting at the gate, Glenn Allen from Enforce

Security followed Anderson with a presentation on the risks associated with access control. While we may all be used to the various access control processes at estates, Allen noted the risk is still high as about 80% of crime on estates is perpetrated by people who gained access through the front gate.

“Today’s technical solutions not only provide better security, but can also, if planned correctly, save money.”

Allen went through the various access controls we’ve seen over the years, starting with a drawbridge with manual facial recognition for those staying in very old estates. More recently we’ve seen the use of guards who manually verify and authorise entry, followed by stand-alone electronics, including RFID and cards. Then these systems were networked and controlled from a database in a backroom until today where we see advanced biometrics and third-party verification and integration controlling access. The presentation went on to discuss various methodologies and technologies that should be used in access control, such as setting up zones and different categories of access etc.

Database management and maintenance was also discussed, with Allen providing a few pointers on how to manage and ensure your access data is secure and reliable. Naturally, he also spoke about visitor and contractor management and the data that should be collected before allowing temporary visitors in.

For those who are satisfied with manual access control via a boom and a guard at the gate, Allen ended his presentation asking, “If somebody opens the boom on your behalf and you access the property and a crime takes place, were you there?”

The real cost of security technology

We all know the drill. You get a few quotes for a project and take your time assessing each proposal before choosing the cheapest one. A few months, or maybe a year later, you are surprised when your maintenance, repairs and call-out bills are bigger than your full security budget. And it seems that your installer is harder and harder to get hold of.

Roy Alves from Axis Communications was on stage next with a presentation focusing on the total cost of ownership (TCO) of your security installation. He started by examining TCO studies from other industries to show that security is not the only market that doesn’t consider the full lifecycle costs of its solutions.

A 2016 study on mobile devices, for example, showed that CIOs were unaware of 54% of the costs they would be faced with. A 2012 study on the total cost of HR payroll systems showed that HR managers were unaware of 63% of the costs. Most unnerving, a 2011 study on the cost of IT servers showed that 75% of the costs incurred were operational costs, not the purchase price.

Alves then focused on the security industry, using a recent case study from an upmarket golf estate in South Africa as an example. He noted that the costs estate customers are aware of are normally the purchase price and the installation costs; operational and maintenance costs are generally ignored. He offered a simplified view of TCO, broken down into three
areas: total cost of acquisition, total operating cost, and total decommissioning cost.

In the case study presented, the TCO over 10 years was around R28 million. This was broken down into R18.7 million for the total cost of acquisition, R8.7 million as the total operating cost, and around R500 000 was the decommissioning cost.

Alves broke the various sections down into more detail, giving attendees a clear insight into the various costs involved in a security system over a number of years. He also touched on the labour and manpower costs, as well as the costs of staffing a control room for the life of the project.

**Design for longevity**

To assist delegates in recovering from the shock of seeing the real TCO of security systems, Selvan Naidoo from Cathexis Africa was up next to talk about how to ensure the CCTV system you choose will keep on doing its job for the long term and not collapse in three years or less.

His experience in designing and setting up surveillance systems that deliver value stood him in good stead as he highlighted what was required to ensure a return on your CCTV investment.

Naidoo started out talking about how to define the effectiveness of a surveillance system before focusing on the factors required for success. He then highlighted common risks found in surveillance. These included:

1. Poor camera selection and placement.
2. Integration overkill.
3. Operator overload, which reduces their efficiency.
4. A lack of meaningful processes and reports.

Ending the presentation, Naidoo also touched on a few maintenance and operational best practices which estates can make use of to keep their surveillance systems running optimally for the longest period of time.

**Practical PoPI for estates**

John Cato from IACT Africa was up next, explaining how the Protection of Personal Information (PoPI) Act will impact estates and how they handle the data they collect. He explained some basics of PoPI to attendees and went on to describe what estate managers should do to ensure they comply with the act. The *Residential Security Handbook* has covered more of Cato's advice in the article on page 10.

**Practical cybersecurity for estates**

Estates need to be PoPI compliant, but they also need to protect their data from the many cyber attacks that seem to be launched every day. David Cohen from BDO Cyber and Forensic Lab was next up to give delegates some insights into how estates can protect the data they gather from cyber attacks.

Cohen offered keen insights into the types of cyber threats we all face as well as the types of people or organisations that may launch them, including the threat faced from insiders looking to profit from the information they have access to. He then went on to describe the many ways of social engineering, tactics used by criminals to persuade you to give them sensitive information, such as phishing, vishing and whaling. And, of course, the risk of ransomware was also highlighted.

It’s also worth noting that sensitive information doesn’t always have to be hacked from afar. Guessing easy passwords is one way of getting into someone’s account, and dumpster diving (going through the garbage to find documents with interesting information that have been thrown out) is another way of gaining access to useful data.

He then introduced the audience to the six cyber-readiness steps Continued on page 20
organisations can and should take to give them the best defence against the many cyber risks out there. Ending off, he made the point that training is one of the most important aspects of cybersecurity, not only training experts, but also training your staff and making them aware of the risks they face and how that can impact everyone – and, of course, how to deal with the threats.

Surge and lightning protection
One of the more technical presentations was made by Dr Andrew Swanson from the University of KZN. An engineer, specialising in the area of high voltage engineering, Swanson spoke about how best to protect equipment against lightning damage.

South Africa has had an increase in lightning activity recently and the expertise Swanson offered is invaluable to estates as they try to keep their security (and other electronics) running.

The presentation looked at the various instances of lightning and surge damage, such as direct and indirect strikes, and how equipment can best be set up to avoid damage. Of course, a direct lightning strike on an electronic device is going to cause problems for the device, but there are ways and means of preventing the damage from spreading far and wide.

The power must flow
Staying in the power management arena, Riaan Allen from Ultimate Group followed with more insight into how to set up and maintain your power systems (specifically backup systems such as generators and UPSes) for the best performance and longevity.

Riaan was able to provide expert advice on what estates need to look out for when purchasing power management equipment, and he also gave good advice in terms of deciding if your existing installation is going to be reliable or if it’s likely to fail at a moment’s notice. The presentation started with the sales process, moved through the design and installation of these systems (including compliance to various standards), and touched on the tricky issue of sizing the equipment you actually need.

His advice is that buyers should look at the cost of replacing inferior (cheap) products and the expense of repairing bad systems and installation jobs rather than the initial purchase price. When you’re playing with electricity, cheap is not a selling point. In addition, he suggests that a quote should always be accompanied by design documentation and information on the certificates of compliance the installer is authorised to provide.

Sensible connectivity
Coming full circle, MJ Oosthuizen from PinnSec delivered the last presentation of the day in which he referred back to Rob Anderson’s opening presentation. Connectivity is a given in today’s world, even on an estate, but if the systems installed in the server room and on the edge of the estate are installed in a haphazard manner, it increases the chance of something going wrong, increases the time and cost of maintenance as technicians have to sort through piles of cables to find the one they need, and generally makes any repairs or upgrades much harder.

Keeping your servers, storage and the relevant accessories in order and coded according to what the various bits and pieces are used for is critical for successful maintenance and servicing.

Oosthuizen also touched on identifying all the estate’s network and networked assets, which can amount to a large number in the Internet of Things (IoT) age, and ensuring you have a security plan to keep your connectivity up and running safely – which will ensure your users and devices are able to function as required.

He also touched on the IoT in the home, looking at how connectivity can transform a modern home and estate into an easily manageable IoT hub. Of course, security plays a critical role in this regard as your weakest link is the entry point criminals will choose to get into your network and all the data and devices attached to it.

Conclusion
The Residential Estate Security Conference 2017 ended with another round of networking and a final cup of coffee in the exhibition area. Comments from attendees showed that the conference hit the spot in terms of the technology issues estates are facing today and provided insights into how to better plan and manage security technology.

Hi-Tech Security Solutions and Rob Anderson would like to thank all the presenters for the time and effort they put into their presentations, which were all well received. In addition, a note of thanks goes to all the sponsors who supported the event.

Hi-Tech Security Solutions would also like to extend its thanks to Rob Anderson for his guidance, advice and the work he put in to help make the conference a success. Look out for the next Residential Estate Security Conference when the show hits Durban and Cape Town.
From the outside in

The perfect residential estate security solution is one that derives from a synergistic integration of various elements.

Global perimeter fencing leader Betafence believes that the perfect residential estate security solution is one that derives from a synergistic integration of various elements. By leveraging its own knowledge and experience garnered over the past 137 years, and on occasion partnering with professional security consultants like Rob Anderson, the company has built up an admirable footprint of clients.

According to Dan Edwards, Betafence South Africa mirrors the achievements of its international parent company, with successful installations since 1997 at a number of South Africa's premier residential estates, including Monaghan Farm, Zimbali Coastal Resort and Estate, Simola Estate, Kingswood Golf Estate, Kindlewood Estate, Fancourt Hotel & Country Estate and Brettenwood Coastal Estate.

Edwards points out that all of Betafence South Africa’s perimeter fencing products are certified to the highest international standards such as ISO 9001-2008, and products and coatings are tested independently by the likes of CSIR to ensure they meet specific local and international standards. All Betafence products sold in South Africa are manufactured in South Africa from South African products.

“Our products are then tailored to meet the needs of South Africa. It is important to estate managers and Body Corporates to know that the perimeter fencing they have installed is built to endure the harshest conditions. A pre-treatment process guarantees a perfect PVC coating adhesion to the product surface and is therefore proven to withstand the elements, with extreme anti-corrosion features, making it suitable for estates in coastal regions. We in fact offer a 10 year underwritten guarantee against corrosion, making the products especially popular in areas like the KZN North Coast.”

The company offers a complete integrated solution that ensures the deployment of holistic security offerings such as the perimeter fencing, the access control system and surveillance solutions. “By strategically planning the integration of all of these elements with third-party suppliers and a security consultant, Betafence is able to create a solution that covers all the bases in a quality-controlled manner,” says Edwards.

He explains that the fencing has great visual appeal with residential estates, providing not only high levels of security, but furthermore providing aesthetic compliance, an important factor at an elite residential estate. The design of the fencing allows for almost unhindered visibility, therefore allowing optimisation of any lighting and surveillance systems used on the estate.

“The Hi-Tech Security Solutions conference and exhibition allowed the company to showcase its perimeter fencing capabilities and maintain brand awareness. Edwards says that the company is well known in the estate sector but as new estates arise or existing ones upgrade, the event gives them a strong brand exposure opportunity.

For more information contact Betafence South Africa, +27 (0)21 868 7300, www.betafence.co.za.

Partnering with estates for security success

Technical partners who make sure systems work 100% efficiently all of the time.

The team at Elf Rentals considers themselves to be specialist partners in the electronic security sector in terms of the financing, installation and maintenance of security contracts.

The company's Chris Lovemore points out that that the sophistication of electronic security equipment, including fencing, access control, biometric access, power supplies and networking, results in long-term reliability issues. “This sophisticated equipment, by its very nature, is not able to be installed and run smoothly ad infinitum. This means that it requires continual maintenance and upgrading during its lifetime.”

This, he says, is where Elf Rentals enters the fray. “By offering clients a number of customised options, we are able to eliminate the issues they commonly face with security system purchases, such as unreliable suppliers who go out of business and can no longer support the equipment.

“Any residential estate that is serious about their security needs to enter into a partnership with a company that is able to provide a great knowledge base, as well as high levels of service and technical capabilities,” he adds. Lovemore says that a number of defining elements differentiate the company. Firstly, Elf automatically extends the warranties on all security equipment it supplies to clients from the standard 12 months to 60 months. This additional cover is supplied to clients at no additional cost to them, thereby providing them with complete peace of mind, as Elf covers the risk of failure on all equipment it provides.

Secondly, Elf insures all the equipment supplied. Typically, if equipment is damaged by, for example a lightning strike, the downtime that ensues while insurers are contacted and forms are submitted, could compromise the security of the estate and its residents. In what can be deemed a completely seamless operation, Elf simply goes straight to site and fixes the equipment and thereafter makes the necessary claims with its insurers. This ensures that systems are never ineffectual for extended periods of time.

“We are able to link to third-party guarding companies, providing equipment training for the security requirement. We are also able to provide direct financing for clients. We do not use an intermediary financier and are therefore able to write contracts where we can take much more risk, and we are not holding clients to ransom, as with some finance contracts. We see ourselves as technical partners who make sure systems work 100% efficiently all of the time,” says Lovemore.

For more information contact Elf Rentals, +27 (0)41 368 3701, www.elfrentals.co.za.
Elvey cemented its involvement and presence in the residential estate market at this year’s Hi-Tech Security Solutions’ Residential Estate Security Conference held in August 2017. Not only did the company have a stand at the event, but Pentagon, Elvey’s integrated systems design and supply business (a subsidiary of the Hudaco Group), reinforced the company’s residential estate offerings with a presentation on a variety of cameras suitable for the sector.

Max de Sousa discussed key technical considerations estates should make when designing and implementing perimeter CCTV systems. She focused on four main categories – camera technology; network technology; redundancy; and the planning of power. De Sousa weighed up the advantages and disadvantages of optical versus thermal imaging camera technology.

With regard to network technology and redundancy, she pointed out that, generally, the large distances as well as other factors on estates have a negative influence on network reliability. She cites the example of fibre optic cables running to surveillance cameras. When a garden service, for instance, is busy digging in the grounds, they could possibly damage the fibre. By using an intelligent technology like Turbo Ring, which is a self-healing cable that automatically seeks out an alternative viable route, any communications problems are eliminated.

De Sousa says that many estates are victim to power spikes and surges via Eskom, interference from electric fences and lightning. The solution is to be able to ensure that power is clean, which results in interference and damage being minimised. She also touched on the use of video analytics to provide accurate detection of the type of intrusion experienced. By knowing whether the presence is human or animal, the necessary actions can be taken.

Highlighted technology from Elvey’s intruder detection range included alarm systems with various detectors for any type of application. Pentagon’s thermal imaging, Bosch Starlight low-light cameras and Bosch VOT cameras were augmented with the screening of relevant video clips and interactive presentations.

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

Elvey cemented its involvement and presence in the residential estate market at this year’s Hi-Tech Security Solutions’ Residential Estate Security Conference held in August 2017. Not only did the company have a stand at the event, but Pentagon, Elvey’s integrated systems design and supply business (a subsidiary of the Hudaco Group), reinforced the company’s residential estate offerings with a presentation on a variety of cameras suitable for the sector.

Max de Sousa discussed key technical considerations estates should make when designing and implementing perimeter CCTV systems. She focused on four main categories – camera technology; network technology; redundancy; and the planning of power. De Sousa weighed up the advantages and disadvantages of optical versus thermal imaging camera technology.

With regard to network technology and redundancy, she pointed out that, generally, the large distances as well as other factors on estates have a negative influence on network reliability. She cites the example of fibre optic cables running to surveillance cameras. When a garden service, for instance, is busy digging in the grounds, they could possibly damage the fibre. By using an intelligent technology like Turbo Ring, which is a self-healing cable that automatically seeks out an alternative viable route, any communications problems are eliminated.

De Sousa says that many estates are victim to power spikes and surges via Eskom, interference from electric fences and lightning. The solution is to be able to ensure that power is clean, which results in interference and damage being minimised. She also touched on the use of video analytics to provide accurate detection of the type of intrusion experienced. By knowing whether the presence is human or animal, the necessary actions can be taken.

Highlighted technology from Elvey’s intruder detection range included alarm systems with various detectors for any type of application. Pentagon’s thermal imaging, Bosch Starlight low-light cameras and Bosch VOT cameras were augmented with the screening of relevant video clips and interactive presentations.

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

Bringing comprehensive security to estates

Elvey cemented its involvement and presence in the residential estate market at this year’s Hi-Tech Security Solutions’ Residential Estate Security Conference. According to Derek Lategan, MD of Enforce Security, a residential estate security risk treatment plan should be intelligence driven. Thereafter, one can apply a converged blend of human resources, supported and enhanced by technology. Enforce Security, specialists in risk assessment and mitigation, have developed numerous risk solutions based on rigorous ISO 9001 systems and procedures, all operating within a centralised command and control environment.

Enforce has a number of success stories within the residential estate market that include the deployment of thermal imaging CCTV cameras with analytics. Glenn Allen, Enforce’s technology director, points out that this technology has gained traction as it is able to alert security operators when criminals attempt to penetrate perimeter fences late at night. These cameras are especially useful in areas with very low lighting or where there is a prevalence of mist.

Enforce Security has realised the importance of forming professional partnerships with consultants such as Rob Anderson and Associates. “Over the past 25 years we have leveraged these relationships to design dynamic security solutions that are customised to suit individual requirements.

“Recognising the need for specialised consultative services, Enforce now also offers professional assessment services which include the development of personalised risk management programmes for clients. Flexibility and adaptability remain important factors, especially in an ever-changing environment and economy,” says Lategan.

The company’s estate offering encompasses not only specific security personnel and training but also includes the full spectrum of on- and off-site CCTV surveillance, access control and admission solutions, TV distribution, fire detection, and private investigations.

Enforce Security recently added bundled property services (Excellerate Services) to its business model, which incorporates manned security, security technologies, parking management, property care (cleaning, hygiene, gardening and indoor plants), pest control as well as a variety of ancillary services.

The company’s presence at the Residential Estate Security event allowed it to reiterate its increasing growth in the residential estate sector, highlighted by a number of successful deployments at, for example, Zimbali Coastal Estate.

For more information contact Enforce, +27 (0)31 573 7600, info@enforce.co.za.

Dynamic environments require dynamic solutions

A residential estate security risk treatment plan should be intelligence driven.

According to Derek Lategan, MD of Enforce Security, a residential estate security risk treatment plan should be intelligence driven. Thereafter, one can apply a converged blend of human resources, supported and enhanced by technology. Enforce Security, specialists in risk assessment and mitigation, have developed numerous risk solutions based on rigorous ISO 9001 systems and procedures, all operating within a centralised command and control environment.

Enforce has a number of success stories within the residential estate market that include the deployment of thermal imaging CCTV cameras with analytics. Glenn Allen, Enforce’s technology director, points out that this technology has gained traction as it is able to alert security operators when criminals attempt to penetrate perimeter fences late at night. These cameras are especially useful in areas with very low lighting or where there is a prevalence of mist.

Enforce Security has realised the importance of forming professional partnerships with consultants such as Rob Anderson and Associates. “Over the past 25 years we have leveraged these relationships to design dynamic security solutions that are customised to suit individual requirements.

“Recognising the need for specialised consultative services, Enforce now also offers professional assessment services which include the development of personalised risk management programmes for clients. Flexibility and adaptability remain important factors, especially in an ever-changing environment and economy,” says Lategan.

The company’s estate offering encompasses not only specific security personnel and training but also includes the full spectrum of on- and off-site CCTV surveillance, access control and admission solutions, TV distribution, fire detection, and private investigations.

Enforce Security recently added bundled property services (Excellerate Services) to its business model, which incorporates manned security, security technologies, parking management, property care (cleaning, hygiene, gardening and indoor plants), pest control as well as a variety of ancillary services.

The company’s presence at the Residential Estate Security event allowed it to reiterate its increasing growth in the residential estate sector, highlighted by a number of successful deployments at, for example, Zimbali Coastal Estate.

For more information contact Enforce, +27 (0)31 573 7600, info@enforce.co.za.
Why moving to IP is the best move

The security industry, as with everything else, is moving towards the Internet and IP networks. It’s no secret that the security industry, as with everything else, is moving towards the Internet and IP networks. Advances in this field now offer residential estates and home owners access to the latest in security technology without having to pay a fortune for hardware, installation costs or complex cable runs. But not all suppliers and technologies are equal, and it’s important to find a partner that can provide the right advice and supply the best hardware to successfully complete your solution.

It’s this dedication to quality and service that sets MiRO apart from its competitors. By partnering with industry giants LigoWave and Uniview, MiRO is able to provide its business partners with the best solutions for their wireless security solutions.

Uniview’s IP surveillance solutions are easy to install, user friendly, feature rich and their products are of the highest quality. Their solutions include everything you’d need to set up your security network from scratch, regardless of project size. From network video recorders that can handle anything from 8 to 128 channels, switches and IP cameras with the latest on-board edge analytics and compression technology, to video management software and a free mobile app for easy management and convenient viewing options.

By integrating Uniview’s IP surveillance solution with an estate’s wireless network, estate managers save on complex cable runs, over-priced hardware and installation time. LigoWave’s solutions offer carrier-grade features that are ideal for data-hungry security applications (video footage) that cover large properties. Estates can deploy point-to-multipoint topologies between the homes and guard house of a residential estate and wireless backhaul from the guard house to a remote monitoring site.

Not sure how these solutions will work for you? Contact your nearest MiRO branch where MiRO’s sales staff can provide you with advice on what solution would suit your project best.

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

Robust and reliable

When implemented correctly, body-worn cameras provide tremendous value.

In the ever-changing and harsh conditions in which our security professionals operate it is critical to align oneself with body-worn cameras built for its purpose. These units sometimes get manhandled, put through their paces in harsh outdoor activities and every now and then meets the ground via clumsy hands.

Kedacom’s range of body-worn cameras was designed, keeping the harsh requirements in mind when working in any residential access controlled environment. The unit, as default, features a ruggedised housing with high quality rubber buttons giving one the ability to press them even submerged under water. In essence, the entire range was designed keeping IP67 in mind, protecting the unit from ingress of harmful dust and water submersion at 1 m for 30 minutes. Kedacom’s body-worn cameras also provide drop protection of up to 2 m.

Body-worn cameras have certainly taken the residential estates by storm. They form a vital part in protecting the dignity of both residents as well as contracted security professionals when dealing and interacting with each other. Units such as Kedacom’s body-worn completely avoids the ‘he said, she said’ scenario as the truth behind video and audio recording does not lie. When implemented correctly the units provide tremendous value and should not become a white elephant in any guarding application.

For more information contact Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co
Flexible biometric solutions from Morpho

Morpho discussed the issues around fingerprints for access control on estates.

Morpho South Africa has a strong presence in the residential estate market, with its biometric readers managing access to a number of estates around the country. Nicolas Garcia, sales manager of the company, recently sat on the panel at the Hi-Tech Security Solutions residential estate conference, discussing the issues around fingerprints for access control on estates.

One of the questions posed was ‘what should be done if an estate’s visitor does not want to use fingerprint enrolment to gain access to the complex? ’ Morpho, he says, has a wide range of products that allows control from the most basic to highly secure requirements. Solutions include hardware- or software-based fake fingerprint detection readers that check the ‘liveness’ parameters in the finger as well as the fingerprint itself.

Similarly, the company can offer diversified solutions including the combination of biometrics with embedded card readers and keypad if a pin is required for access, should it not be physically possible for a fingerprint to be read. Interestingly, it is often difficult to enrol small children on biometric readers. Morpho has overcome this with what it terms Juvenile Mode. When activated, it allows the reader to enrol smaller, thinner fingers where the fingerprint has not yet fully developed.

He points out though that in instances where a fingerprint can be read but the guest chooses not to present their fingerprint, the biometric reader should backup the estate policy and not the other way around. In other words, it the estate policy is ‘no scan, no entry’, the technology should allow for it.

Morpho presented its full range of biometric readers from the compact range to its tablet options. Forming the centerpiece of its display was the MorphoAccess SIGMA Extreme biometric reader. Launched at Securex, this rugged successor to the previous-generation Outdoor MorphoAccess 500 series, features a touchscreen and is IP65 rated. The video camera can not only perform the functions of an intercom but also provides mugshot photos and simple monitoring functionalities.

Garcia explains that the Extreme provides three options: (1) fingerprint only; (2) best effort, which produces a mugshot of whoever/whatever is in front of the reader as a finger is presented; (3) face detection mode, whereby the reader first seeks out a definite face image and then takes a mugshot as a finger is presented to the reader.

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

Smart, integrated security solutions

Paxton offers simple access control solutions for residents and installers.

Electronic access control can provide an efficient and convenient way of securing a residential building instead of using traditional locks and keys. Tokens are issued to allow access through the controlled doors and can be blocked easily if they are lost or stolen. Blocked tokens will then not allow access through a controlled door.

Access control offers flexible control over users’ access rights too. For example, all residents can gain access through the main door of a building, while at the same time specific areas could be managed with higher security by setting varying permissions depending on each user. Visitors can be granted temporary access rights, for example contractors working on the site, with the permissions set to expire once their work has been completed.

If you are looking to extend building security beyond access control, it is also possible to integrate networked access control with video door entry systems, CCTV, fire and intruder alarms.

With over 30 years’ experience, Paxton is a market leading designer and manufacturer of IP access control and door entry systems. Our products harness the latest technology to provide powerful, yet easy to specify and install solutions.

Paxton’s Net2 system is a user-friendly and flexible networked access control solution that is designed to make the management of any building incredibly simple.

Sitting directly on a building’s network and managed via a central PC, it allows a building concierge, caretaker or managing agent to manage security from one central platform, making administration straightforward.

Comprising smart, simple door hardware and advanced, yet easy to use software, Net2 moves beyond the basics of securing access to doors to provide features like energy saving, system integration, building management and security lockdown.

Net2 Entry, Paxton’s award-winning video door entry solution is a simple security solution that allows you to identify and authorise a visitor before they can gain access into a building. It is easy to use and comes in a stylish, discreet design, offering a flexible and high security solution that suits a range of environments including residential complexes.

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

The benefits of automated visitor management systems outweigh the cost.

Electronic visitor management systems are generally placed in the same category as other security systems – a cost centre. However, the benefits which can be derived from deploying an appropriate card/biometric reader and software far outweigh the initial investment cost.

Powell Tronics has built a solid base of clients in the residential estate sector, with a number of premier estates around the country currently successfully operating its access control and visitor management solutions.

For the fourth consecutive year, the company participated in the Hi-Tech Security Solutions’ Residential Estate Security Conference as a premier sponsor. John Powell, CEO of Powell Tronics, says that the event provides the company with an unrivalled opportunity to specifically address one of its major target audiences in a one-on-one environment.

This year’s event saw Powell Tronics promoting the use of its in-house developed PT-Guest visitor management software. According to Powell, PT-Guest caters for the pre-authorisation of visitors to an estate with a link back to a specific resident.

“When it is used together with a licence disc scanner, we can ensure that accurate information is captured when a visitor arrives onsite. No longer will the infamous ‘M Mouse’ be scribbled in a traditional visitor book when a guest visits. The system doesn’t stop there though, as it then ties in a visitor request to the fully integrated access control system. Full details of the visitor’s transactions are then provided via a web-based reporting system for analysis after the visitor has left,” Powell explains.

Powell continues that the company can also offer a scaled-down version in the form of PT-Scan. This Powell Tronics-developed software offers a simple interface that replaces the traditional visitor book with a small hand-held scanner that also provides a host of web-based reports.

Powell Tronics also used the event to underline the advantages of the new MorphoAccess SIGMA Extreme terminal. “The MorphoAccess SIGMA Extreme is more rugged and durable than any of the readers Morpho has previously released. It has an IK09 rating which means that the device is protected against 10 joules impact, or the equivalent impact of a 5 kg mass dropped from 200 mm above the impacted surface,” says Powell.

Powell Tronics adopts a customised application philosophy that entails consultation with installers and end users to determine the best hardware and software for their specific access control and visitor management requirements.

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

Supporting residential estate security

Integrated residential access control solution from ZK Teco.

This year ZKTeco South Africa provides the residential estate security sector with the latest innovations in biometric technology. ZK has developed products that provide residential estates with a platform to integrate access control devices with visitor management apps.

The ZKBioEstate solution (part of ZKBioSecurity) makes use of UHF readers, car tags, parking barriers, full height turnstiles with fingerprint and RFID access control systems. All these can be monitored on one platform: ZKBioSecurity.

The UHF reader is waterproof and is suitable for use in a wide range of RFID applications, such as transport management, vehicle management, car parking, production process control and access control. The ZK parking barrier prevents entry of unauthorised vehicles to restricted areas. It is raised by the linkage between the gate, the remote control, access control system, long distance reader and number plate recognition system. The LED light tape changes colour in boom raising or lowering, thus helping the driver avoid hitting it, and a pressure plate ensures that the barrier gate doesn’t close too soon.

The biometric full height turnstile with fingerprint and RFID access control system, which features a modular design, visible indicator, semi-automatic mechanism and SUS304 stainless steel cabinet, ensures that pedestrians entering into the estate can also be recorded. The new ZKTeco visitor management app not only enhances efficiency, it ensures that visitors can be registered within seconds, with all necessary information captured.

The app enables authorised personnel to preregister visitors, thus helping to streamline the waiting process. This app also ensures that the handling of visitors is in accordance with estate policies. Visitor approval is sent to the authorised person via the app and the proper access rights can be assigned. All information is stored in a secure database and can be conveniently retrieved for repeat visits.

This visitor management app also allows the user to track visitors, assets and deliveries as they enter and exit the premises. It helps improve the efficiency, productivity, security and visitor service of any residential estate.

ZKBioEstate is a comprehensive security package offered by ZKTeco that can complement any residential estate and can be customised to fit the specifications of any estate.

For more information contact ZKTeco (SA), +27 (0)12 259 1047, johlene@zkteco.co.za, www.zkteco.co.za
The scouts’ motto of Be Prepared is probably more suited to those responsible for managing the security of residential estates.

The role of a security manager would be hard enough if you just had to deal with the criminal element trying to gain entry to your estate. Unfortunately, security managers are in a situation where they need to deal with ever-growing criminal attacks, but also with obnoxious residents, poorly performing staff and service providers who want to take the money and run. And that’s on a good day.

To get a better idea about the challenges of securing a large estate, Hi-Tech Security Solutions invited a few security managers to join us in a round-table discussion where we discussed the realities of their jobs. As is the case in most security managers’ lives, a couple couldn’t make it due to unforeseen circumstances on the day, but we were joined by:
- Mark Lightfoot and Hans Jorna from Blair Atholl.
- Juan Koch from Eagle Canyon, and
- Titus Sithole from Monaghan Farm, who joined telephonically.

One of the biggest challenges Sithole is dealing with at the moment is the maintenance of security equipment. There is no shortage of volunteers when it comes to installing a big security solution, but there are few companies that will commit to effectively maintaining it for you over the long term. Then, he notes, when you do find someone to handle maintenance, they only focus on one aspect of your solution, such as access control, for example, meaning you still need to look for another service provider for surveillance and other technical support.

This leaves the security manager in a tight spot as maintenance must be undertaken regularly by skilled people. And if one service provider doesn’t live up to the job because they are looking for the big deals, the change-over to another untried provider is fraught with uncertainties and a potential for security disruptions.

While this is one of the challenges Blair Atholl also faces, given all that could happen
Lightfoot says his biggest challenge in terms of security is the day. "What's going to go wrong in a day? No matter how precise your planning is, you can't account for everything."

And the things of the day simply carry on. From break-ins to community involvement, fence statuses and so on. And he agrees with Sithole that service providers can be a challenge. There is no shortage of candidates to install a solution, but after-sales service is where the service provider market generally falls flat. The same applies to guarding service providers. The estate needs to manage them carefully to ensure it gets what it is paying for. You need not be aggressive, but you need to stand your ground and demand performance.

After-sales support
Jorna handles the maintenance and infrastructure for Blair Atholl. The problem he faces is service providers not having stock available when equipment breaks or fails due to an attempted break-in. He often finds that sending something to be fixed results in the device being missing for three to six weeks before it comes back. That means the system is down, or at least vulnerable if the estate doesn’t keep its own store of spares, which is very costly when it comes to surveillance or access control products.

His second biggest challenge is nature. Fire is always a problem in winter and electrical cables used for fencing, for example, are ‘absolutely not fire resistant’. The cables, the bobbins and everything else are plastic and melt. A small veld fire can mean your electric fencing is gone.

And then it seems jackals around Blair Atholl are able to chew through electric fencing, regularly resulting in an alarm in the early hours of the morning. Apparently the electric fencing industry has yet to develop a jackal-proof solution.

Jorna also confirms the previous comments on service providers. “As long as they can sell you something new, that’s fine, but the repair side needs to be improved dramatically.” He would like to see a joint venture between a few estates and a service provider to ensure a reasonable amount of spares are kept in stock. This would assist Blair Atholl and other estates that are in the same boat.

What do you want from security?
When trying to understand all the challenges one has to face, Lightfoot says the first step is to define what security is. "What do you do in security and what forms part and parcel of security?"

At Blair Atholl, security goes beyond access control and guarding. Lightfoot says it incorporates anything from catching dogs and snakes to being a paramedic, to being the guy that goes to your wife’s aid when she gets stuck without a spare wheel, and so on. "Security is, in a nutshell, everything. So you need to decide on how you are going to approach your onion with lots of layers.” (The security onion refers to the layers of security, each built on top of the other.)

In fact, Lightfoot includes maintenance in his security operations, because, in his view, maintenance is a critical part of security. "I can’t run the security if the maintenance doesn’t work and vice versa," Lightfoot states.

Koch says there is no silver bullet for the problems estates face in terms of security. He says Eagle Canyon’s security focus is to render service to residents on all layers of the onion. “Our motto is, how can we be of service to the residents. The residents, at the end of the day, must experience a seamless integration of technology, hardware, software and everything in between.”

An important part of the layered (onion) approach to security is making sure the correct triggers are in place to initiate the correct responses to various situations, be they criminal, fire-related and so on. Koch says you must ensure every event triggers correctly in your control room, which will then oversee the response required. Critically, this will also require the seamless integration of all aspects of the security operation, whether technical or human, internal or external.

“IT’s the integration of all those levels into a well-oiled, functioning system that allows our residents to go off to work in the morning and know that everything will be looked after, from animals that are lost to kids that are safely back from school. Ensuring that everything is looked after, almost invisibly, is the biggest challenge.”

And when it comes to technology integration, seamless integration is the key to success. Koch says Eagle Canyon has everything centralised into the control room which is run by a service provider. The control room really is the heart of the estate’s security. In addition, making the data collected in the control room available to everyone who needs it is another critical aspect of effective security.

In Koch’s case, he has access via a smartphone, through which he can log into the estate’s cameras, see what’s happening in the control room and so on. He also gets regular reports on the security situation at the estate.

Service providers who are able to make the relevant information available to the estate manager and those responsible for security in the HoA will find their jobs much easier.
Continued from page 27

as having the relevant information ensures decision making becomes so much easier. It also allows the security leaders to identify and mitigate emerging risks before they become a problem. And bringing all that information into one device for easy access makes the process efficient and much simpler for all concerned.

Processes and scenarios

When it comes to human resources, Sithole raises the issue of which option is best for staffing an estate’s security function. The benefit of internal staff is they are committed to the organisation and can get to know all the relevant rules and processes, as well as the people they work for and with. However, as Sithole notes, ensuring they stick to the processes set by the estate can be difficult when individuals only comply when under observation.

He notes that, despite having policies and procedures in place and in writing, as well as going through training processes, there are some that just don’t want to adhere to them. This is not only a breach of their contract, but it can result in security vulnerabilities and the relevant consequences in a worst-case scenario.

Lightfoot says this is why he believes in contracting a guarding service provider. The guards and operators who meet the standards of the estate are just as valuable to the security function as if they were employed directly, but if someone refuses to stick to the prescribed processes, the estate can simply ask for that person to be replaced. If the individual was directly employed that can become more of a challenge. Of course not all security functions can be outsourced so there is still a need to select internal employees carefully.

Koch adds that a service-level agreement (SLA) is critical in this respect. “I as the security manager know that I am only as good as the people reporting to me and those in my command centre. I therefore work closely with service providers and internal staff to ensure my SLA is in place and is being adhered to.”

Added to this, Koch believes discipline among the security staff is important, as having processes and scenarios for them to work according to. Standing operating procedures (SOP) that are managed and updated where required is the first step in ensuring everyone works towards the same goal.

He also believes in the positive implementation of discipline. “As a manager, you need to walk that extra mile with the individual who is battling to align himself with the standing operating procedures, policies and scenarios.”

All round table participants are believers in scenarios, where every incident a security officer may face has been dealt with in a scenario, giving them a clear path on what to do when it happens. Koch gives the example of when a resident arrives at the estate, driven by a visitor. Most often, the resident leans over from the passenger seat to scan a biometric for entry, which is a breach of protocol at the estate and the access guards need to know this and how to handle it.

Adherence to the security policies of the estate applies just as much to third-party providers. This is why Koch says the contract must detail what is expected from them and there must be people who are held responsible. Eagle Canyon has regular meetings to address these issues, both with members of the estate’s board and the service providers themselves.

Part of Lightfoot’s SOP is that his team always needs to know what to do in any given situation. In the instance where they don’t know what to do, his standing rule is for them to phone him. This ensures that if something goes wrong, the people involved will have the backup to say they did call and then followed instructions.

Risk management is preparation

While the talk revolves around security, estate security managers are actually risk managers. It is their job to identify risks and the probabilities of those risks happening. In every risk management scenario, the goal is to be prepared for possible or known issues, so that the response when they happen is streamlined and the negative impact minimised (although the best scenario is if the preparations prevent those risks from ever happening). Estate risk is no different.

Lightfoot and Jorna give the example of maintenance. Their estate has an issue with veld fires and the impact they can have on their electric fencing. Good risk management therefore dictates that fire breaks should be prepared before winter sets in to minimise the potential for damage. Although, this doesn’t always stop the damage when flames move at four metres-per-second, as has been experienced at Blair Atholl, it does minimise the risk overall.

An estate is a continually changing environment, says Koch and you need to be on top of whatever the latest situation is. Whether it’s school holidays which means more kids around during the day, or being situated next to an industrial area with the implications thereof, being prepared for anything is the job. Do your due diligence, states Lightfoot. You need to know your risk, build a risk profile and manage it. The more you know, the more you can prepare and the better your security function performs.
Invest in Secure access

It’s a lifestyle.

When you add Suprema’s internationally acclaimed access devices to your integrated estate security solution you can expect a comprehensive access control platform which is intelligent, fast, accurate and easy-to-use. Not only functional, it also lives up to the lifestyle of the estate through beautiful design and flexible mobile management.

So the next time you’re at the drawing board, consider Suprema. We have a device for every need. Indoors, outdoors, hands-free, with and without biometrics.

Over-and-above secure gate entry, Suprema’s extensive range can also be incorporated directly into homes, providing residents with a key free solution that is easy to use and manage.
The total cost of ownership can hurt your security budget

By Andrew Seldon.

The purchase price is only the beginning of your security spend. The TCO tells the whole story.

Total cost of ownership (TCO) became famous as a concept in the last century when Gartner made it a household name in the IT industry. TCO is basically a financial estimate that allows buyers to determine the full cost of a product or service over its expected lifespan.

In the security industry, the cost of a surveillance camera, as a simple example, would include the purchase price, the cost of maintenance over its lifespan, and could even include the cost of bandwidth required to transfer images to a central server, the partial cost of the operators monitoring the camera and so on.

Of course, in an estate environment, nothing will be as simple as that since you have multiple cameras, access control systems, electric fences, significant network installations, control rooms and their equipment and people, as well as guards and their equipment to consider. And that’s just a starting point.

Unfortunately, most people see the initial cost of the hardware and software as the cost of the solution, ignoring maintenance and upgrades, breakages and other aspects that are a normal part of any security, and in fact, any electronic system. Getting a good idea of what the full TCO of the system is over its lifespan – say five years, although this changes depending on what products you choose – is important because you need to budget for all the ‘small things’ you will need to pay for over that lifespan.

Budget too little and you will have a choice of either asking for more money, which is never a pleasant option; making sacrifices in terms of postponing the purchase of new and improved solutions because you’re spending more on maintenance; or cutting down on maintenance (or using a cheaper service provider) in order to afford new equipment – a choice that can have significant consequences on the effectiveness of your security as a whole.

Given the importance of a reliable TCO estimate at the start of a project, Hi-Tech Security Solutions asked a few experts for some insight into what exactly goes into a TCO calculation for a new installation or a significant upgrade.

Finding your formula
Brian Sharkey from Security Management Consultants (SMC) says there is no perfect formula. “We have found that each project and every client (homeowners association and body corporate) have different needs. Dependent on those needs, we can estimate the TCO over a number of years.”

He adds that issues such as maintenance costs are vital in the calculation, and not just the initial costs. “We firmly believe that you can spend millions of Rand on upgrades and new installations, but if you don’t include a detailed maintenance plan, you could be wasting your money. Another important component in calculating the TCO is to provide for ‘unforeseen circumstances’: Mother Nature, for example, can be an unforeseen circumstance through direct lightning strikes despite installing adequate lightning protection, as can floods which have been known to break 50 and 100 year flood lines.”

Continued on page 32
You **REALLY** should be speaking to us!

As the security industry and everything else is moving towards the Internet and IP Networks, you need a partner that can provide the right advice and supply the best hardware to successfully complete your next project.

At MiRO, we are **computer network specialists and experts in wireless networks**. We can assist you to plan a wired or wireless network of any size to provide reliable capacity for the demands of your project.

All MiRO hardware solutions are backed by our technical support services team to make sure you get everything working as planned. MiRO offers proficiency and certification training to help your team master the technology you are deploying. Project finance solutions available.

086 123 MIRO (6476) | sales@miro.co.za | www.miro.co.za
Continued from page 30

SMC also always advises clients to build in a reserve for when insurance doesn’t cover the full expense of repairs or replacements.

Etienne Jurgens, technical operations manager at Xone, “Especially in larger installations where the investment is typically in the millions of Rand, it becomes the responsibility of the security adviser to ensure the correct investment decision is made by the client. Sadly, TCO is normally not the main driver when any investment decision is made.”

The immediate cost of the system and availability of funds are always the driving factor, he says, with TCO only becoming a factor when the costs of different options are similar. The TCO therefore is only quoted at a very high level with the following items typically focused on:

1. Period of warranty offered by the supplier when equipment becomes faulty.
2. Operational life expectancy of equipment before it is due for replacement.
3. Maintenance time and cost required on equipment to keep it at its operational best.
   “We find that TCO is therefore limited to the yearly maintenance required to keep the system operational.”
   “For a new installation, all elements need to be taken into consideration,” says Sasha Bonheim from Axis Communications, focusing on the surveillance aspect of TCO. “This is a somewhat challenging task. For example, looking at the infrastructure; is there power on the perimeter fence or does one have to install solar panels? Then you look at the distance the perimeter covers and calculate how many cameras you would need.

   “From there you can start to assess your costs for network, storage, cabling and accessories. These are all physical costs. From there we turn to maintenance, staff, training etc. Using a TCO model can help capture all the costs associated with a video surveillance system over its complete lifecycle."

Pieter van Wyk, senior manager: fire and security, BT-SA, notes, “When I do costing on a design for a new installation or an upgrade on a complex or estate, I look at the environment and outside conditions.

   “For example, if I do a design on a solar powered system, which is the new-age or green way, I would do a special costing or maintenance and SLA proposal to accommodate, for instance, the battery life of your solar system. The fact is, batteries never last long in our harsh temperature conditions in South Africa. The ideal temperature for a battery is in a dry temperature controlled environment consistently on 20 to 22 degrees Celsius.”

The camera question

When looking at a security operation, we often focus on the impressive technology like surveillance cameras, but forget about everything else required to make the cameras worthwhile. We asked what percentage of a project (roughly) is spent on cameras and what is spent on infrastructure (networking, storage, servers, software and so on)?

Surprisingly, while cameras may be the coolest toys to play with, they do not make up the largest cost in a project. Bonheim says that they can account for roughly 16% of the total cost. “If we break it down, we can see the largest costs have to do with maintenance, coming in at around 19%.”

Maintenance and repair costs play a significant part of any TCO. The importance of product reliability is often underestimated when considering the cost of maintaining and operating a system. High product quality is, of course, a critical aspect to keeping maintenance and repair costs to a minimum.

She adds: “Every project has a unique cost distribution and it is up to each project team to determine which cost factors to take into account and how to judge the monetary aspect of each factor.” (See the cost breakdown in Figure 1.)

Sharkey agrees, noting, “We have been fortunate to have been involved in some very large and some very small upgrade projects on CCTV, and often the ‘back-of-house’ equipment, such as networking, servers etc. are not considered at the outset. Clients are often not fully aware of the advances in technology that are available, and it is critical to explain what the advantages are in planning for future growth in the system. Often the infrastructure costs can be greater than the actual cameras.”

Jurgens states that the answer is not straightforward and there are many factors that influence the spend on CCTV cameras compared to their supporting equipment. These are typically:

1. Layout requirements of perimeter CCTV where the perimeter is influenced by geographical limits, like rivers or hills or by municipal zoning that are quite often not straight in nature.
2. Ease of routing of cable compared to wireless costs.
3. Information retention time required by client.

   “To look at the typical percentage spent on cameras compared to the supporting infrastructure, I had a look at our last 10 quotes for CCTV equipment with an ex-VAT cost of more than R2 million. These projects also required that the CCTV equipment was hard wired with no wireless connectivity.”

Figure 2 reflects the percentage of the camera cost compared to the overall cost of the installation. Jurgens advises that the average of the cost spent on cameras only was 52%, but as mentioned, this depends on various factors.

   “Additionally, the brand of camera quoted for also has a huge impact. As an example, a quote recently supplied for R4 million worth of CCTV equipment, the camera contribution to the total overall cost was 69% for brand A compared to 51% of brand B, with the latter using six more cameras than brand A.”

Van Wyk adds that it also depends on the project. In a perimeter surveillance solution, if you choose to hard-wire the whole solution...
there is a huge amount of trenching, conduits, labour and cable involved which will push the cost of the surveillance aspect up.

“Not only is it expensive, but time consuming and a big inconvenience for the residents of the estate, assuming it is an existing estate. Wireless and solar options are a lot faster to install and not as messy, and are thus less inconvenient to the end user.’

And then there’s the fence
As noted, the surveillance aspect is only one area of your security’s total cost. Even for those estates with significant investments in cameras along the perimeter, they still need a fence or wall of some kind. And while it’s simple to get a costing for your perimeter fence at Rx per metre, what else should be considered.

Each perimeter is a custom design, says Van Wyk. “For this reason I always walk the full perimeter to provision for all such different encounters like streams and different types of walls. For instance, most of the designs I have done includes the fence changing from a brick wall to a palisade fence at some point. This is, to me, the most common change you will find.”

Sharkey has a similar opinion. “We have in recent years successfully devised and undertaken the project management of a number of perimeter upgrade projects for estates with perimeters from as small as 1 km to as long as 8.5 km. Each one is different and often extremely complex due to difficult terrain. Some perimeter upgrades have been undertaken on rocky terrain, often with stream and river crossings.

“On very large and complex perimeter upgrades we recommend working with quantity surveyors to ensure costs are controlled on not only the supply and installation of the final solution, but also the amounts of concrete required and the types of under-dig solutions proposed. We have found that in erecting a very secure perimeter solution, cameras are not required initially, but should be planned for in future expansion, with the infrastructure being provided at the outset of the perimeter project.

Jurgens says the perimeter budget is never a simple calculation as various factors have to be taken into account. These include steep slopes or whether there is an under-dig and so on. However, he says most of the larger estates have cameras to support their physical fence, so the final cost will include the combination of cameras, poles and other necessities.

Focusing on cameras as a crucial part of perimeter security, Bonheim notes that thermal

Continued on page 34
Continued from page 33

technology has proven to be the best option in long distance detection on the perimeter as it allows for detection in fog, haze, pitch darkness and extreme sunshine. “This solution coupled with an advanced analytic that allows for early detection will minimise false alarms, thereby reducing the overall labour costs of guards physically manning the perimeter.”

The maintenance gremlin

As mentioned before, maintenance is always a factor due to normal wear and tear, bad weather, vandalism, accidents and so on. It would be great if there was a set formula an estate or systems integrator could use to calculate a reasonable value that will need to be spent on maintenance over the course of the security solution’s lifespan. But does one exist? Or is it a case of taking a chance that your technology will behave and succeed against the elements?

Bonheim says that maintenance plays a huge role when considering a TCO lifecycle. “As mentioned earlier, it is important to consider the quality of the product that you are installing as this will be a factor when keeping repair costs to a minimum. Unplanned events that cause a system to fail can lead to excess costs for an estate.

“For example, in a residential estate, if the surveillance system fails, it could lead to very high costs as extra security guards may need to be dispatched and other measures taken. It’s always important to invest in good quality products that are reliable and have been tested to withstand extreme weather conditions.”

Echoing this, Jurgens adds that security upgrades do not have a set time span of operational life as it can vary depending on when what piece of equipment was installed. “The cost forecasted to be spent on a security installation is therefore based more on past experience per financial year. Taking the cost over a set number of years gives you an average spent on the security installation cost.”

Van Wyk puts a number on this, saying at least 10% of the total value of the installation over three years is a reasonable amount to budget for maintenance. This will allow for a few cable replacements and for a few cameras lost to lightning or other damage over that timeframe.

Sharkey’s advice is that maintenance and service-level agreements (SLAs) are critical to the long-term success of a security installation or upgrade. The cost of these agreements varies, dependent on the conditions and terms of the contract proposed. “A strictly enforced SLA ensures the client receives value.”

Buy or use?

When considering costs, the vast majority of estates look at security as a cost centre and something they have to spend huge sums of money on. While we can’t get away from the need to spend on security, there are options apart from the big spend. In other words, estates can look at a leasing or rental model.

In this scenario, service providers offer a full solution (products, installation and maintenance) at a set monthly or annual price, with annual escalation all encompasses in a contract – including a service-level agreement. In this way, the service provider is responsible for the technology as well as its functioning (and perhaps even the guards and other security personnel), and they are contracted to deliver a specified service in terms of uptime, response times and so on.

Sharkey says rental options are attractive in the short term as a quick solution can be obtained without having to go through the often lengthy processes trustees are required to follow in spending large amounts of owner’s money, or raising special levies to pay for the solution.

“The advantages are that while paying for the system at a higher cost in the longer term than an initial outright purchase, full maintenance and upgrades for hardware and software is included. The contractor/supplier are required to keep to their side of the rental agreement over the agreed period in terms of services and ad hoc repairs.”

He warns that an important aspect to look at when considering this type of option is the right to sell the rental agreement should the existing service provider’s business be sold during the contract period. “That is something to take cognisance of in the contract.”

Van Wyk notes that the rental or lease option would be more expensive in the long run due to interest and escalations, but it is an option to avoid a huge capital expense. “At the end of the day, it is up to the client to make that decision. I would however recommend, whether or not they take the rental agreement or the capex option, to include offsite monitoring. This will allow them to save on physical security guards, control room layouts and onsite control room operators. This can all be handled offsite at a monthly rate.”

Another word of advice comes from Jurgens, who says it’s important to split the services at contractual level. “This will allow one to separate the installation, maintenance and any other services. If your integrator is not performing on any level, you can simply terminate that portion. You do not want to be tied to a company providing poor maintenance simply because they did the installation.”

He adds that extended warranties are very desirable in this context to align the leasing period to the lifespan of the system.

It’s clear that the TCO of a security system is far more than the purchase cost, and far more than what we can include in an article. However, it is clear that planning the installation or upgrade of a security system requires more than mapping out vulnerable points and deciding how you are going to deal with them, and then getting a quote for a bundle of technology. Maintenance, upgrades, replacements, personnel and a host of other costs all add up to the real value of the system you’re installing, and that value should relate to the protection service the solution will provide.

In cases where estates save a few Rand by buying cheaper technology at the start of the project, which happens more often than any will admit, the savings are almost guaranteed to be lost over the next few years as maintenance and technical callouts increase. And while we all want a bargain, in the case of security, are those few Rand worth the risks residents and staff face when security fails?

For more information contact
• Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com.
• BT-SA, 0860 105 183, sales@bt-sa.co.za, www.bt-sa.co.za.
• Security Management Consultants, +27 (0)11 795 2693, brian@smc.co.za, www.smc.co.za.
• Xone Integrated Security, +27 (0)82 906 7600, ian@xone.co.za, www.xone.co.za.
Do you know who’s on your ESTATE?

Knowing who is on a residential estate is one of the biggest challenges facing estate managers. This challenge increases when there is a golf course or similar public facilities. Add in contractors, residents’ staff, estate staff and visitors, and that’s a lot.

That’s where Impro Technologies’ access control solution can help.

Features include:

- **Mobile phone solution** with their tag, for residents to enter by presenting their phone instead of a tag
- **Biometric readers**, such as fingerprint or face, for indoor and outdoor use
- **Automatic number plate readers** to reduce queues of vehicles and increase resident convenience
- **Emergency features** on the management software to immediately lock down or open all access control points
- **Integration** with other equipment such as CCTV and intrusion alarms.

For a free consultation, simply visit [www.impro.net/estate](http://www.impro.net/estate), complete the form and we’ll contact you to discuss your specific needs – no obligation, no risk.
Buy and manage, or use?

By Andrew Seldon.

Security-as-a-service is a reality for many estates in South Africa.

The as-a-service concept has found acceptance in many areas, such as IT, where companies and people are taking the option of using applications, systems, platforms and more in the form of a rental contract rather than going through the hassle and costs of buying, installing and managing everything themselves. An example in the consumer space is using Gmail as your email service, you don't have to install or manage anything as Google does it all, and you just use the email service.

The touted benefits of these services is that companies pay for what they need and use, while the service provider handles all the hard stuff. In the security industry we have seen similar concepts in the form of video surveillance-as-a-service (VSaaS) and even in some remote monitoring scenarios where the customer pays an annual (or monthly) fee and the monitoring company buys, installs and manages the technology, while providing operators to handle surveillance duties.

But how popular is this in the security market, and especially in the residential estate market? Most estates, as well as most companies still prefer to splash out on buying their cameras, access control systems, software, hardware and so on, only relying on service providers to do the installation and maintenance, and perhaps manage the monitoring.

Hi-Tech Security Solutions decided to find out more about the as-a-service model and how it is being adopted in the estate security market. We spoke to Chris Lovemore, CEO of ELF Rentals, as well as Dave Sleep, reaction division director at Stallion Security.

Lovemore says the guarding aspect of security-as-a-service is very mature. The move is now towards “reducing costs and improving effectiveness using the full maintenance operating lease model of electronic security equipment, where the service provider funds the equipment and then provides a technical backup service to the equipment to ensure it is fully functional at all times”. The service provider also takes the risk of any equipment failure.

“The more established and professionally managed estates have increasingly adopted this approach over the last 10 years as they have realised that electronic security equipment that is well-maintained by a reputable and well-resourced service company that carries the funding risk, results in better overall security.”

It is important, however, to ensure you partner with a professional business that offers a holistic approach and a provider that is not only geared to enable payment plans on technology solutions, but those that will do so with a view to reducing manpower to enable the cost to remain, or be as close as possible to current spend, adds Sleep.

He also notes that these service models provide an opportunity for estates and complexes without large cash reserves to also implement a solid security infrastructure. Not having funds should not mean residents and their assets are poorly protected.

While the idea of everything happening invisibly while we simply reap the benefits of the service is appealing, the problem with the security industry is that it is a people industry. In other words, there needs to be human interaction on a daily basis – a guard at the gate for example. So which security functions can be translated into an as-a-service model run without the security manager looking over your shoulder?

What services work?

This depends on the provider and what they are willing to bring to the table in terms of a solution, explains Sleep. “Cost plays its part, but there are no current surveillance systems that cannot be operated at optimum with the technology we have available today. The pricing models for using data and bandwidth differ, but we do not believe this is a hindrance to providing technology.”

Lovemore’s experience dictates that there are a host of services currently available, these include electric fencing, CCTV, access control, networking of security devices, power management and data storage. “Surveillance is very much a service offering, but it needs to go hand in hand with a service provider that ensures the equipment is fully functional at all times.”

He continues, “The advantage of an ‘as-a-service’ security offering where a service provider has taken risk in funding the installation and then services it is that estates can hold their service providers accountable. Service providers are incentivised to do high quality installations and use quality equipment since they will suffer the consequences of poor workmanship and/or inferior equipment.”

Of course, finding a service provider that can finance a security project upfront and recover its investment over time is a challenge.
as well as in serving estates. Elf offers its estate
customers a turnkey electronic security solution
including electric fencing, CCTV, access
control, networking, power supply and
data storage management.
“We do this from design,
to installation, to providing
the capital and then to maintaining
the equipment in such a way that it operates
to its maximum operating
efficiency at all times,”
explains Lovemore. “We offer a
5-year extended warranty on all our equip-
ment and assume the risk of equipment
failure outside of the manufacturers’ warranty.
In addition, we supply insurance on all our products so that we can quickly resolve and restore problems caused by lightning and other insurable incidents, and then deal with the claim without it having an effect on our clients’ administration systems or their insurance premiums.
“Our services are primarily onsite, however,
our technicians are increasingly able to
manage, identify and solve problems via
offsite network access.”
Stallion’s services depend on the estate or
complex. “Those that have control rooms can
have the on-site option as there is no further
money to spend,” says Sleep. “It is, however,
not recommended to have to spend huge
amounts of money to put this together and
remote site monitoring is a fantastic option
which is proactive and will be a definite enhancement to security.”
He continues that Stallion offers services as follows:
• Physical security at all grade levels,
• Dedicated vehicle service, manned by
either armed response personnel or secu-
ritry officers at Grade B level and above,
• All technology options including CCTV,
access control, remote monitoring, set-
ing up control rooms, biometric systems,
Bin the book, evolve to electronic

Hi-Tech Security Solutions looks for the solution to the visitor management issue.

Visitors to residential estates are a regular, daily occurrence, so learning how to effectively handle their entry and movement throughout the estate’s grounds is critical. There needs to be a balance between ensuring that the security of residents and tenants is upheld, but without unnecessarily hindering the passage of visitors, employees and contractors. Hi-Tech Security Solutions looks for the solution to this thorny issue by chatting to some industry visitor management veterans.

A good visitor management solution can be used in a court of law as corroborating evidence. It not only helps prevent crime, it also makes a statement to anyone wishing to visit the complex, as well as to criminals. Furthermore, it will greatly enhance overall estate security while helping minimise opportunities for criminals.

According to Mark Paynter of the Terpay Group, the question of denying access to a visitor if they refuse to cooperate with regard to presenting a driver’s licence raises often-asked and important points which have several relevant considerations. The legal onus is on the estate to ensure compliance with legislation as well as with relevant commercial agreements with insurers and other service providers. Property managers and contractors could be held individually or jointly criminally and/or civilly liable for failure to comply with legislation, especially in the event of death, injury, or loss.

“An even lesser known fact is that in terms of the Occupational Health and Safety Act, incorrect visitor register entries could potentially mean a criminal record as per Section 39. (4). Body corporates/trustees/security companies therefore have several obligations in terms of the occupational health and safety act, the sectional title act, and in terms of their public liability insurance cover,” says Paynter.

“These obligations, logically, should override and supersede visitor comfort, satisfaction, or ease of access. So first and foremost, they need to ensure that they are not putting the estate and the residents at risk due to a non-compliant process or procedure,” he adds.

In summary, the trustees can legally and should regulate visitor access to the common property. At worst, the widely acknowledged ROAR (Right of Admission Reserved) applies and can be enforced.

John Powell of Powell Tronics says that generally, if an estate is private property and right of admission is reserved and is clearly stated in their constitution, then they can enforce specific rules like forcing contractors to be certified through their security process before they can do any work on site.

Dave Rampersad of SNIPR South Africa adds that in general, estates should erect signboards that clearly indicate that the right of admission is reserved and that the driver’s licence and vehicle registration plate and disc will be captured as they enter the premises.

He continues that the majority of the market is still using the intrepid visitor book, but in order to ensure speed and efficiency with visitor management, it is important to go the electronic route. This not only allows the estate to verify the visitor’s details, but it also mitigates risks. He explains that the system SNIPR uses does not capture the information on a driver’s licence, but rather scans the barcode and decodes the information thereon in terms of the person’s name, surname, ID number and photograph. The GateBook visitor management system also scans the vehicle licence disc and will highlight if the vehicle has been used in a previous crime or has been flagged as suspicious, should their SNIPR module be added to the device.

Powell says that the most efficient way to speed up the processing of visitors is to use features like the one found in PT-Guest, which allows for the pre-authorisation of visitors. On arrival the visitor simply has to be verified by the security staff and linked to the host they are visiting and the correct data is then quickly acquired by portable units that can decode the driver’s licence of the visitor as well as the vehicle registration details.

This alleviates the time that the security guard would typically need to gather information from a visitor and to contact the host. A similar process is followed for contractors, whereby the verification and management process would apply to allow access for the contractor for pre-specified scheduled times for precise hours and dates. At any other times outside these times, a pre-authorisation override would be required from a host.

Once the visitor has been verified and has passed through the entrance gates, how does one track their movements? This, says Ramperaad, is rather challenging for most residential estates to find a cost-effective solution, as while it is possible to see where they enter and leave an estate and where they are supposed to be going with traditional surveillance monitoring systems, the routes in-between these points do not always have surveillance and may not be set up strategically to track vehicle movement and irregularities.

However, says Powell, it is possible but the proviso is that you have additional access points within the estate. Therefore, there will be a primary entrance gate then secondary areas that give access to common areas like golf courses, gyms, clubhouses etc. Using a zone occupancy report one can see what zone the visitor last accessed.

Less haste, more speed

Continued on page 40
Identiscan Access Control

- Instant scan using lazer technology *(not camera)*
- Scans all forms of South African ID’s & Licenses
- Water resistant
- Ruggedized Rubber Case
- Cradle charger *(not fragile mini USB)*
- You can open the gate from the hand held unit
- User definable fields for data to be collected
- Logs and controls contractors & their workers
- POPI compliant
- *(PushToTalk)* application
- Dual Sim
- Time & Attendance application
- Remote management

**R13 999 + vat**, thereafter you pay R499 per month - Software as a service. Your Data and photos are stored on our secure cloud server on a month to month basis. *(no contract)*

R13 999+vat
(Finance available)

FOR MORE INFORMATION CALL:
021 701 7777
www.identiscan.co.za
VISITOR MANAGEMENT

Continued from page 38

“If the visitor does enter the estate and then parks their vehicle, there isn’t a lot to prevent them from entering other zones if there is no physical barrier. To combat this one can provide colour coded visitor lanyards/ID cards and then if they are spotted walking in the incorrect zone, security can intervene.”

Paynter adds: “Over the last decade, the capabilities and intelligence of security systems and surveillance analytics has progressed enormously. Facial recognition and LPR (Licence Plate Recognition) video surveillance analytics is now widely available and when combined with powerful tracking analytics these systems can track pedestrian and vehicular traffic at an almost granular level, accurately and in depth.”

Pedestrian traffic heat mapping and tracking can be done using intelligent Wi-Fi signal analytics in conjunction with an estate-wide Wi-Fi mesh network. This solution would be complementary as opposed to primary, and would bolster the intelligence of other systems. It cannot provide faultless tracking of all visitors, as many would not have Wi-Fi enabled and device signal strengths are not an exact science as there are many factors which create variables in terms of signal strength and quality.

A team effort
It is in the best interests of all stakeholders that everyone works closely together to gather information on known criminals as well as vehicles that have either been used in crimes or have been stolen.

SNIPR South Africa is an early warning system that uses ANPR (Automatic Number Plate Recognition) technology to recognise number plates and cross reference this across its global database of suspicious vehicles which includes subscription to the national law enforcement database of suspicious vehicles. This technology relies on strategically placed cameras or GateBook handheld devices at entrance points or high valued areas. This database of suspicious vehicles is extremely useful in providing estates and other stakeholders with the necessary information to identify these vehicles and issue alerts.

Rampersad says that the company has over 140 trusted vetted and verified sources that provide information for its national live database. Once a number plate is received by the SNIPR server, it is cross referenced to the plates on file and on the law enforcement database. If it turns out to be a suspicious vehicle, the security teams at estates will be prompted in the control room and on the app via their mobile device to take the relevant immediate action.

“I strongly believe that it is time for the

Dave Rampersad
private sector to work together more strategically in a more coordinated way, to gain the upper hand against violent crime. There are many ways this can be done,” says Paynter. They include centralised rule driven data. This is technology which references a unified database of identities as well as high-risk ID numbers, vehicles and cellphone numbers is far more powerful than technology which does not check the visitor data against anything.

What’s available?
Powell says that in addition to an integrated solution such as PT-Guest, the company also has a standalone visitor management system called PT-Scan. This cost effective system is ideal for smaller to medium-sized estates and allows users to replace the manual visitor book with an electronic solution by scanning the driver’s licence and vehicle registration.

PT-Guest has a full bouquet of features such as pre-authorisation, in-zone reporting, late exit of contractors and is fully integrated with access control systems, linking the homeowner with a pre-authorised guest and allotting time zones to visitors.

PT-Guest also provides a web interface where registered authorised persons can log in via email and a password, and can request single or multiple access packs for visitors. Standard and custom management reports are available.

SNIPR’s GateBook Access app is another pre-authorisation method that sends a PIN to a guest and stipulates how many guests are permitted to enter when the security guard scans the PIN. Similarly, when contractors are entering premises, the system takes a photograph of the guest and scans the vehicle registration.

Paynter suggests that when choosing a visitor management solution, estate managers/trustees should use the EVIMS checklist, which covers the five most important considerations for an effective visitor management solution:

• Every identity transaction must be ‘live’ screened in real-time and not in retrospect.
• Visitors’ identities must be verified to check that they are who they say they are.
• Identity sample must be kept for evidence of permission and presence – fingerprint/photo/DNA.
• Must comply with legislation – PoPi, ECT, OHSA Acts.
• Secure offsite cloud hosting of data – secure compliant backup. Lower data theft/tamper risk.

He adds that a system which merely records the persons ID or vehicle disc without any cross checking or verification has several vulnerabilities. It is therefore important to use a system which can perform a live ID check to ensure that visitors are who they claim to be.

Electronic visitor management is a rapidly evolving technology. However, for various reasons, including budgetary constraints and ignorance of benefits, many estates are still deluded into believing that the inaccurate and highly inefficient manual visitor book is sufficient to control and monitor visitor access to estates.

Given the ability to verify visitor identities, thereby eliminating criminal elements having access to private premises, the shift to electronic alternatives should be a no-brainer for estates. The return on investment is proven across a wide footprint of success stories and dubious estate managers and HoAs should take the time to visit estates where residents are reaping the benefits of adopting the technology.

For more information contact:
SNIPR South Africa, +27 (0)71 887 3619, dave@snipr.co.za, www.snipr.co.za.
Terpay Group, +27 (0)74 566 3663, mark@terpaygroup.com, www.terpaygroup.com.
Central identification, information and data synchronisation repository that manages your central database across multiple platforms and sites anywhere in the world.

BioHandheld makes use of Honeywell's OEM 2D and Barcode Scanner. Our mobile devices are used to manage vehicles, visitors and contractors effectively by conclusively recording and matching entry and exit events.

BioLobby is a self-service Visitor Management Kiosk or Desktop Solution that allows Visitors or Contractors to self-deploy.

BioInduction is a customisable Induction, Occupational Health and Safety and Compliance Training platform. This platform has the ability to create any training course with user definable Questions and Answers. The solution utilises all multi-media tools.

Alcoscan is a high speed automatic industrial breathalyser that is used to check the breath of workers for alcohol at turnstiles, gates and entrances to sites, offices, mines, refineries and warehouses.

BioCheck utilises southern Africa’s market leaders in background screening. The key to BioCheck has been the company’s uncompromising commitment to providing a focused and cost-effective Background Screening service of the highest quality.

BioAccess takes the frustration out of traditional access control. It’s a fully IP-based solution, that’s easy to install and configure, with features rivalling the biggest access control solutions.
Islington on the Green

Net2 Entry provides simple access control for central London apartments.

Islington on the Green is a residential complex consisting of 70 modern, high-specification apartments. Based in the heart of Islington, these properties boast all the benefits of an unbeatable central Islington location, while maintaining the security of a private development with concierge.

Islington on the Green required an update to its existing access control solution that had ceased to function. It also required an improved access management system that would be simple to use, and could enable the concierge and residents to grant access to visitors from the reception and their individual apartments respectively.

The general manager of Islington on the Green, Ashley Proctor, approached MAS Systems to specify a new system, having previously worked with the company on a large hospitality establishment.

Neil Matthews, MAS Systems’ fire and security systems manager, recommended Paxton’s Net2 Entry system, combined with the Net2 software, to meet his clients’ requirements.

Networked solution

Net2 is a user-friendly and flexible networked access control system, designed to make the management of any site straightforward. Matthews says: “I’ve worked with Paxton products for more years than I can count. Its technical support is always great, which is why I thought Paxton’s Net2 range would offer the ideal solution.”

The new Net2 system electronically controls the main entrance to the building, as well as the private entrances to each of the 70 apartments. With the Net2 Entry monitors, residents can permit access to visitors following visual or audio verification. The concierge can easily program new access tokens for residents onsite, and cancel them from the system should any be lost or stolen, significantly increasing the level of security compared to a standard lock and key system.

“Paxton’s Net2 Entry system is a real plug-and-play solution, which we feel is its biggest selling point. It’s so simple to install, and the ease of operation made it the best choice for Islington on the Green.”

– Neil Matthews

Net2 system can be administered from one central PC, with external IT management able to monitor and maintain the system remotely via the network.

Simple, secure access

The Net2 system, with Net2 Entry, has provided Islington on the Green with a secure access control solution that provides residents the ability to grant, or deny access to visitors and gain access themselves with a simple token.

Proctor says: “The software is really easy to use, the Net2 Entry system is simple and it does what we need it to: enabling the concierge to visually verify visitors and residents to buzz people into the building.”

With potential plans to refit the adjacent Islington on the Green Theatre, the Net2 system also provides the opportunity to expand and secure the new site, included in the same development complex, from the same centrally managed system.

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

Project statistics

Type of site: Residential
Location: London, UK
Number of doors:
• 71 doors.
• 150 users.
Solution required:
• Manage and control access to the building and individual apartments.
• Simple keyless entry system.
• Update and improve existing access control system.
Result:
• Simple to use door entry system.
• Flexible management, enabling property-owners and residents to control site access.
• Central management with remote access capabilities.
Paxton products used:
• Net2 Entry standard panel with rain hood.
• Net2 Entry monitors.
• Net2 software.
Effective, PoPI-compliant visitor management

By Andrew Seldon.

Hand-held visitor management solution streamlines access to estates.

Establishing the correct identity of visitors to an estate or complex is crucial to effective security. In the past, the tattered visitors’ book was standard at every gate, but now, everyone knows that these books are ineffective as information is largely inaccurate and mostly illegible. Moreover, with the Protection of Personal Information (PoPI) Act, paper-based access control registers will no longer be compliant and will become obsolete.

OnGuard has developed a solution for visitor management called Identiscan, a hand-held mobile data terminal effective in scanning both motor vehicle and driver’s licences. When using the Identiscan Electronic Visitor Management System (EVMS), all data is encrypted and stored offsite on a secure server to meet the most stringent regulatory requirements.

“Identiscan is a good security solution for access control and we offer it as a service to all our clients,” says Charl du Toit from SJC Security. “It takes away the work of handwritten security tasks and increases control procedures at estates and places of business.”

The system ensures both the identity of the user (the guard) as well as the visitor. Before using the device, the user first enters their PIN to identify them. This ensures that they remain accountable for management of the scanner as well as the allocation of the access record to the specific guard. There is no longer an option to say “I didn’t let that person in”.

Peter Bicar, estate manager at Silvertree Estate in Tokai, notes, “We have seen a real benefit in reduced crime by percentage on the estate since using Identiscan. It enables us to ascertain if the driver has a valid driver licence and that the vehicle is valid as well. All visitors, including contractors, are recorded entering the estate and I receive daily reports on the day’s activities. I am able to retrieve backup information from the server in order to follow up should an incidence occur.”

The benefits of using Identiscan are:
• Accuracy of information.
• Elimination of paper-based access control registers.
• Improved speed of processing visitors and contractors.
• No computer required as the data stored offsite.
• Automatic warnings of undesirables people/vehicles.
• In-depth reporting.
• Direct control of the gate or boom via the scanner.

“Identiscan is a massive deterrent for someone who wants to enter illegally. It also prevents people who don’t have a valid registration or identification from entering – there is just no basis for argument. If they don’t have a driver’s licence, they simply don’t come in,” explains Tony Heath from Stable Yard Estate.

He adds, “We have received very good service from Identiscan; there is never any downtime. We once needed something to be looked at and it was attended to in a matter of hours. The product is not just limited to use for guarding companies either. I am the chairman of a complex of 1550 houses and we have direct access to a list of all visitors on a daily basis, with their photo ID and full details so we can trace any internal incidences as they occur.”

For more information contact Identiscan, +27 (0)21 701 7777, www.identiscan.co.za.
Planning for unexpected power outages has become an essential part of any security strategy. While the primary types of equipment available for supplying backup power haven’t changed much in the last few years, continual technological advances mean that some equipment becomes more relevant than others, depending on the subtleties of their operation.

The UPS is the main backup power mainstay, and is differentiated between off-line and on-line models, as Eurobyte Technology’s Neal Thomas describes: “With an off-line UPS, as the name suggests, the inverter module is off-line and does not feed any power to the protected device. The batteries are however connected to the mains power so they stay charged at all times in the event that there is a power failure. Because the inverter module is not feeding power to the protected device, it is not protecting it from other power issues such as power spikes. Once the power goes off there is a slight delay for the inverter to respond, usually between 2 to 10 milliseconds which could adversely affect sensitive electronics.

“An on-line UPS is always on-line and acts as a buffer between the main power and the powered devices. This regulates the electrical flow from the mains to the devices, which also protects them in the event of power spikes and brownouts. Because this unit is always on-line it means there is no switchover time from the UPS once the mains go out and your electronic devices are not affected by any form of a switchover.

“Lastly we have the line interactive UPS, which uses bits of the technologies from both the off-line and on-line UPS. This allows it to function in the same way as an off-line UPS with the difference that it incorporates a voltage regulator which helps to protect devices from more than just power failures, but also against power spikes and brownouts which we experience frequently in South Africa.”

Legrand South Africa is another company that supplies UPSes and related backup power equipment, and the company’s Marius Labuschagne summarises the differences between on-line and off-line models by saying that “Generally on-line UPSes, unlike off-line alternatives, are expensive and inefficient as the inverter is continuously in operation, however it provides better quality of power as compared to an off-line UPS.”

Further exploring inverter technology, Labuschagne explains that the role of the
inverter is to take the utility’s pure AC sine wave and convert it into DC in order to charge batteries. The DC is then rectified back into AC, and two main types of rectifiers are available for this step. “Firstly, square wave rectifiers are a cost effective solution to achieve AC. However, the voltage is not ramped on a smooth curve but instead is pulsed on and off at a frequency of 50 to 60 Hz, thus producing a square waveform. Though this technology works well for the majority of electrical goods, unfortunately certain electronics depend on a smooth sine wave and may not function correctly with the square wave.

“This brings us to the second type: the true or pure sign wave rectifier. The advanced electronics used in these are more costly, but the stable waveform offers high-end electronics and sensitive equipment a true, smoothly ramped sine wave.”

When it comes to longer-term power outages, a generator is the go-to solution, and should always be specified at a higher power rating than the UPS that is being used, according to Thomas. “The reason for this is that the generator is running to your devices through the UPS, so if you are using a generator that has a lower power rating you will still be running down the UPS battery and this could cause damage to your UPS, and in turn damage the electronic devices you are trying to power. Also keep in mind that the generator should have a built in voltage regulator to ensure that the power coming through is clean, so as not to damage the electronic devices – this is also where your choice of UPS becomes important.”

As Labuschagne explains it, “the UPS operates from charged batteries and, depending on the autonomy available, can offer a full load supply instantaneously as the mains fail. This gives the generator time to start up and ramp to the required load, at which point it will support the UPS by recharging in order to sustain power. The full UPS load on the generator should be around half to a maximum of two thirds of the full load capacity of the genset. The reason for this is that any switching of equipment on a generator running close to full load may cause dipping and ramping of voltages and frequency as the generator tries to compensate with little reserve. In order to avoid this fluctuation manufacturers recommend 50% to 70% operating loads on gensets.”

Petrol and diesel powered generators have long been the main contenders, but the use of gas generators is now becoming more common. Labuschagne summarises the main differences between the three options as follows: “Gas gensets are silent with clean combustion. They provide moderate power levels and are very expensive to buy, but the running costs are lower. Diesel units are more noisy and the combustion is not clean, however they are more powerful and cost effective to run. Petrol generators provide strong power output and versatility in application, but are less cost effective than diesel and a bit noisy.”

For more information, contact:
• Neal Thomas, Eurobyte Technology, +27 (0)21 551 2804, neal@eurobyte.co.za, www.eurobyte.co.za.
• Marius Labuschagne, Legrand South Africa, +27 (0)11 444 7971, marius.labuschagne@legrand.co.za, www.legrand.co.za.
Five safety rules

Safety first is always important, but is even more crucial when addressing electrical installations.

Working on electrical installations can be dangerous as those that are not properly connected or maintained pose a serious risk to both people and property, and can lead to injuries or even death. For this reason, DEHN Africa has adopted five safety rules according to the German standard series DIN VDE 0105 to help prevent electrical accidents.

**Step 1: Disconnect completely**
When working on an electrical installation, it is best to ensure that it is disconnected from live parts on all poles.

**Step 2: Secure against reconnection**
To prevent an accidental reconnection of an installation where work is in progress, you need to replace the unscrewed fuses in the low-voltage system with lockable lockout devices, or ensure that all breakers on the off position are locked and adequate warnings are placed.

**Step 3: Verify that the installation is dead**
To verify that the installation is dead, you can use suitable test equipment such as a voltage detector to verify on all poles that the installation is dead. You also need to check the correct function of the voltage detector prior to using it.

**Step 4: Use earthing and short-circuiting devices**
After verification, connect the cables and the earthing system with short-circuit-proof earthing and short-circuiting devices. It is also important to ensure that the relevant parts must be earthed before they are short-circuited. Only after a successful application of the earthing and short-circuiting devices can the installation be considered dead and safe to work on.

**Step 5: Provide protection against adjacent live parts**
According to the five safety rules, adjacent parts are located in the vicinity zone. If parts of an electrical installation in the vicinity zone of the work location cannot be disconnected, additional precautions must be taken before work is resumed. In this case, it is essential to use insulating protective shutters or covering material as protection against any accidental contact.

For more information contact DEHN Protection South Africa, +27 (0)11 704 1487, alexis.barwise@dehn-africa.com, www.dehn-africa.com.
Deepening the value of surveillance

Deep Learning has swept through the IT industry, now it’s changing security as well.

Deep Learning has swept through the IT industry, bringing benefits and better classifications to a number of applications. Inspired by the way the human brain works, the technology uses a layered learning process to enable the computer to classify, store and access data, which it can then refer to for learning.

This means it can use a whole image for recognition, rather than relying on separate elements of that image. This is a cumulative process – the more elements it has to draw on, the better the classification – thus, the better the ‘learning’.

The benefits of this technology for face recognition and image classification makes it valuable in the field of security. It touches on every aspect of the security industry – from facial and vehicle detection to behaviour analysis. This, in turn, starts to change the focus of security from being reactive to being able to predict problems before they happen.

Hikvision has used this technology and created a family of products to maximise its use. The DeepInview IP camera range and the DeepInmind NVR range work together to provide all the power and benefits of Deep Learning. While the cameras provide the smart ‘eyes’ of the system, the NVR represents the analytic and storage capabilities of the brain. The products help to tackle security on two fronts – recognition, monitoring and counting of people, and recognition and detection of vehicles. This uses Deep Learning technology at its most effective, for its ability to classify and recognise thousands of features.

Obviously, this multi-layered approach uses a lot of memory and CPU performance, which is one of the reasons the technology has become more widespread in the past few years. To put this into perspective, in the first stages of the technology, it took 1 000 devices with 16 000 CPUs to simulate a neural network. Now, just a few GPUs are needed.

Hikvision is partnering with the largest of the chipset brands – Intel and NVIDIA – to explore the possibilities of Deep Learning for the surveillance industry. Hikvision’s innovation also facilitates and improves on this – the H.265+ codec radically reduces transmission bandwidth and data storage capacity requirements. This means there’s no loss of quality, even though the data being shared and stored is exponentially higher.

Applications are numerous. The technology could enable the system to provide a black list/white list alarm, for example, which could come in very handy in access control scenarios. It could also be used to recognise unusual behaviour – possibly allowing security staff to prevent an issue if people are found loitering, for example.

The new premium range of products will further extend the quality and capabilities of security systems. They will also allow security professionals to start planning to avoid issues, rather than reacting to them. This could be the next evolution of the whole industry – using AI to change the world.


For more information contact Hikvision South Africa, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com.
Cameras don’t equal surveillance
A beginner’s guide to an end-to-end surveillance network.

When you purchase new cameras for your estate, you may be tempted to think that you are well on your way to securing your space, but cameras are just one pixel in the picture of security. In a world where surveillance is crucial in protecting assets and monitoring daily operations, where it would often be costly or impossible to have a person standing guard in every area of your business, a surveillance system that works together to keep your assets safe is indispensable.

In this article we take a step back and look at surveillance as a whole from a beginner’s perspective. We know that cameras are not the sum of surveillance, so we will explore what an end-to-end surveillance system means, its key benefits and how your surveillance system really does the hard work for you.

What does end-to-end surveillance mean?
Creating a truly effective end-to-end surveillance system, means bringing together a mixture of different products that work together to make securing your assets more effective and easier. That basically means considering factors such as the cameras you’ll need for each area, infrastructure, PoE switches, storage and surveillance software to help you manage your cameras.

Surveillance cameras
Your IP cameras will be the eyes and ears of your surveillance system, so choosing the right camera for what you need to keep an eye on is crucial. An overwhelming number of surveillance cameras are available from consumer to professional business cameras, indoor and outdoor, vandalproof, night and day, pan/tilt or fixed lens, or cameras with microphones and speaker output.

So one of the most important things to consider before buying a surveillance camera is what you want to achieve with each camera you place. Is the goal to monitor a small or large area, to record details such as faces, or to give an overview of operations?

Here are a few features to take note of before heading out to buy a surveillance camera. Firstly, note the video resolution, the higher the video resolution the better the image quality. Take note of the horizontal field of view or whether it can pan/tilt, as well as built-in infrared LEDs to let you see in the dark. Depending on the specific goal of the camera you could also consider whether it has motion or sound detection, a MicroSD card slot for on board storage and supports PoE (Power over Ethernet).

Infrastructure
It is important to consider the infrastructure required to link up your cameras. This goes hand-in-hand with considering the placement and amount of cameras that will be deployed and weighing it up with your budget.

Installing a surveillance system for the first time can be costly, but if done correctly, the value of an effective surveillance system will quickly outweigh the costs incurred.

PoE switches
Switches may not be the first thing that comes to mind when thinking of surveillance, but switches help a great deal to provide the best possible quality of surveillance traffic, saving on operation and infrastructure costs along with a host of other features.

Important features to look for are PoE ports, surveillance VLAN and IEEE802.3az Energy Efficient Ethernet. PoE ports let you power other devices that support PoE over a single Ethernet cable. This means less cabling as you’ll only be running one cable to each camera, saving on infrastructure costs, as well as maintenance.

A surveillance VLAN gives video traffic high priority and guarantees the quality of surveillance traffic thus saving businesses the added expenses required for dedicated hardware and facilities while IEEE802.3az Energy Efficient Ethernet means these switches consume less energy by cutting down on power consumption when port utilisation is low.

From the most simple to advanced network management, D-Link’s switches also provide important security functionality to protect your network from malicious attacks, so you’re safe on the outside and inside.

Storage
If you are recording surveillance footage around the clock you’ll obviously need to store it somewhere where you can access it later. This is where network video recorders (NVRs) come in. Not only do they offer comprehensive video display, storage and management solutions, but also provide reliable remote monitoring functionality that means you can instantly view what is happening from wherever you are in the world.

These useful devices also offer powerful event management which means you can control what should happen when a camera is triggered, while intelligent playback makes it easy to search through your recorded data to find notable events. It is also worthwhile to consider buying a NVR that has built-in PoE ports to help ease camera installation by providing power to PoE-enabled cameras.

Key benefits
It is thus easy to understand the benefits of approaching surveillance from an end-to-end point of view, because it considers the role of each component and allows you to choose the best fit for your needs. In the same way that any team has specialised team members that make it function optimally, your surveillance system has components that work together to make up a truly effective surveillance system that looks after your assets 24/7.

With a holistic, carefully considered surveillance system set up, you can enjoy the most advanced functionality and manageability that will save you time and money, not only during installation and maintenance, but also in terms of daily operational costs.

For more information contact D-Link Southern Africa, +27 (0)12 741 2000, support@d-link.co.za, www.d-link.co.za
As the resolutions of digital surveillance cameras have increased and new technologies such as thermal imaging have been introduced, the ability to detect details and recognise objects has improved dramatically. To assist in automating recognition tasks and reduce the chances of human error, analytics technologies are continually advancing to keep pace by not only alerting to potential threats but also reducing the occurrence of false alarms.

Hi-Tech Security Solutions interviewed four providers and developers of video analytics solutions to learn more about the latest cutting-edge advances. They were: Avigilon, represented by Jenna Livergant; Bosch Security Systems SA, represented by Quintin Van Den Berg; Cathexis Africa, represented by Gus Brecher; and Reditron, represented by Brian Wynberger.

**Hi-Tech Security Solutions: What analytics do you offer for the residential estate market, and how do they mitigate false alarms?**

**Avigilon**: Avigilon offers full end-to-end security solutions, including advanced self-learning video analytics. Its video analytics are embedded directly into many of its cameras and are also part of its video management software. Its self-learning video analytics can be applied to many verticals, including the residential market.

In regards to false alarms, Avigilon's advanced pattern-based analytics solutions are able to recognise the movements of people and vehicles with high accuracy, helping operators to focus on the events that matter most. Teach-by-example technology enables users to provide feedback about the accuracy of alerts in order to refine the self-learning capabilities of the technology. The ability of the technology to continually learn helps reduce false positives and ensure alerts are meaningful, which can improve efficiencies.

**Bosch**: With video analytics at the edge as standard in the new Bosch IP 4000i to IP 9000 cameras, we have a full intelligent portfolio suitable for the residential estate market. Security managers can set up their own alarm rules and be alerted when needed. For example, if the security manager wants to count people entering and leaving a compound, that’s also possible.

Bosch’s Intelligent Video Analytics technology is designed for the most demanding environments, and is ideal for perimeter protection of residential estates. It provides the ability to differentiate between genuine security events and known false triggers such as challenging environments with wind (moving trees), rain, hail, and water reflections or applications that require video content analysis over large distances.

**Cathexis**: Cathexis supplies various analytics algorithms, including line crossing, loitering, time in area, direction, speed, etc. It has various methods of rejecting false alarms, such as size and speed filters, dynamic background modelling (for rejecting things like rain, flashing lights, camera shake and so on), shadow suppression and more. The improvement and lower cost of thermal cameras have also helped a lot in the reduction of false alarms.

**Reditron**: The Arteco technologies provided by Reditron include detection of intrusion, loitering, lost people and objects, slip and fall, facial detection and recognition, panic, ATM-specific events, fire, and licence plate recognition, amongst others.

Arteco’s solution only needs 25 pixels on target to create an event, and with the use of thermal cameras it delivers an accuracy of 95% and above. Its intrusion rule can be set up so that a predefined amount of tripwires need to be crossed before an event is created. Added to that is the ability to filter shadows, car lights, reflections and illumination changes caused by weather.

The ideal situation is to have more than one technology introduced to your perimeter. As with any solution that is linked to a camera, we can only work with what we see, and it is beneficial to combine analytics with other solutions such as microwave barriers, fence detection systems, even electric fencing and traditional beams. The idea is to have both the solutions triggered at the same time and then only create an event. This method reduces false alarms even further.

**Hi-Tech Security Solutions: What options are there to follow intrusions beyond the fence?**

**Avigilon**: Avigilon’s analytics solutions can monitor an area 24/7/365. With alerts in near real time,
as well as the ability to send alerts to a mobile device, security operators can be alerted of critical events as they happen.

When needing to search for a person across a site, Avigilon Appearance Search video analytics technology can be applied. This technology uses a sophisticated deep learning artificial intelligence (AI) search engine to sort through hours of footage with ease. This technology allows security operators to click on a button and search for all instances of a person or vehicle across all cameras on a site, quickly and efficiently.

Bosch: An innovation offered by the new MIC IP models is video analytics whilst moving. An operator is alerted, or the camera's Intelligent Tracking feature is triggered the moment an intruder is detected at the fence while the MIC IP camera is panning, tilting or zooming. Once Intelligent Tracking is activated, it ensures that the intruder is automatically tracked. Optimal capture of the intruder is assured by dynamically adjusting the field of view.

Another solution for perimeter protection is the new DINION IP thermal 8000 camera. It ensures early detection over distances up to 762 metres thanks to the combination of thermal imaging and Intelligent Video Analytics. At residential estates with limited vision due to poor lighting conditions, or even in complete darkness, operators can be assured that they are alarmed at an early stage.

Cathexis: This really depends on the coverage of the cameras on the estate. A lot of estates only have cameras focused on the perimeter, so once a perpetrator has left the camera view, there is nothing one can do. If there are cameras covering the other areas, in CathexisVision we have a feature called 'adjacent camera mapping' which enables you to easily follow objects across multiple cameras. One can also use tracking algorithms on PTZ cameras for this purpose.

Redtron: Arteco firmly believes that security for an estate starts on the outside and moves inwards. It is too late to react when an intruder has passed your perimeter defences. Yes, this does happen, but if the correct solutions are applied on the perimeter then such breaches should be very rare.

Should a breach occur, Arteco is able to have the event linked to cameras that are closely associated with each other. For example if we have a thermal camera on the perimeter that detects an event it will automatically pop-up live video and recorded video of that event of that particular camera. The operator can then easily select cameras by association that will display cameras in the same area as the camera that initially detected the event. This will provide the operator with total situational awareness which will allow him to take the required action. These cameras can also be populated on a map so even a new operator to the site can instantly understand which cameras he is dealing with.

Hi-Tech Security Solutions: How has analytics advanced, and can it be relied on as the sole perimeter protection mechanism?

Avigilon: Perimeter protection is typically a multi-layered approach. The end-user and system integrator should work together to design a system that works best for the particular site, and video analytics can be an important part of that system. Advances in video analytics have resulted in greater site monitoring efficiencies as video analytics have evolved from Video Motion Detection (VMD), to Advanced Video Motion Detection (AVMD), to Advanced Video Pattern Detection.

VMD is now a standard feature included with most new surveillance cameras, recorders and video management software. VMD focuses on detecting any pixel movement from scene to scene based on a simplistic user-defined threshold. The industry then progressed from VMD to AVMD. AVMD is based on background modelling, alerting on any change that deviates from an established background model. AVMD technology focuses on monitoring a scene and using the data captured via complex manual calibration to identify moving objects.

The latest evolution is Advanced Video Pattern Detection, which is based on pattern modelling algorithms, alerting on any change that has a pattern of a known object type such as a person or a vehicle. This technology focuses on recognising the objects in view and using information regarding the movement of an object to accurately classify it. As a result of this technology, analytics have gone from being a strictly forensic tool to being a potentially powerful proactive solution.

Bosch: Video analytics is not the ‘silver bullet’ to perimeter protection but it is a significant enhancement to physical barriers and man guarding. Video analytics acts as the ‘brains’ of a security system, using metadata to add sense and structure to video footage. This in turn enables the network video cameras to understand what they are seeing and alerts on any potential threat the moment it happens. Each camera in effect becomes ‘smart’ - allowing security guards/operators to retrieve the right footage from hours of stored video instantly. It analyses the scene by providing all kinds of statistics (metadata) and takes appropriate action faster, easier and more efficiently.

Cathexis: Because of processing power advancements, one can do more sophisticated processing on multiple cameras simultaneously on less hardware. This enables software vendors to look at more parameters like colour. It has also enabled sophisticated dynamic background modelling to be done in real time, making the analytic algorithms more accurate and less susceptible to false alarms.

I believe that in the right environment, one can use analytics as your sole perimeter detection technology. There may be unique situations where one may prefer another fence monitoring technology, or in high security environments maybe even use both. We have many residential estates successfully using our analytics as their sole detection technology.

Hi-Tech Security Solutions: What impact are deep learning and artificial intelligence having on video analytics?

Avigilon: The vast majority of recorded video data is never viewed. This isn't for a lack of interesting content or inadequate resources, but rather a gradual decline in human attention spans. Adding more cameras increases the amount of video data collected, but if it's not viewed, useful information is missed.

There is an imbalance between the amount of video data collected and the human attention available to effectively mine that data. A person conducting a search needs to answer who, what, when and where, not just in the context of a single camera, but across an entire site. This is
where the need for AI comes in. We believe that the continued evolution of AI will provide security operators with even more powerful tools not just for forensic purposes, but also for real-time event response.

One of the new artificial intelligence technologies Avigilon is developing is Unusual Motion Detection (UMD), which brings a new level of automation to surveillance. Without any predefined rules or setup, it is able to continuously learn what typical activity in the scene looks like and detects and focuses the operator’s attention on atypical events that may need further investigation.

**Bosch:** We believe that the logical next step for security is to enable customers to start repurposing the huge amounts of video data. The ability to interpret video data directly from the source helps to substantially improve levels of security.

Despite the huge amounts of video data collected, statistics show that only 10% of data is ever used and most of the data collected loses its value within seconds after being generated. Why are we only using such a limited amount of data? We are mainly focused on delivering the right information in case of an emergency or providing the correct evidence after a criminal act. We believe that the future is to utilise the hidden potential and use 100% of the video security data, allowing this data to do far more than security alone.

**Cathexis:** One needs to define ‘learning’. One may learn the environment with a view to adjusting for changing backgrounds to reject false alarms, and this is very successful. The other learning algorithms that some vendors are promoting are based around behavioural analysis, where the system ‘learns’ what is the normal behaviour on a site, and triggers an alarm when an abnormal situation occurs. There have been varying degrees of success in this technology at this stage. I don’t believe that one can get away with using this as the sole analytics technology.

**Reditron:** Deep learning and artificial intelligence are no doubt words that are thrown around more and more today. Arteco’s analytics for intrusion and retail applications already use advanced algorithms and artificial vision to provide the results, but moving on with technologies such as deep learning analytics does indeed have its benefits. Whether the customer is willing to part with the money needed for such software and hardware remains to be seen. The goal is to have such solutions with as little processing power as possible – if so this can even be installed on the edge.

Unfortunately we are seeing that companies that boast of having solutions that ‘think for themselves’ require the rip-out-and-replace approach in favour of a single end-to-end brand offering. With Arteco, this is not the case as it is completely camera agnostic and so can offer a very high rate of detection even for a solution that is not IP based.

The good news is that these more intelligent technologies are being developed at lightning speed and will see prices drop as time goes on. That being said, it is still required to approach every site and every camera with caution so that the solution offered meets and exceeds the end user’s expectations.

For more information, contact:

- Avigilon, +27 (0)79 079 6528, charntel.loftus@avigilon.com, www.avigilon.com.
- Cathexis Africa, +27 (0)31 240 0800, sales@catafrica.co.za, www.cathexisvideo.com.
- Reditron, +27 (0)87 802 2288, sales@reditron.co.za, www.reditron.co.za.
Enhancing estate control rooms

Integrating all aspects of security into a single management platform enhances the effectiveness of the solution.

World-class security systems that offer peace-of-mind may be one of the biggest contributing factors for an increasing number of local and international buyers in some of South Africa’s luxury lifestyle estates. For those that can afford it, the allure of comfortable and convenient living, combined with the assurance that comes with a well-established, carefully managed and holistic security system is rapidly driving investment.

While CCTV surveillance has become a key component in estate security, a truly integrated security system requires that all aspects of the security system work seamlessly together, while being managed by the heart of the system, which is the control room.

Working in a 24/7 CCTV security control room environment demands a lot of physical and mental commitment from operators. Thankfully several security product providers are designing and manufacturing products that not only reduce the risk of human error but are significantly enhancing the control room operators’ working environment.

Real-time information followed by prompt decision making and immediate action can make all the difference in estate security to prevent a house robbery or other security breaches, which is why sophisticated video management software is central to the control room environment and its operators.

“The true power of a CCTV surveillance system, and what it can offer secure estates in terms of security, operations and infrastructure management becomes even more apparent when combined with sophisticated video management software,” says Gus Brecher, managing director of Cathexis Africa and business development director of Cathexis Technologies.

The world of CCTV surveillance is greatly enhanced by the association of synchronised video and full integration with other third-party security systems, including access control, alarm panels, fire panels, analytics, building management systems and so much more.

This integration provides a powerful single-user interface, enhanced by video verification of events that occur, as well as rules-based events that can be initiated from event data. Integration leads directly to a dramatically improved control room environment with improved efficiency and effectiveness. Integration enables the system to guide the CCTV operators to specific cameras associated with third-party systems events, speeding up response times and resultant efficiency.

“Imagine control room operators having their world greatly enhanced by having the system automatically choosing cameras for them to view based on events or alarms from access control systems, alarm panels, fence monitoring systems and the like,” says Brecher. “Once the benefits have been experienced, their world without integration is almost unimaginable.”

There are also several key features associated with video management software, which make it one of the most powerful control room assets. The software is characterised by ease-of-use that makes it an adaptable and intuitive fit for residential estates of any size. Key features of successful VMS products include high-definition camera support, smart video analytics that minimise data usage, automatic licence plate recognition, and unlimited scalability which ensure that security systems can grow with the estate.

Given the sheer size and scale of residential estates, the surveillance system should include the ability to monitor hundreds of IP cameras, often across multiple sites. In addition, a flexible and scalable video management solution will be required to accommodate the future expansion of the estate as well.

The analytics feature provides triggers to the system, which enables the system to take user defined actions depending on the specific trigger received. With its open platform and ability to customise to specific industry requirements this is ideal for managing vast estates.

Anti-tamper technology will notify the control room via an alarm in the event of any IP surveillance camera tempering, including: lens covering or spray painting. Clients can also include a user-defined specific action for the alarm, to which the person tampering with the device will be unaware of.

While control rooms are often designed strictly around functional requirements, the development of IP VMS in the security industry is demonstrating how the control operators’ working environment can be dramatically enhanced.

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

Surveillance on the move

By Andrew Seldon.

Is there place for body-worn cameras in estate security?

Body-worn cameras (BWC) have been available for some time, but are usually associated with police services or security operators that are active in public areas. The benefits of these devices is that operators have video from every situation, clearly demonstrating who did and said what. For those cameras that are connected in real time to a control room, it offers operators the ability to manage a situation by dispatching additional resources, be it armed response or medical services.

Many of these cameras have additional functionality, such as the ability to record on the device or stream live footage to a control room, provide the location of the wearer and so forth. But are these devices suitable for an estate environment as well? After all, an estate is where people live and would want to feel relaxed and at home, not under constant watch.

Hi-Tech Security Solutions asked a few BWC vendors for their insights into whether these devices are suitable for estate security, as well as what is on offer today. Our participants are: Forbatt SA, Jaco Nel from Vantage MDT, Kevin Croft from Starbase, and Shaun Stanley from Doculam.

Hi-Tech Security Solutions: What do body-worn cameras add to the guarding function in residential estates, assuming you think they add value in this type of environment?

Croft: BWC add a number of advantages to residential estate guarding. Firstly, many complaints (from residents or visitors) are in the form of a ‘he said, she said’ argument. And while many of the guard houses have CCTV cameras, these are not able to record audio. Using a BWC allows for the recording of both audio and video directly from the guard’s point of view.

Secondly, many of these guards are required to do patrols around the estate. Having a BWC on them during these patrols allows them to collect evidence immediately in the event that they discover something unusual. In many cases, security guards are accused of looting a scene before reporting it to their superiors. Wearing a BWC can confirm whether or not this actually happened.

Lastly, BWC footage can help supplement access control data to confirm identities of anyone going onto and leaving the estate.

Hi-Tech Security Solutions: As with any other technology, there are cheap BWC and there are good BWC. What does an estate manager or estate security manager need to look for when considering BWC? What are ‘must-have’ benefits and technologies in a BWC, and what are nice-to-have extras?

Nel: For the South African environment, a compact BWC is the best solution. Some BWC have a combination of different components (camera, separate microphone etc.), and the risk of failure is much greater. Quality can be an issue and I would suggest any company purchasing several BWC to test the product first. A good quality BWC will have an IP68 rating and should pass a drop test.

The must-have benefits would be the...
ability of the BWC to record a full shift, record audio and video, have infrared night vision, be able to take pictures and have GPS tracking integration which is synchronised with the video footage.

The nice-to-have extras, which could also be essential for certain estates, would be the ability to dial into the BWC from a control room through the 3G/4G module and a panic button. These features do increase the price somewhat.

Croft: Must-haves include password protected media and ideally internal (inaccessible) storage. They must also be built tough so they don’t break when dropped. Data removal also needs to be as easy as possible. Ideally, the guard should be able to drop the camera into a docking station which will charge it and download the media files automatically.

Nice-to-haves include infrared night vision (if intended to be used at night time), real-time live viewing and a built-in screen to review files on the camera itself.

Stanley: After introducing one of the first body-worn cameras to the South African market four years ago, there has been an influx of various models and makes of cameras, from online businesses offering a range of cheap cameras to the manufacturers around the world approaching the SA market directly. Considering it took the USA and the UK more than a decade to go through this learning processes, I believe South Africa is in its infancy and customers are easily mislead when making a purchase. The key components to making a decision on a BWC is quality of image, quality of battery life, firmware and device protection from operators. Then you need to look at the software platform for management of footage, protection of footage and storage of footage. Then consider the quality of the internal components of the camera and the after sales service from the company offering these solutions.

Forbatt SA: Kedacom provides two options for BWC camera, one is a Wi-Fi model, the other is Wi-Fi and 3G/4G model. The choice depends on whether you have Wi-Fi coverage over the whole estate. We also recommend ensuring you have audio and video recording and snapshot functions.

The nice-to-have extras are the touchscreen for easy operation, IP67 and drop-proof protection in case of different kinds of unexpected situations, and a panic button for popping up the alarm video in the control room.

Hi-Tech Security Solutions: How do BWC send data to control rooms (Wi-Fi/3G/GPRS/etc)? Is it necessary to have on-device storage or can everything be transmitted in real time?

Croft: In an ideal world, the cameras would automatically send the data to the control room via Wi-Fi (much cheaper) or via the cellphone data network. However, this isn’t currently possible in South Africa due to the limited network coverage and the high cost of data. Therefore, it is imperative that data is stored locally on the camera itself.

Live viewing is a different story, however. Although it does face the same challenges as wireless data transfer, the requirements for uninterrupted data transfer are much lower. With our live view model, there is only data transfer at the point where the control room has logged into the camera (saving unnecessary costs).

All that being said, live view is more likely to be relevant to other security situations (armed response, metro police, special forces units etc). For residential guarding, the most likely scenario that would require live view is for checking up on guards to ensure they are carrying out their duties correctly.

Nel: Data can be transmitted to the control room via USB cable, wireless or 3G/4G. The on-device, storage is necessary for full shift recording. As with all camera solutions, the 3G/4G option is great for proactive intervention or monitoring from a control room in real time, but can become very expensive through GPRS networks and many BWC on one site using wireless can create a bottleneck on the network. It would be best to use the 3G/4G option for the panic button and proactive monitoring.

Stanley: WiFi/3G/GPRS/etc. are all features currently available in some models of cameras, but I would be very reluctant to say that there are many products that are market ready. Although cloud storage is available in your higher-end cameras, very few institutions, especially law enforcement agencies are willing to outsource their storage due to confidentiality. Residential estates and their guarding companies would more than likely feel the same way for fear of repercussions and invasion of privacy lawsuits should footage be made public.

Devices that have real-time streaming capabilities also have built-in storage capabilities, the user has a choice of both options but would need to decide on a data storage procedure. If customers are wanting to live stream from an officer wearing a camera, data charges would become a factor for consideration as charges are high and clients would need to factor this into their decision-making process. The use of Wi-Fi can reduce this somewhat, but would be relevant to each application and the availability of Wi-Fi. It is however a great function to have available in a camera.

Forbatt SA: It is absolutely necessary to remotely access the BWC from the control room to view a situation in real time so that the operators can guide the guards in each situation and call for backup if necessary.
Real-time video is delivered to control room via Wi-Fi/3G/4G. Kedacom offers its own protocol with auto video adjustment technology to deliver better video even in areas of poor bandwidth.

Hi-Tech Security Solutions: Do BWC store and/or transmit only video or is other data recorded as well – such as GPS coordinates, audio etc.? What does your range of BWC offer in terms of data that can be recorded or transmitted?

Stanley: Our entry level model allows our customers to capture and store an HD quality visual and audio file, which is stored on a device and then transferred via manual download to a software package which will then be stored on an external hard drive or server. The high-end cameras can perform these functions and have the ability to stream images to devices or cloud software through Wi-Fi or 3G communications. Some can be integrated to some of the more popular video management systems.

Forbatt SA: All Kedacom BWC, no matter which transmission mechanism is chosen, can store and transmit video, audio and GPS coordinates. When an emergency occurs, the control room can check the positions of security guards on a map and then can communicate with other security guards via audio and direct them to the site.

Nel: Our BWC will store and transmit video, audio and GPS coordinates. A distress signal can also be transmitted via the panic button.

Croft: All units are able to record both video and audio together. Our mid and top-end units also store GPS information (which is displayed on a Google Maps interface). Our top-end unit stores GPS information, which is displayed on a Google Maps interface. Our top-end unit both stores and transmits video, audio and location data so the control room operator can assist the guard in the best way possible.

Hi-Tech Security Solutions: What BWC do you supply and what are the main features of your range? What accessories do you supply – such as battery chargers, video download options etc.?

Forbatt SA: We offer the following:
- Qualcomm 8 core 1.5 GHz processor with a customised Android OS,
- IP67 waterproof, dust-proof, 2-metre drop protection,
- KTWP protocol for improved 3G/4G/Wi-Fi transmission,
- 13 MP snapshot resolution, IR and LED light for night monitoring, 2 MP video recording,
- 2.2-inch touch screen display, and
- GPS positioning function, panic button/important files tag button.

The accessories include earhook cameras and button cameras. The docking station is also the recommended option for video, audio and snapshot downloading, and it supports up to 24 slots for BWC for simultaneously auto charging, auto upgrading, auto time sync and auto uploading of video, audio and snapshots. It also can be used to manage the users for each BWC.

Nel: We supply the Along range of BWC. The main features are:
- IP68 rating and 2 m shock resistant,

Continued on page 56
Continued from page 55

- Wide-angle camera view,
- GPS built in,
- 3G/4G transmission,
- Wireless transmission,
- Infrared for night vision,
- Video and audio recording,
- Panic button,
- 12-hour recordings, and
- The ability to rotate or change batteries.

We supply batteries, chargers, clips, belts and car kits for mounting. We also offer a portable data station for 8 or 20 cameras where footage can be downloaded and the units charged simultaneously. The stations can be downloaded and the units or 20 cameras where footage

Croft: We have four units on offer at the moment. Our entry level model is the E8 which includes all the standard BWC features one would expect (audio/video recording, photograph capture, IR night vision, white light, laser guided recording). This unit has an interchangeable battery and comes with a spare battery and a charging unit.

Our most popular unit is the X2. This unit has all the features of the E8 but comes with a built-in battery that is capable of recording for up to 10 hours. These two units are also compatible with small external lenses. These lenses are useful in situations like VIP protection (where the cameras need to be less conspicuous). They are, however, not intended to be used as ‘spy wear.’

The next model is an X4. This is similar to the X2, however it includes a built-in GPS. The top of the range model is an X6. This camera has a full set of connectivity including Wi-Fi, 3G, Bluetooth and GPS all built into the camera.

The software to manage the downloading and storage of media is included with our cameras (at no extra charge) and we offer a 10-camera docking station (for charging and downloading media).

Stanley: Doculam supplies the Watchdog body worn cameras which include:

- 32G/64G built-in storage capacity,
- 8-hours of battery life,
- A 30-second pre-record function to protect an officer who is taken by surprise,
- Photo snapshot for evidence purposes,
- Officer protect passwords,
- Setting protection on the devices to prevent tampering, and
- Our software platform for file storage and organisation.

Accessories include a variety of mounting options, including a chest harness and in-car mount, a single or 8-port docking station for charging and image download, charging connectors for desktop and mobile applications. Our top-end range, which will be available soon, will feature all the above and include Wi-Fi, 3G/4G, GPS for live streaming and software with both stand-alone and cloud storage capabilities.

**Hi-Tech Security Solutions: What back-end does your system require? Do you offer a ‘full solution’ including storage and software, or can your systems be integrated with third-party management platforms?**

Croft: Our software back-end will run on any Windows 7 or later computer. We don’t dictate which storage system to use as all our customers have vastly different requirements. It can, however, be as simple as a laptop with and internal hard drive (for small numbers of cameras) and adding an external hard drive for larger numbers of units. Our management software can also be set to upload the files to an FTP server for an additional backup.

Third-party applications are capable of being integrated into system as the operating system on the cameras is similar to that of an open source mobile phone. We haven’t had to do anything like this to date, however, because the standard system is sufficient to cover most of our clients’ needs.

Nel: We offer a complete solution. Our software does not require licensing and is purchased with the hardware. Our system can be integrated with third-party management platforms and vice versa.

Stanley: The back-end will depend on the application. Standalone systems come with software and are downloadable to a hard drive or external server for storage and file management purposes. If you are looking for cloud reporting, this is available with some brands of camera, which will also allow you to link direct to your own existing server – which will require integration. There is a possibility for unique third-party integration, but you would normally find most development has been done around your more popular VMS platforms. All custom third-party applications would require development and integration with the involvement of developers.

Forbatt SA: Kedacom offers the full solution including all the hardware and software. This includes the BWC and its management software for configuration or footage download, a central management VMS and client software, central storage (IPSAN), and the docking station. We also offer a NVR for the medium to small solutions like residential estates. The NVR provides ONVIF functionality to access the third-party management platforms.

For more information, contact:

- Doculam, +27 (0)11 888 5110, jhb@doculam.co.za, www.doculam.co.za.
- Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co.
- Starbase, +27 (0)11 804 1727, kevin@starbase.co.za, www.bodycameras.co.za.
- Vantage MDT, +27 (0)87 702 9761, jaco@vantagemdt.co.za, www.vantagemdt.co.za.
Securing what is important to you

G4S understands the “secure village” concept of lifestyle estate protection. We offer a range of integrated secure solutions to protect you and those dearest to you.

- Risk consultancy and investigation services
- Perimeter protection
- Access control with biometrics
- Intrusion detection
- Secure monitoring and response
- Vehicle patrols
- Video surveillance
- Manned guarding trained for the lifestyle estate environment
- Close protection officers

Contact details:
Telephone: +27 (0) 10 001 4500
Email: ess@za.g4s.com
Website: www.g4s.co.za

Securing Your World
BIOMETRICS

Let’s face it, biometrics is no longer the big deal it was a few years ago when South Africa led the way in the adoption of fingerprint biometrics. Today the world has caught up with the release of biometrics on smartphones and some incredible developments in face recognition technology as well as other forms of biometrics.

Yet, while it may not be the magical cure-all that was going to change the world it was way back when, biometrics, specifically fingerprint biometrics, is still the staple diet for businesses, governments and estates looking to streamline access control while improving the security of who is allowed in or not.

The key to biometrics is that it is hard to fake. Of course, those who keep tabs on the media know that iPhones (among others) have been ‘hacked’ with fake biometrics, but if you cast your mind back, some very prominent biometrics brands had their readers starring on YouTube a few years ago as people hacked them with photocopied fingerprints. Since then, the technology has improved significantly and you won’t find it quite as simple to fool today’s readers from tier-1 brands that invest in their products.

The key to biometrics is that it is hard to fake. Of course, those who keep tabs on the media know that iPhones (among others) have been ‘hacked’ with fake biometrics, but if you cast your mind back, some very prominent biometrics brands had their readers starring on YouTube a few years ago as people hacked them with photocopied fingerprints. Since then, the technology has improved significantly and you won’t find it quite as simple to fool today’s readers from tier-1 brands that invest in their products.

The key to biometrics is that at the moment of entry to an estate or a building, while you can offer up a fake identity document or driver’s licence and get away with it (unless the document is scanned electronically), it is hard to hand over someone’s finger or a fake finger to scan in real time. Even the most exhausted guard would raise an eyebrow if you told him to wait while you kept trying to get the reader to accept your plastic finger.

So how do biometrics and secure estates go together? Hi-Tech Security Solutions asked a few biometric experts to tell us about the fit between modern biometrics and secure residential estates.

Biometrics and estates?
If you believe the marketing material, biometrics is perfect for the access control to your estate and there are many estates you can use as an example where these systems are working well. But how does an estate know if its particular environment would be an appropriate location to use biometrics?

Deon Janse van Rensburg from ViRDI South Africa says that virtually any environment is suitable for some form of biometrics. “However, it is very dependent on how the entry and exit gates were designed, i.e. is there provision for goosenecks, can multi-tier goosenecks be deployed for different sized vehicles, how were the contractors’ or workers’ entrances designed etc.”

He mentions the physical design as some, especially contractor and worker entrances, sometimes seem to be set up as an afterthought. Then the question is what type of barrier is being used and, critically, whether the estate is able to afford its chosen biometric solution. As is mentioned in many instances in this publication, Janse van Rensburg is not only referring to the capital cost or affordability of the hardware, but also the hardware maintenance costs and the maintenance of the databases, hosting (if required), the costs of designated employees to manage enrolment and the general management of the system.

Similarly, Walter Rautenbach from Suprema South Africa agrees that biometrics is beneficial in any gated estate to ensure that true identity is used to gain access to the environment. Of course, he notes that the implementation of the same where the estate is not enclosed with secured fencing or barriers will not serve any real benefits.

“The starting point is usually the implementation of biometrics for residents and employees, as this is normally much easier than implementing and enforcing the same for visitors,” Rautenbach adds. “The main benefits are seen as convenience as well as security, although the element of security is normally diluted by persons accessing the estate without biometrics, be it due to unwillingness or just the practicality of using biometrics for visitors or day-to-day deliveries.

“General visitor access is normally made more difficult by introducing pre-visit booking, real-time host authorisations for entry and visitor management systems which can also use biometric capture as part of the process, but which is not normally used for physical access.”

While Hendrik Combrinck, MD of ZKTeco South Africa agrees with the above, he also cautions that each estate has an ecosystem of its own that needs to be taken into account when considering biometrics.

“Probably the most important factor is the logistics at the entrances and exits. The two main issues an estate needs to consider at these points are the speed and security they need.

“I always recommend that estates do a
proof-of-concept before making the final decision. The main benefit of biometrics technology is that it replaces other technologies that can be lost, stolen or even passed on to people that must not have access to the estate."

Weakening your security
This concept is expanded by Rautenbach, who adds that residents not participating, due to fear of sharing their biometrics or due to their being unable to use biometrics, introduce risks biometrics is supposed to avoid. “When issuing one person with a password or a PIN on a biometric controlled infrastructure, it can be argued that the whole security system is compromised as PINs or cards can be shared or lost. In this case, when a syndicate gets hold of your card, it can introduce risks to the entire estate.”

He notes that the new trend of using mobile credentials, such as NFC or Bluetooth Low Energy (BLE) opens up new ways of reducing these risks. With mobile credentials, the ‘secure credential’ is loaded on the user’s mobile and acts as the card for access. The reason why this improves security is the fact that the card is specific to the mobile device, and in today’s mobile-dependent society, one will definitely realise if your phone has been lost, and one does not easily share it with someone else. Standard insurance requirements to block a mobile device if it is stolen also means that the card becomes null and void.

“Although criminals and syndicates will continue to find flaws in security systems, biometrics does make it more difficult when managed correctly, and the deterrent alone does help reduce breaches in security,” Rautenbach says. “The measure of controlling employee, domestic and contractor access through biometrics on its own enhances the safety of the estate without a doubt. For me personally, however, the convenience is enough to win me over.”

Given the publicity around other forms of biometrics, Janse van Rensburg notes that it is important to note that certain biometric technologies are just not mature or robust enough for use in estate applications. “Facial recognition and iris or retina systems, for example, are not optimal for estates as they are not designed for external applications and are reliant on the user being face-on or in the same position every time they transact, which is almost impossible as the biometric system will more than likely be deployed on vehicle access points. “Basically, this leaves fingerprint biometrics, which has its own set of challenges, but if the correct product is used then the system works wonderfully well. Once again, dependent on the product being used, fingerprint biometrics are secure and it allows the management of the estate to keep a better handle of who has access and who doesn’t. The challenge with any estate access system is always how to handle contractors and workers, as this tends to be fluid once the right biometric technology is chosen and installed and managed properly.”

How to handle refusals
No matter how you promote the benefits of biometrics, whether it be speed or security, there will always be those who can’t or won’t use it. On the one hand, people may see it as an invasion of privacy and refuse to enrol because they don’t know how biometrics works and nothing you say will dissuade them. Then there are those who will balk at fingerprint technology due to, shall we say, a less than sterling past they fear will catch up with them if their fingerprints are checked against a law enforcement database or are ‘out in the wild’, as some people believe will happen when scanning a finger on a biometric reader.

Then there are those whose fingerprints just won’t be read. Elderly people can often fall into this category as their prints are
Continued from page 59

worn, as can people who are involved in manual labour.

The list of people who can’t be fingerprinted, as well as those who should not includes children younger than 7, which Janse van Rensburg explains have little or no friction ridge definition. Additionally, he says children between 7 and 18 have friction ridges that constantly evolve, while people over the age of 65 start losing friction ridge definition due to the skin losing its structure.

Moreover, he says people with diseases such as psoriasis have awful friction ridge definition and people undergoing chemotherapy often have issues with friction ridge details constantly changing. He adds that the Multispectral Response Imaging technology VIRD uses addresses many of these challenges and has a usability rate of about 98%.

To handle these and other ‘no-read’ scenarios, estates will need to make another plan. Fortunately, Combrinck explains, multi-biometric terminals are becoming a popular option at estates. This can allow a combination of biometric recognition, such as fingerprint and facial recognition combined, or it can also include additional verification modes, be it a type of card reader or PIN pad people can use to access the estate.

At the same time, Rautenbach notes that while there used to be a significant percentage of people who could not be ‘read’, technology has advanced and ‘over the past 10 years we have seen a 90% decrease in these cases.

“Alternatives that exist include multi-modal biometrics, where either one or the other can be used, such as facial recognition. In the past facial recognition did not work in direct sunlight or fluctuating light conditions, but once again technology has shown that these hurdles can be overcome.”

He adds that not every estate can afford to implement multi-modal systems and therefore the go-to solution is issuing cards or PINs. “Once again the utilisation of mobile credentials does offer some benefits over standard cards.”

Another option would be to use combined fingerprint and finger vein readers, which are more popular today. This technology reads the unique patterns of the veins in your finger, even if your fingerprint is unreadable. Combrinck suggests that an option would perhaps be to use finger vein readers at vehicle entrances and facial recognition at the employee entrances and turnstiles.

He adds that one can’t force someone, such as an employee, to use biometric access systems, but it can be made mandatory depending on the rules of the estate. If the written policy is that all employees need to be vetted, for example, they will have to agree to being fingerprinted at least once if they want the job. Naturally this is a sensitive subject in this country and should be handled with care.

On this topic, Rautenbach adds that most employers require criminal clearances as part of the screening process, and this applies to estates as well where failure to do so can cause harm to the residents and everyone else on the estate. “Employees are therefore well aware of biometrics, and employers using it for access control are not frowned upon in South Africa.”

The privacy question

Although many raise their eyebrows when questioned about the safety and privacy aspects of using biometrics, and in this instance we focus on fingerprint biometrics, it is a concern for many. The standard argument is that when using a PIN, password, card or mobile credentials to gain access, if your identity is compromised you can block the access and issue a new one. With fingerprints, if someone does manage to copy your prints and somehow manages to use it to identify themselves as you, what can you do? You certainly can’t be issued with a new fingerprint, and the same applies to other biometrics, be it face or finger vein etc. How do the biometrics vendors counter this?

“Your system is only as good as the installation,” says Combrinck, “and this is very true in this context. All the manufacturers take these points very seriously and go out of their way to secure the whole experience, from the hardware, communication protocol and the database storing all the information. This is the same with ZKTeco.”

It all comes down to the product being used, says Janse van Rensburg. “There are some biometric products that will keep a physical image of the fingerprint on the database and these are the ones that are prone to hacking. Most tier-1 products, however, only keep the fingerprint template as a hexadecimal string in the database. These templates only carry information in regards to minutiae points and not the complete fingerprint, so even if the database does get hacked, the complete fingerprint is not there.

“Think of it as GPS coordinates without a map. Add to this that tier-1 vendors encrypt this template to a proprietary AES standard and the whole trope about stolen fingerprints falls apart.

“Many systems are vulnerable to ‘spoofing’ where fake fingerprints can be manufactured from household items such as bathroom silicon or candle wax and it is important that the product being chosen have LFD (Life & Fake Fingerprint Detection) technologies as part of the product specification. It must be noted that in instances where spoofing is involved, the fingerprint was stolen not from the system, but physically – in other words, lifted from glass etc.”

It also helps putting the whole issue in context. Rautenbach counters, “It is far easier to steal your neighbour’s fingerprints..."
off a glass after an invitation for sundowners or for a stranger to do the same while ‘collecting recyclables’ from a dustbin, than trying to hack a fingerprint reader.

“Fingerprints are so widely used because it is what you leave behind at a crime scene, or at your neighbour. If you have concerns such as this you should ensure your fingerprint provider uses certificate-based, industry-recognised encryption and live finger detection, which is now the standard against spoofing, and it counters the fear of your finger being chopped off to get access.”

Technology options
Fortunately, all the interviewees in this article represent tier-1 biometric vendors, meaning that their products will incorporate the latest in terms of security and privacy technologies.

When asked what would be his recommendation for using biometrics on estates, Combrinck says he always recommend a robust and cost-effective solution. “Since the launch of the ZKBioSecurity system, which includes access control, visitor management and camera integration modules, we have seen a dramatic uptake by estates because of the ease of use. This system dramatically cuts costs for estates by integrating to our inBio controllers that only need slave biometric readers to provide access.”

Janse van Rensburg’s recommendations include IP65 rated products that have the necessary user count required for the estate. “From a ViRDI perspective, I would only use our AC2200H and ACS000Plus units for estates. If the user count exceeds the user count capability of the terminal, we can always revert to network authentication

---

Total estate security

Ensure you and your residents have peace of mind with an intelligent security solution designed to protect your estate inside and out.

security.gallagher.com

---

For more information contact
Suprema, +27 (0)11 784 3952, enquiry@suprema.co.za, www.suprema.co.za.
ViRDI Distribution, +27 (0)11 454 6006, deon@virditech.co.za, www.virditech.co.za.
ZKTeco (SA), +27 (0)12 259 1047, hendrik@zkteco.co.za, www.zkteco.co.za.
BIOMETRICS

Selecting your biometric solution

By Andrew Seldon.

Considering biometrics? What questions should you be asking?

We know biometrics can solve many access and identity related problems, but what does one need to know when shopping for a biometrics solution. The sad reality is that all biometrics are not created equal, and while it may be a budget bonus to buy your products over the web at a cheap price with free shipping, you may be buying a world of trouble.

Then there’s the challenge of selecting an installer or systems integrator to advise you and do the installation of the biometric solution. Can you rely on the chap in the bakkie to set up the system properly, including the server and backups (and the security)? Can you count on them to support you over the long term?

We asked a few people to give us some insights into how an estate manager should go about making sure the biometrics and service provider chosen makes the grade. We also asked what needs to be done, or changed, with PoPI (the Protection of Personal Information Act) just around the corner.

Installer selection

So, what does a good biometric (or even a good access control) installer need to know? What questions should the security manager ask to see if they make the grade?

Marius Stoop and Marcel Kooiman from Security & Communication Warehouse say that a sound solution methodology is key to the standard offering. Further, a detailed requirement statement will help clarify the ability to meet the requirement. A good question would be to find out where similar systems have been implemented successfully, as well as:

- Understanding of the terms involved with access control is a good indicator if the installer is knowledgeable in the field.
- All access control systems require a firm understanding of IP networks, hence the installer needs to be able to set up a basic network.
- Operation of the software is easy once the IP setup is complete, if the installer can set the network up, the software training is usually the easiest part of the solution.

Andrew Levell-Smith from Regal Distributors says, “The simplest and most effective way of selecting an installer is to ask for references. Don’t only ask for reference sites, but actually visit them. Quality of installation is largely a matter of taste. Make sure that you like what you see and not only what you hear from others who may have different preferences to you. Ask their previous clients about their experiences.”

Embracing and extending this thought, PinnSec’s MJ Oosthuizen adds that the estate should ask to see the system or product in their own environment. “Enrol two or three users and test it for yourself. Too many products and offerings are made by integrators that work from a datasheet, without realising the true relevance of the product.”

Other issues Oosthuizen raises include whether fingerprint biometrics work in all environments on the estate. Additionally, what is the verification time for a user to be granted access, and what is the longevity, scalability and support on the system?

Selecting the technology and brand

How does one make the decision about which technology and which biometric modality to choose? Every vendor will tell you that their products are fast and secure, which is important, but what makes the technology work in the real world?

“In my opinion, speed and accuracy of the transaction in addition to the quality of the device should be a major consideration for residential estates with many tenants, visitors and contractors,” says Levell-Smith. “It is essential that devices that have international quality certifications, independently tested algorithms that aid in the accuracy and speed of transactions.”

Oosthuizen adds that, whether we like to admit it or not, budget outweighs requirements on many occasions. Considering a vendor requires one to look at the scalability of the system, and the ability to upgrade and grow the system as budget/requirements changes. “The time the proposed system takes for authentication (especially in high traffic or visitor access areas) needs to be considered as well as the longevity of the proposed system.”

Just as reference sites are crucial, so is the ability to develop specialised features the estate may require, note Stoop and Kooiman.

“Many advances have been made through development and integration. Some new...”
features, like recording the conversation of a visitor at registration, stored in a centralised database where the visitor can be audited and reviewed, should be considered as valued features.”

They add that access control boils down to three basic flavours:
• Memorised PIN: A very crude and ineffective access control method.
• Card: An intermediate option, card systems provide better security and are easier to install than biometrics, but are not as secure.
• Biometrics: This can be fingerprint, facial, iris scanners and many more. Though difficult to roll out, the system gives excellent security and is easy to use if set up correctly. It is well known that fingerprints are not always viable for all persons, so a mixed biometric/card system is recommended.

Levell-Smith agrees, noting that it is important to note that fingerprints do change as we get older, and even with all the advances in fingerprint technology, there are still fingerprints that simply cannot be captured. “So systems that are able to use multiple token types like cards, PINs and fingerprints should be considered above devices that only authenticate a single token type.”

And as an additional, although (we hope) unnecessary warning, he adds that there is a vast difference in terms of functionality, price and quality between the lower-end devices and top-tier devices. This is clearly evident in the pricing of a biometrics system. The old adage of ‘you get what you pay for’ is certainly apt when considering biometrics devices or systems.

“I would not recommend facial recognition devices for a residential estate until it is a proven method of accurate recognition under multiple environmental conditions. Having said that, there have been some amazing breakthroughs in this method of biometric recognition and it is definitely one to watch for the future.”

When selecting a vendor, Stoop and Kooiman advise that good communication between the vendor and their supplier is the key to a system. Brands that build their own readers and supply their own software are a must, as it eliminates many issues when software or firmware fixes are needed. A good variety of readers is also good, as customers will be responsible for the way their staff handle personal information – such as fingerprints and other identity data.

Moreover, people are increasingly worried about where and how their private information is stored, notes Oosthuizen. How secure is the data? Where is it stored (on a PC workstation in the guardhouse at the estate entrance)? One needs to ask the question on what the relevance of the requested information is. If there is no live and direct feed to a database to verify details like an ID number, any information, fictitious or real, becomes irrelevant.

Some key aspects of PoPI, according to Levell-Smith, are:
• How is the personal information processed?
• What reasonable measures are in place to ensure the personal information collected is secure?
• What reasonable measures are in place to ensure the personal information collected will not be used for or distributed to any third party?
• What reasonable measures are in place to ensure the personal information collected is only held for the necessary period?

In terms of fingerprints, it is important to ask how the actual fingerprint is processed. Is it possible to recreate the fingerprint from the collected template? Is the actual fingerprint image stored or simply the unique minutia information? Has a reasonable effort been made by the manufacturer to ensure that fingerprints cannot be copied and used on a device to gain access? This is commonly known as liveness detection or ‘fake and live detection’.

“What measures are in place to ensure that the personal information is deleted after a certain period or when the resident moves out?” Levell-Smith asks.

Data encryption and a chain of data custody can address most of the PoPI concerns, says Stoop and Kooiman. Also, the flexibility of the enrolment and management software and process should be able to help manage these requirements.

“The estate should always ask the level of the software’s encryption. Encrypted data is safe data. The estate should also be aware that they need to manage their own passwords and access to the system. It is also recommended that the supplier is not a state-owned company, experience has taught us that the state can and will abuse their access to other people’s systems, the WannaCry scandal should serve as a warning here.”

At the end of the day, selecting a biometric solution for an estate (or anywhere for that matter) is different from selecting a boom for your gate. Not to discriminate against booms, this equipment needs to be able to open and close hundreds or even thousands of times per day in large estates. However, your biometric solution needs to work fast, accurately and the estate also needs to secure the information collected and stored in accordance with regulations. Choosing the cheapest solution is not an option. You can always revert to a guard opening the boom if the electronics fail, but if your biometrics and data management fail, you will be compromising your security and your legal obligations.

For more information, contact:
• Pinnacle Security Solutions, +27 (0)11 990 6000, sales@pinnsec.co.za, www.pinnsec.co.za.
• Regal Distributors, +27 (0)11 553 3300, info@regalsecurity.co.za, www.regalsecurity.co.za.
• Security & Communication Warehouse, +27 (0)12 653 1005, marketing@securitywarehouse.co.za, www.securitywarehouse.co.za.
Remote maintenance is a reality

By Andrew Seldon.

The annoying thing about technology is that it breaks. The perplexing thing about technology is that sometimes we can leave it alone and it somehow decides to ignore the settings we prescribed, or adjusts them for reasons unknown.

When something does happen, it’s an investment in time and money to get someone clever to fix it or replace it. While there is nothing we can do about the limits of technology today, there is something we can do to limit the losses in time and money, and in the security world, potentially more serious losses when systems aren’t working. In other words, we can perform regular maintenance on systems to ensure they are in working order and doing what we want them to do.

The traditional way of maintaining your security infrastructure (or any electronic infrastructure) is to wait until something breaks or starts misbehaving and then calling in a technician. In some cases, estates contract with their service providers to have a technician on call with specified response times and so forth. There are even those who contract with service providers for regular maintenance calls, although many are loathe to do this as the HoA often sees it as spending money when there is no ‘real’ reason to do so.

But the world is changing. If we can guard our perimeters via remote monitoring, why can’t we keep our systems in check remotely as well? Even better, why can’t we remotely monitor our technology in a way that can proactively warn us before something goes wrong, allowing those responsible to fix the problem, where possible, before it actually becomes a problem?

Rise of the machines

With the Internet of Things (IoT) and artificial intelligence (AI) becoming more accepted in general, this has in fact become possible. More than possible, Bernard Senekal, MD of Naxian Systems says it has become a reality.

“IoT means that we connect the physical (in this case the devices and systems on site) to the Internet (securely),” explains Senekal. “IoT technologies then provide a mechanism for data collection and automation. Simply put, we can obtain real-time data about the health of systems while ensuring that responses (usually in the form of automated workflows) execute far more effectively than the traditionally manual, unconnected method.”

That’s not the whole answer to the proactive service we want, however. While IoT provides the facilities for data collection and process automation, Senekal says it is just good for data collection and advanced automation capabilities. The IoT does not provide the ultimate keys to the castle in the form of predictive and hence preventative maintenance (ensuring a technical issue is addressed before it occurs). For this we need AI and the associated learning technologies.

“In the case of a residential estate, you would typically want to ensure that the boom gate and/or biometric entry system is maintained before it simply becomes unusable and leads to increased risk because a manual procedure has to be put in place until the issue can be resolved. IoT with AI and learning avoids makes this a reality.”

Trust the machine?

Allowing a computer somewhere to keep your electronic equipment in good working order sounds good, but what about when it doesn’t work. Electrical outages, Internet blackouts, workers digging in the wrong place and cutting your estate off from the world, and a host of other potential problems may impact your ability to constantly monitor your devices.

Granted, an hour or two of not checking your electronics shouldn’t result in any major problems, but we all know that sometimes systems just don’t work. How reliable would an automated, electronic monitoring system be in the real world?

“If the architecture of your system is built in a way that ensures data from the site is available consistently, and you know how to make use of the data, then you have reliable results,” states Senekal. “You can never predict every problem that may arise from a site beforehand. Sites do however mature over time and become 100% predictable if you follow some good practice guidelines.”

He says the following points will help ensure reliability at an ever-increasing level:

1.) You don’t keep the resolution of the fault as the intellectual property of a specific field engineer, but force the capture of the resolution back into your systems.
2.) Monitor the strengths and weaknesses of your field resources and automate customised e-learning for them in order to address weaknesses.

3.) Reference back to libraries or expert systems that obtain the resolutions for specific problems so that even the most untrained or incompetent resource has a resolution matrix to follow when they get to a site.

4.) Ensure your systems and site experiences are logged and are the intellectual property of the estate rather than remaining with a few human resources that eventually move on, placing you back at the ground floor.

One of the greatest challenges faced by the IoT industry is data gathering and processing. Two primary issues exist. One is that the vastness of the data in terms of the amount of data records that are being captured, while the second is the processing of this data after it has been sent to a central location.

“Currently the cost of distributing this data collection and processing function to the edge (to the site itself) so that we have filtered data in the offsite processing environment is costly because of the processing required for advanced automation algorithms. At Naxian we have recently ‘cracked’ this challenge and we are in beta stage with a technology that will ensure that data collection, data retention and advanced automation and analytics can run on extremely affordable hardware at the edge.

Impress the boss

While this publication is focused on the security aspect of residential estates, IoT covers everything electronic, including security. Therefore, while the security manager may want to monitor and manage security equipment automatically, the option is there to use the same infrastructure to manage any electronic devices used in an estate.

When asked what else can be included in the list of electronics that can be managed, Senekal says, “think battery life-cycle management, air conditioners, traffic lights, locomotives, diesel engines, transformers, multi-function office automation machines, the ECUs on motor vehicles and so on.”

Basically, this automation can be applied successfully anywhere one finds electronic ‘things’ that require predictive and preventative maintenance and life-cycle management in order to optimise efficiency, reduce risk and cost, and enhance profitability.

Naxian performs the above services for estates (and for a host of other industries) using its locally developed product, Synapse, and its AI agent, Annie (Artificial Neural Network Inside Everything). “Our platform stems from the PSIM command and control environment, but has been adapted to the IoT space where we see any and every device as just another signal with a specific signature. We are therefore not limited to a specific technology discipline or manufacturer in terms of what we can talk to.”

Listing the benefits of Naxian’s service, Senekal says the company is ideal for local estate customers because:

• It is locally developed, which means it is built for South African conditions. Where else in the world do you have the type of residential estates with the level of security that you have in SA?
• Because it owns the technology, clients can select from various pricing models which are not affected by currency fluctuations.
• Naxian’s IoT platform is linked to its AI, so it can provide predictive and preventative maintenance, whereas most of its competitors can’t.

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

The concept of setting up security in layers is not new, it has been one of the integral aspects of security since castles had moats with a drawbridge as the only entrance. The idea that layers are necessary came about as people realised that one layer is never enough. No matter how secure you think a particular layer is, there is always someone who will figure out a way past it, which is why we need other layers to deter them from further incursion.

In the residential estate environment, the perimeter is normally the first layer of security designed to keep people safe. In reality, there should be an external layer made up of community safety efforts and law enforcement, but this is often a missing link in the local environment.

Today an electric fence is seen as a standard accessory for the perimeter, and many will say this isn’t even enough. Over the years, technology has improved the ability to protect the perimeter and Hi-Tech Security Solutions asked a few experts how today’s estate can more effectively protect itself.

Maurice Williamson, CEO, Stafix Electric Fence Centre confirms that conventional walls and fences provide a physical barrier to would-be intruders and that they may in fact even deflect some, but a determined intrude will ultimately scale a wall or cut his way through the fence. To deal with this, walls can be built higher and have obstructions along the top of them (broken glass, spikes etc.) and fences may be barbed, but ultimately, on their own, they can both be breached with no warning given to those inside.

Williamson also warns that these measures could also cause physical injury to an intruder and, as strange as it seems, this may lead to expensive litigation.

“The only system that can be added to walls or fences that really offers both a strong deterrence as well as detection is a monitored electric security fence, “ Williamson says. “One only has to drive through the streets of our cities and towns to see the proliferation of what was formally an agricultural management tool that has been adapted for security purposes, to appreciate the popularity of this system of perimeter security.”

Unlike every system, electric fencing has its detractors and its weaknesses. They can be shorted out, cut or bridged, but as criminals have become smarter, so too have electric fences. He explains that modern fences can detect cuts, shorts or heavy loading by monitoring the voltage or amperage along the fence line, and now even a change in resistance on the fence line can be detected, making bridging all that more difficult.

“Monitored electric fences can also be sectorised into multiple sectors, facilitating accurate and speedy response.”

When addressing perimeter fencing, Cliff Rose, MD of Modular Communications says physical fencing technology has seen enormous change over the past five years. The market has seen an increase in the use of welded mesh panel products which are marketed as ‘high security’ fencing options.

“In fact,” says Rose, “the market has found that it is possible to climb over or cut through these mesh panels, it just takes a little longer. Where the market has changed dramatically is in the electronic detection technology with complementary applications to the above-mentioned mesh security panels. Detection systems which listen to what is happening on your fence and give an early warning is becoming the norm for the layered approach to security on the perimeter.”

Alarm, location and image

It’s not only fencing technologies that have advanced. Today there are other technologies that complement these solutions, adding additional security to the boundary. “We
have seen the emergence of thermal imaging cameras in this area as the technology has become more affordable for such applications,” notes David Montague, EMEA sales director for security at FLIR Systems.

“Thermal offers several key advantages for perimeter security. You can achieve detection of an intruder in the day and at night, and in most weather conditions. They can theoretically detect a man up to 20 km, but all lens options provide extended detection distances in comparison to visual cameras. This also means the installation cost can be considerably less than other solutions as fewer cameras are needed.

“With an uncooled thermal camera, there is little or no maintenance and hardly any moving parts, which reduces the risk of failure.”

Another adherent to the idea of having cameras as a critical component of your perimeter security is Charles Harrison, MD of Secu-Exports.

“Traditionally, securing a perimeter is done using static cameras. We have recognised a weakness in these systems in that once the intruder has breached the barrier, it is impossible to know where they are and to successfully track them. We recommend using PTZ (pan tilt zoom) long-range thermal cameras on high sites that allow you to get a 360-degree view that covers not only the perimeter, but also the internal and external areas.”

Harrison calls this wide-area situational awareness as it helps security operatives not only detect a breach of the perimeter, but provides the ability to track the target as they move around.

The costing issue
Not only are perimeters long, especially in the larger estates, but securing them is expensive – simply consider the costs of erecting a wire-mesh fence over a few kilometres. However, the question of costs comes down to the value estate management places on its occupants and their security.

“Electric fencing pricing can be tailored to fit an estate's budget, starting with a simple high voltage single zone, single sector monitored fence going right through to sophisticated multi zone, multi sector installations. In general, electric security fences are very economical and effective,” says Williamson.

Rose adds that AcoustAlert is also an option as it is a versatile product and has applications on various types of fences and walls, as well as below the fence line to detect under-digging. For larger perimeters (greater than 600 metres), multiple field processors are required around the perimeter and these need to communicate alarm conditions back to the central or off-site control room. However, if the estate also has surveillance cameras around the perimeter, it could include the AcoustAlert field processors and sensor cable onto the perimeter fence, or the estate can integrate the CCTV onto the AcoustAlert LAN.

Of course, cameras are somewhat more expensive to use on the perimeter, but as noted above, they provide additional security over and above other technologies. Montague notes, however, that justifying the use of thermal cameras on the perimeter is easier today because of the significant decrease in the prices of these devices. “Some of the benefits of thermals are that the initial purchase price is affordable for most, the failure rate is very low, you tend to need fewer cameras compared with other solutions as the distance viewed is greater. In addition, Flir

Continued on page 68
Continued from page 67

offers an advanced replacement programme, if needed, and a local repair facility.”

Adding to the cost benefits one can derive from thermals, Harrison says Secu-Export’s systems can be solar powered and run independently of your power infrastructure, and a wireless data link can be used if there is no fibre optic cabling. He adds that the software can be integrated into “just about any existing VMS backbone”. Secu-Exports can also offer a rent-to-buy option.

After the breach

It is in the ability to track suspects after they have breached the perimeter that Harrison believes Secu-Systems comes into its own. “Our long range PTZ thermal camera, supported by software analytics, allows you to track the target. Depending on the camera used, we can pick up targets well before they reach a critical area.”

Montague agrees, noting that Flir is seeing “a significant uptake in the detection and tracking”. He suggests using a fixed thermal camera to view down a fence line that hands off to a PTZ multi-sensor system when a person breaches the boundary line, which will then track the target.

Rose adds that while AcoustAlert is primarily a detection system used on the perimeter for the specific purpose of early warning, CCTV cameras should be used to track intruders, firstly at the point of intrusion (which is identified by AcoustAlert) and then to see where they may have gone.

The concept of tracking is also fraught with difficulty in residential estates as there is always the potential to be accused of invasion of privacy. The important issue, he says is to know as soon as possible when you have a potential intrusion or violation of your perimeter security. “This highlights the importance of the layered security approach which should include your earliest warning systems.”

An electric fence on its own can’t track an intruder, but can identify a breach and cameras. Following that, the estate can consider the analytics that will produce the best results, whether resident on the camera or remotely.

“Following this you would need to think about the video management system where there are many options to consider.

Once you have created a detection system, consideration should be given to the actions following an alarm, what will you do with the alarm and what will be the response: armed response, drones, etc.”

As far as Rose is concerned, if consulted for a greenfields project he would specify the following perimeter solution as a minimum:

1. A high security mesh panel fence system of at least 2.4 metres high.
2. A concrete under-dig which includes an AcoustAlert detection cable.
3. A five or six strand electric fence above the 2.4 metre fence, split into manageable detection zones.
4. AcoustAlert as your fence detection to protect the mesh panel fence and to be your early warning for intrusion or interference on the fence line.
5. Fixed thermal CCTV cameras to verify and validate any alarms.
6. Lighting that switches on in vicinity of the violated detection zone.
7. Audible warning via a distributed speaker system to give a verbal warning to intruders.

Besides the above, the most important consideration will be:

1. How do we respond as quickly as possible to the intrusion, and
2. How quickly can the threat be neutralised.

“If you have difficulties with these two questions you may need to revisit your perimeter detection, deterrent and delay principles in order to mitigate the risk at hand.”

Harrison advises estates to plan for the installation of a control room where an operator can monitor the perimeter cameras and respond accordingly. He adds, “Detect, respond and arrest. Don’t respond and hope-fully detect and arrest.”

Best greenfields advice

Existing estates have the advantage, or some may say the disadvantage of having some form of perimeter security in place. This will play a strategic role in deciding how to further enhance their perimeter security, either by adding or enhancing the current installation. In greenfields (new) projects, those responsible for security can look at all the options and decide on what the best solution is to start with, and plan to enhance this over time.

When it comes to new projects, Williamson advises starting with a multi strand, multi zone, multi sectored monitored electric security fence, which can be added to a well-constructed wall or mesh type fence. Furthermore, he suggests this should be integrated via a VJA Perimeter Patrol system to the camera surveillance system, all of which is monitored in the guard house as well as at the monitoring security company’s headquarter.

“T’d also recommend installing outdoor beams at more vulnerable areas. The whole system should be managed by a competent and reputable security reaction company.”

After the physical fence is in place, Montague says you can plan for thermal security. Flir offers a design tool at www.flir.com/security/content/?id=74677 (short URL: securitysysa.com/flir17a) where one can upload a site location and set out the

“Detect, respond and arrest. Don’t respond and hopefully detect and arrest.”

– Charles Harrison, MD, Secu-Exports

provide the security team with the location of the incident. Williamson explains that for further security, Stafix also distributes the Roboguard and Askari outdoor beam systems and the CP-Plus range of cameras, “both of which, strategically sited, can track an intruder’s progress.”

Rose adds that while AcoustAlert is identified by AcoustAlert) and then to track the target. Depending on the camera

Ndlovu Fencing T/A Stafix Electric Fence Centre, +27 (0)33 342 6727, ndlovu@stafix.co.za, www.stafix.co.za.

Secu-Systems, +27 (0)11 794 7834, charles@secusystems.co.za, www.secusystems.co.za.
PERIMETER SECURITY

Thermal buffer zone

Keeping your perimeter on the boil with thermal perimeter security solutions.

By combining Flir’s thermal security cameras and video analytics control and management software, the thermal fence system provides automated perimeter surveillance, intrusion detection, and alert capabilities for any perimeter security application. Secu-Systems has developed a complete perimeter protection solution that addresses estates’ specific needs, as long as standard operating procedures are followed in respect of the estate protocols.

**Increases security buffer zone**
- Provide earlier warning.
- Improve event response time.
- Increase situational awareness.
- Respond effectively and efficiency.

Achieving reliable thermal perimeter security around critical assets often comes down to detection accuracy and solution cost. Thermal perimeters have proven to be the most effective means of securing a perimeter. Thermal imaging has significantly advanced over recent years and the result is a market tipping point for thermal solutions in relation to other approaches.

The PTZ tracker analyses captured video signals to send alarm notifications of people, vehicles and objects that cross a perimeter line, enter a predefined region or are left behind or removed from a scene. Users can set customised rules and criteria to define the perimeter and what should be detected.

For sites with Pan/Tilt/Zoom (PTZ) cameras, the unit controls the PTZ camera to autonomously track and zoom in on the threat. These capabilities are now more cost-effective, making it possible to introduce thermal perimeter security cameras to a new range of mainstream applications.

Fewer cameras are therefore required making this more economically viable. In short, using long range analytic thermal imaging for your perimeter can do more than just protect the perimeter, it can increase your buffer zone with high accuracy.

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

**Importance of Perimeter Security**

By combining FLIR’s thermal security cameras and video Analytics control and management software, the thermal fence system provides automated perimeter surveillance, intrusion detection, and alert capabilities for your perimeter security application. We understand your challenges in securing your critical infrastructure and protecting your perimeter. We also understand that, like every customer, your requirements are unique. With that in mind, we have developed a complete perimeter protection solution, that addresses your specific needs. The solution is a game changer in the security arena and allows for little human error. Standard operating procedures must however be followed in respect of the estate protocols.

**Increase security buffer zone**
- Provide earlier warning
- Increase event response time
- Increase situational awareness
- Respond effectively and efficiency

Contact us for more info | info@secusystems.co.za | +27 (0)11 794 7834
Security by radar

By Andrew Seldon.

A little bit of radar makes the estate world go round.

The perimeter is one of the most vulnerable areas of a residential estate, as these are normally long and impossible to have under observation all the time. Apart from traditional fences and walls, other surveillance methods are today used to create a more complete perimeter defence – as evidenced in this year’s Residential Handbook. Another technology that has not been widely used in perimeter defence to date is radar.

In the article below, Hi-Tech Security Solutions looks at radar solutions that have been, or are about to be, released that can be used for perimeter security, as well as securing other areas within an estate.

It stands to reason that radar is not the only perimeter solution one needs on an estate or in any other environment. While these solutions will be adept at finding intruders, loiterers and so forth, they are unable to identify people and require integration into a broader security platform for a more complete security solution.

Axis network radar detector

September 2017 will see Axis Communications expanding its range of products with the addition of a network radar detector that the company says offers cost-efficient perimeter protection and will also decrease false alarms.

In talking about the product, Axis co-founder Martin Gren said the network radar detector will help to secure outdoor properties where there is normally no human traffic. The solution will be cheaper than a thermal camera, covers a broader area and will work in almost all types of weather conditions. Users will also be able to use their surveillance solutions with the radar to obtain visual footage of an intrusion or other alarm event.

The radar detector will also work in a variety of markets, not only the residential market, from warehouses to construction sites, and so on. Details are still under wraps at the time of writing as Axis will only formally be launching the radar detector later this year.

Avigilon IoT radar sensor

Avigilon has also launched a radar solution, its Presence Detector. Unlike the outdoor Axis product, the Avigilon Presence Detector (APD) is a sensor that combines self-learning analytics with impulse radar technology to accurately detect the presence of a person even if they have stopped moving or are hidden. This sensor is designed for indoor locations, such as ATM rooms, clubhouses and other closed indoor vestibules and can accurately detect a person’s presence through blankets, cardboard, wood and drywall.

The company says the combination of self-learning analytics with impulse radar technology provides up to 99% accuracy in the detection of a person.

With a small and discreet design, the APD can be hidden above ceiling panels or behind interior walls. Available in surface, corner or wall-mount options, it uses standard IP security camera infrastructure and cabling, making installation fast and easy. The indoor impulse radar sensor scans and learns the environment, continuously adapting to reduce false positive events, providing high accuracy in detecting the presence of a person at distances up to nine metres from the sensor.

The APD is expected to be available in the third quarter of this year.

Integrated flat panel radar

The third company releasing radar-based solutions is Management and Supply of Security Solutions (MASS). The company explains that the Athena flat panel radar combined with the Silent Sentinel rugged dome camera provides early warning of activity along the perimeter or in an open space. Athena is able to detect activity within the preconfigured field of detection, issue a notification and automatically position and track the target, providing visual identification through either the Oculus or Aeron surveillance platforms.

The Athena offers a modular solution to open space detection without the need for extensive infrastructure installation, enabling the solution to be quickly deployed. Available in four range options from 130 m to 1350 m, the panels can be combined to provide up to 360-degree coverage with four panels.

Each panel can be configured to provide detection zones with increasing levels of sensitivity. For example, where a footpath passes near a secure boundary there may be a zone where alarms are not triggered, then a zone warning someone is straying near the boundary, and then another to say the boundary has been penetrated with escalating responses to each zone.

For more information contact:
Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com.
Avigilon, +27 (0)79 079 6528, charnel.loftus@avigilon.com, www.avigilon.com.
Management and Supply of Security Solutions (MASS), +27 (0)12 142 0000, info@mass-solutions.co.za, www.mass-solutions.co.za.
PERIMETER SECURITY

All-live and kicking

Criminals are getting smarter, more daring and quite simply, more desperate.

Conventional electric fences have been around for a long time and remain a very effective means of providing a strong deterrent to criminal ingress. A conventional electric fence uses alternating wires for live and earth potential. A positive pulse is injected onto the live wire at roughly 1 Hz. (one pulse per second).

If anyone touches between a live and earth wire, or touches a live wire whilst standing on the ground, he/she will receive a non-lethal but unpleasant electrical shock. Touching an earth wire will have little or no effect. So roughly only half of the fence’s wires ‘bite.’

The live wires may be in a series or loop configuration, which can provide immediate notification of a live wire being cut anywhere along the zone or sector. The earth wires are almost always connected in parallel to maintain a good continuous reference voltage for the live wire. Cutting an earth wire will have no effect provided it does not come in contact with another live wire.

Some older fences may still have the live wires in parallel too, a carry-over from agricultural fences, or a ‘cheat’ to make the fence appear to be running at full voltage, while masking some poor installation or maintenance shortcomings. As soon as any wires are placed in parallel, one loses the benefit of cut protection monitoring as the electrical path now has several branches to use and simply diverts to another available path.

A relatively new concept is to deploy an all-live wire configuration. Here the previously parallel connected earth wires are reconfigured to a second live circuit or loop. Two simultaneous, but oppositely charged pulses are injected onto the two adjacent circuits. A positive pulse onto the old ‘live’ circuit and a negative pulse onto the newly reconfigured earth wire circuit.

The net result is a shock if you touch between any two adjacent wires, regardless if you are earthed or not, or a half voltage shock if you are earthed. The net results are: an all-live wire fence, cut protection monitoring on every wire, reduced and equal voltage across all insulators with respect to earth and a fence which is far less vulnerable to manipulation.

This concept also works particularly well on wall-top installations where an assailant will not necessarily be in contact with earth while attempting to challenge a fence. The new SANS regulation requirement of regular earth spikes takes care of providing a continuous reference voltage around the perimeter.

Elf Rentals started converting some of its premier clients to the all-live wire fence configuration in 2015 to afford these residential estates a new and improved level of protection. The result has been a transformation of what were high-maintenance sites to very stable and very secure perimeter fences, where both client and service provider are reaping the rewards.

For more information contact Elf Rentals, +27 (0)41 368 3701, www.elfrentals.co.za

High-end performance, quick search results, ultimate satisfaction!

A security manager responsible for the security and welfare of the residents and personnel of the estate wants:

- Crisp, clear images irrespective of ambient lighting
- Products from an internationally recognised market-leader
- Seamless integration with his access control system, perimeter detection and video analytics
- No licence fee hassles
- A long term solution, with complete backward compatibility of his software and firmware
- The fastest video retrieval of incidents of any VMS (Video Management System)
- Indisputably the most efficient data storage in the industry saving him a fortune on server and storage costs

In short, he shouldn’t be talking to anyone other than MASS for Indigo Vision’s solutions........

Call MASS today!

CALL 012 142 0000 NOW!
or e-mail info@mass-solutions.co.za
www.mass-solutions.co.za
Chapman’s Bay Estate is a unique, low-density, security estate set up against a private bay. The estate offers spacious homes with spectacular bay and Table Mountain views. It boasts being eco-friendly and one of the most secure estates in the surrounding area.

In order to maintain this harmony and serenity, it was necessary to ensure that homeowners and their properties are thoroughly protected. The only way to achieve this is through the deployment of an advanced security system supported by cutting-edge products.

Accomplishing this involved dealing with a number of security concerns, including the vast perimeter of the estate. An effective early-warning detection system is of the utmost importance to be able to detect and respond to a range of possible threats from the neighbouring mountain.

Innoza Group, the security system integrator for Chapman’s Bay Estate, selected Axis thermal network cameras to overcome the challenge of providing a surveillance solution within a completely dark environment. The estate required the use of smart analytics for detection and the ability to send out alerts, if an intruder was detected. Another important requirement was minimal false alarms.

Axis was the clear solutions provider of choice on this front as well because it offers one of the most advanced perimeter defences managed by analytical software, the Axis Perimeter Defender. According to the Innoza Group, Axis also offers a much more user-friendly experience to the end-user.

“The Axis thermal cameras are an integral part of our security measures because they helped make a challenging installation simple, whilst providing the Rolls-Royce in surveillance systems, quality products and user friendliness at the same time. This culminated in a very effective perimeter defender and analytics setup that delivered very little false alarms and no perimeter breaches," says Daniel Van De Venter, managing director at Innoza Group.

Today, the absence of illumination no longer hinders the detection and apprehension of intruders. In addition, residents of Chapman’s Bay Estate can enjoy the peacefulness and splendour of their bay-side vistas, without the potential threat of security-related incidents.

Since the installation of this state-of-the-art surveillance system, there have been no incidents or breaches of the perimeter.

**24 hour, 7 days a week detection**

A total of 22 thermal cameras were used, with each one overlapping another to ensure the whole perimeter was covered with no blind spots. The Axis Q1941-E thermal camera is able to reliably detect and provide fast verification of each situation on the perimeter. Since thermal cameras do not need a light source, they can achieve higher accuracy and fewer false alarms than conventional cameras in most applications.

Supporting Axis’ Zipstream technology, the Q1941-E filters out those areas with no motion, and it can focus on the parts of the image that are moving. This significantly reduces the bandwidth and storage required. This is crucial because the Chapman’s Bay Estate site is monitored on- and off site. The security guards on site use the system and then there is another off-site monitoring company that monitors and responds to incidents. The footage is stored on a local- and off-site server.

A thermal camera is mainly used for video analytics and detection in areas where no-one should trespass or walk around. Based on this premise, the video shows no image unless an intruder is detected.

**Visual verification**

Furthermore, a PTZ (pan, tilt, zoom) camera was fitted at the highest point of the estate to be able to react to alerts and provide visual support for guards patrolling the area. Innoza Group selected the AXIS Q6115 due to its high-performance PTZ dome, offering 1080p resolution, 30X optical zoom, and fast and precise pan/tilt performance for wide area coverage and great detail when zooming in.

The Sharpdome technology of the Q6115 includes Axis’ Speed Dry function that will help to provide sharp images in rainy weather. Moreover, it can also simplify dome cleaning, allowing for more efficient methods, such as high-pressure cleaning.

This camera sports IP66-rated protection against dust and strong water jets, and is weatherproof with built-in protection against dust, rain, snow and sunlight (IP66- and NEMA 4X-rated), and impact resistance (IK 08-rated).

Additionally, the camera is further protected with shock detection, a capability that sends an alarm in the event of attempted vandalism or prospective intruders tampering with the system.

There are already plans to expand the surveillance security system. The estate will add more IP cameras to cover risk areas internally once the construction phase is complete. Additionally, there are also other sites planned for similar installations. Innoza Group is going to a world renowned estate in George soon to finalise another solution.

For more information contact Axis Communications, +27 (0)11 548 6780, sasha.bonheim@axis.com, www.axis.com
Is estate living really safer?  

By Terry van Zyl, CTO, RDC.

Estate living is safer, but in no way completely immune to crime.

Is estate living really safer? This is a perception that is mostly true, but several large and seemingly highly secure estates experience burglary sprees and violent robberies. Although less regular in occurrence compared to other popular or more traditional forms of living, it is still not totally immune to crime.

How does security differ between estates and complexes?
Estates are, in most cases, much larger than traditional housing complexes and therefore have larger budgets for increased security measures. They normally feature a larger variety of protection systems including physical barriers, electronic equipment and security staff.

We often hear of criminal activities in estates despite having guards at the gate, cameras and access control systems. Why?
Most people living on estates buy into this lifestyle believing that it is totally secure and crime-free. They generally relax their awareness to identify threats like new and suspect neighbours, worker patterns, etc. Criminals operating in estates vary from professionals who blend in with the residents by renting properties, to petty theft by workers and even young residents with drug habits which they support by selling stolen goods.

How can residents protect themselves to a higher level on estates?
Homeowners can improve their security by installing a monitored alarm system, even while believing that it is not necessary on their estate. It is a well-known fact that very few alarms are installed and monitored on estates because of the security that already exists. A working alarm will deter burglars from entering a home when they know it will attract immediate attention from neighbours, estate security or armed response. Neighbours living on estates are more likely to know their neighbours and their movement patterns than in the suburbs. A monitored alarm system also offers fixed and wireless panic buttons to be used.

How can estate security improve their reaction to incidents inside an estate?
A monitored alarm system can be linked directly to an armed response company (preferably SAIDSA-approved), but also directly to the estate control room for immediate reaction by the estate patrols. The RDC VHF alarm radios have the capability to report to both the armed response company and the estate control room at the same time. The RDC base-station in the control room can receive the alarm signals and immediately display the unit number or address where the alarm was triggered.

Panic packs are also available if residents don’t feel that a full alarm system is required. These panic packs can also be monitored by the base station in the guard house without external armed response.

How does FTTH affect my alarm communication to the control room?
Fibre-to-the-home is a type of digital data communication that can link your home to the Internet. It differs from traditional communication from the alarm panel to the control room using a telephone line. Most FTTH lines are not capable of linking to your alarm panel telephone line interface. The RDC VHF and cellular radios are both capable of replacing the telephone line connection when FTTH is installed. Most new alarm systems also feature an optional IP interface that can be connected directly to the FTTH router or network switch. This can act as a secondary (backup) communication path to the control room.

For more information contact RDC, +27 (0)11 452 1471, brent.a@radiodata.co.za, www.radiodata.co.za.

Terry van Zyl.
Guard monitoring technologies have become an essential tool to ensure secure estates.

Physical security is often still the most effective measure to protect an area, particularly when it comes to residential estates where there may be a high volume of foot and vehicle traffic at all times of the day and night. Security guards are an indispensable part of a physical security strategy, but as always, when it comes to the human element, they can cause more harm by not doing their jobs properly than if they weren’t around at all.

When a breach does happen, the easy way out is often to blame a guard rather than investigate whether there were other reasons for a lack of security. This can be easy to do if there is no way to determine if guards were where they were supposed to be or whether they were slacking off.

Guard monitoring technologies have become an essential tool to ‘watch the watchers’, as well as the converse: to protect guards from spurious accusations by residents or estate management that they weren’t doing their job. Hi-Tech Security Solutions asked three leading providers of guard monitoring technologies to share their thoughts on some of the challenges, and their particular solutions.

Active Track

“During the past four years of being in the guard monitoring business, we have serviced customers of various sizes, ranging from as few as five up to as many as three thousand security officers,” says Active Track’s Casey de Villiers. “However, regardless of the size, all customers are faced with the challenge of personnel management.

“This is particularly so with residential estate security where the monitoring of the comings and goings of all residents, domestic workers, visitors, contractors and personnel, as well as the structures in place to promote the safety and well-being of persons on the estate, is of utmost importance.”

Active Track specialises in workforce management solutions for South Africa’s residential and industrial sectors. One of its key guard monitoring products is the Active Track, an RFID, GSM and GPS enabled, handheld guard monitoring device. Through its GPS functionality, it enables the tracking of movements of security officers, while the GSM capability allows for the triggering of panic and distress functions in an emergency situation, and two-way communication with security officers. The resilient design of the Active Track, being waterproof and tamper-proof, with a battery life of up to 72 hours, ensures that it can withstand the unpredictable environment of residential estates.

The unit can be tracked by estate management and security service providers, remotely and in real-time via Active View, an online portal which monitors and records the movements and events of each Active Track device. A dedicated 24-hour support centre also has access to Active View, and is suitably trained to monitor the movements of Active Track devices, and assist both security officers and management in emergency and panic situations.

To ensure that duties are carried out correctly, site-specific parameters can be set to generate alarm conditions when breached. Alarm conditions are communicated to management by way of SMS and/or email, and the call centre via an alarm. This equips one to respond appropriately – whether this is the support centre calling the device to determine why a patrol was missed, or a response unit being deployed to site where an RFID tag was scanned under duress.

Active Track comes with a workforce management system, and can also be integrated into other management platforms. The patrol records of every security officer, and all events and alarms generated, are recorded and stored on Active View, the cloud-based support software. From this data, automated reports are generated and made available on a daily basis. At a glance, one can determine which security officers are failing to carry out their duties correctly, or at all, and take the appropriate disciplinary action. This results in improved performance overall, and increased accountability.

BetaTrac Telematic Solutions

According to BetaTrac’s CEO, Keith Lawrence, “the greatest challenge to any estate is to find the right passionate personnel to result in the coming together of all security guarding infrastructure into one well organised team of dedicated staff members. We have seen over the years how hard senior management plans and tries to expedite great initiatives, however it is not only the guards who may let them down.”

BetaTrac has created a guarding management solution called AIMSS (Analytical Intelligent Mobile Security System). It is...
built around a device called eGuard, which is body-worn on the left arm, out of harm’s way and allowing the guard to have full use of both hands. eGuard operates continuously by replacing the battery every 24 hours, and reports the guard’s movement and conditions every 30 seconds. Data is collected by the back-end and measured against many conditions, such as correct patrol routes via GPS, no movement, stop/start of patrols, reaching checkpoints, time taken to reach checkpoints, how many cycles as per schedule, as well as others. AIMSS is fully autonomous, producing daily performance reports, detailed reports and off line status reports.

The system has a three tier matrix escalation, ensuring that all relevant people will be notified when an alert is triggered. For example, in the first hour an alert will be sent to assigned supervisors or a control room, and if not attended to within an hour, it is escalated to an operation manager. Reports are generated automatically for senior management to see how the process was managed. “There are zero excuses as we supply an abundance of data to make sure the whole team is aware of status conditions,” says Lawrence.

AIMSS is supplied with a control room software platform which is SQL database driven, enabling integration into other systems if necessary. BetaTrac has also developed a web-based live viewing platform with OTP (one-time PIN) access for senior management to view and analyse live situations, as well as an Android smartphone app for easy, accurate setup of all guard route patrols.

**Econz Wireless**

Econz Wireless identifies major challenges as being guards’ attempts to sleep instead of guarding, or being at the wrong place. It offers the Timecard GPS, Timecard Lite and Eservices solutions, which use GPS and job tracking within a given area, or according to a job dispatched. By providing real-time alerts and tracking, time sheets are eliminated with clock-in/out, breadcrumb tracking, etc.

Econz Timecard GPS and Timecard Lite may be used for one or more guards, and the location can be smart fenced to ensure attendance on site, or at the correct positions at predetermined times. Features available include clock-in lock, pre-determined clock-in times and locations, all of which can be seen from the control room.

Once a smart fence is predetermined, if the guard strays outside of that virtual fence it will be shown at the call centre or supervisors’ devices via an alert so action will be taken. Similarly, if the guard has not moved for a preset length of time, an alert will be sent to the call centre or supervisor, as well as the guard.

Their locations are tracked using GPS technology and automatic checks on location, breadcrumb trails, etc. can all be preset.

Econz provides a full workforce management system in the form of Eservices, which does everything from simple tracking to job alerts, reports, signature and/or photo sign off, inventory for parts, and alerts so that supervisors can check job management, breadcrumb trails and timesheet clock-in/out. The solutions may be fully integrated with existing payroll, job and workforce management and time and attendance systems.

For more information contact:
- Casey de Villiers, Active Track, +27 (0)11 551 1687, casey@activetrack.co.za, www.activetrack.co.za.
- Keith Lawrence, BetaTrac Telematic Solutions, +27 (0)11 782 5335, keith.lawrence@betatrac.com, www.betatrac.com.
- Bette Kun, Econz Wireless, +27 (0)10 500 9637, bettek@econz.com, www.econz.co.za.
Word has it that technology is going to put thousands of guards out of work as electronics take over the security function en masse. However, visit any residential estate and the one common security feature (apart from an electric fence and a gate), is the much-maligned, much disrespected, yet essential guard.

As much as business owners see dollar signs in their eyes when they think of replacing human resources with technology, security will always be a people business and having staff to do the ‘peopling’ is non-negotiable. There may be fewer guards, but until intelligent robots arrive, there will always be a place and a requirement for guards.

That’s not to say the guarding industry isn’t under pressure to change and up its game. Competition is fierce and costs are under pressure more than ever in the dire ‘state capture’ economy we find ourselves in. More than that, the demands of customers are also increasing and changing with respect to what they want from their guards and guarding service providers.

So, what are guarding companies doing to improve their service to residential estates? How do they make sure they keep their customers happy, their guards committed and the never-ending criminal onslaught at bay?

Hi-Tech Security Solutions asked three companies active in providing guarding services in the estate market for their insights into the modern guarding function. Firstly, looking at the guards themselves, we asked what skills or aptitude do people working as guards on residential estates need that may not be the norm in other environments.

Enforce Security is active in a number of estates offering both human and technical resources. Its responses came from Derek Lategan (MD) and Glenn Allen (technology director), who noted that it stands to reason that the security requirements of every site will differ according to the nature of the environment, hence the aptitude of guards working on residential estates will differ to security guards operating in other environments.

“At Enforce Security we talk about tailoring our solutions and services to meet the needs of our individual clients. This is displayed in part in the understanding that various residential estates will require security officers with specific temperaments and personality characteristics, depending on their individual needs and requirements.

“It is important to note that each guard should possess skills individualised for a specific residential estate that he/she is operating in. The skills possessed by guards working in estates should not only be industry-specific but also client-specific, meaning that the skill of every guard should be applicable to the nature of that specific estate.”

Key to security

Tim Timmins, technical director, ESS, at G4S Secure Solutions (SA) adds that the key to ensuring safety and security on residential estates is the ability to communicate effectively. “Security officers deployed in such environments need to have excellent communication skills in English, and an understanding of basic public relations (PR) techniques is highly advantageous. Due to the highly visible nature of the work they perform, which includes but is not limited to access control duties, patrolling and providing security at events, golf clubs or recreational facilities on the estates, security officers must be healthy, with a smart physical appearance. And it is imperative that they are able to multi-task.”

Dave Sleep, reaction division director at Stallion Security contends that this is definitely a specialised market segment in terms of the provision of physical manpower. “Stallion has in fact made this a specialist business within our group. The security officers are trained as per PSIRA regulations to the same graded...
levels as other security officers performing
duties in other market segments. They do,
however, have better communication skills,
particularly in English, in terms of reading,
speaking and writing, and undergo specialist
PR courses to deal with the varied people and
personalities in complexes and estates.

“Although it does take a while to settle into
these environments, mainly due to receiving
abuse from residents at times, they require the
additional PR skills to cope with the demands of
having anything from 20 to 3 000 clients,
because, after all, all residents become your
client. Our residential security officers are also
handpicked. Not just anybody can do this job.”

Having the right fit in terms of the person
on duty is important. Some of the estates they
serve are enormous with a variety of tasks the
guards are assigned to handle. How can estate
managers and guard supervisors ensure their
staff are where they are supposed to be and
doing what they are supposed to do? Is this
simply a function of set schedules and
supervisors travelling around to check up, or
are there technical solutions that can both
assist guards in their duties as well as check that
they are doing the correct patrols and so forth?

Technology as support

The answer is both. Manual processes are
indispensable, but technology assists in the
implementation and management of those
processes.

There is a magnitude of technology avail-
able, says Sleep, which includes guard moni-
toring systems and CCTV options, but regular
physical visits by management and supervisors
can’t be ignored.

“The technology around guard monitoring
systems has improved immensely and most of
them are live-monitored these days and have
panic and phone capabilities for the patrol-
ning officers, should they find themselves in
need of assistance. They are also equipped
with technology to detect and report failed
patrols, point failure and deliberate dropping
of the device, as well as if the device is in a
lying down position. Once these anomalies are
detected, action is taken as either the guard is
avoiding the duties assigned or is in trouble.”

Timmins agrees, but says it starts with clear,
detailed and documented procedures. “This
could be of a manual nature such as parades
inspection at the start of a shift, shift reports
and hourly patrols via the control room. But the
ideal would be basic procedures coupled with
technology for improved reliability.”

The technology he refers to could include
mobile biometric time-and-attendance
systems, or guard monitoring systems such
as Bloodhound, Instacom or CCTV. If security
officers patrol using vehicles, he says vehicle
tracking systems are highly informative.

The Enforce team says technology is pivotal
to managing its staff and sites, as well as
providing transparency and open customer
access to performance information. Velocity,
Enforce’s management platform, encompasses
the following best-of-breed technologies that,
along with manual management systems,
ensure the company manages its operations and
staff effectively:
- Biometric time-and-attendance interfaced
directly into Enforce’s rostering system,
which presents real-time attendance data to
to control rooms.
- GPS-based patrol monitoring.
- Virtual Inspector, a remote monitoring
system Enforce developed for a visual
inspection of guards on remote sites that is
also used in off-site control rooms.
- Velocity Audit, an electronic SLA management
platform the company developed to measure
the performance of teams against pre-defined
outcomes.

Convergence is key

Using both human and technical resources in an
integrated fashion is key to effective guarding
today. Sleep says there is a need for both, but
that technology can reduce total manpower,
reduce costs over long term if the right provider
is chosen, and will enhance the overall security.
“If an estate boxes smart, they should never have
the need for perimeter and/or internal patrolling
security officers, if they use technology properly.”

Timmins adds, “Analytics, automation and
firmware algorithms, integrated into unified
systems provide security personnel with
improved capabilities and shifts the focus to
a more proactive approach. We have seen a
significant demand for automatic perimeter
intruder detection and tracking systems that
use intelligent thermal cameras and native
algorithms.

“These detection systems are aimed at
preventing incidents, instead of reacting to
them, which is a far more modern approach to
security operations.”

Enforce Security also recommends a con-
verged security solution to residential estates
and communities. “By blending technology and
traditional guarding, we are able to provide estates
and communities with the latest CCTV surveillance
technology as well as those who operate it.”

The training question

As noted above, the guarding operation is chang-
ing, as are the functions guards are expected to
perform. Apart from the regulatory training
required for guards, companies today also train
them to handle the environment they will be
operating in – such as PR training for estates.
However, estate guards do not have a set syllabus
as each estate has rules of its own that guards
and their companies must learn and adhere to.

For general training for estate work, G4S
ensures its staff understand the intricacies of these
environments with learning modules such as:
- Introduction to estate security
- Access control
- Security administration
- Radio procedure
- Protection of assets
- Key control
- Legal aspects
- Crime prevention
- Emergency procedures

Furthermore, Timmins says the company
also meets with the homeowners’ association
and/or the security manager to obtain details
of estate-specific procedures and training.

Ultimately the estate security manager is
responsible for implementing the manpower SOP,
says Enforce, but he/she would usually do this in
conjunction with the security service provider. This
is because the estate manager is knowledgeable
on all matters pertaining to the estate, such as the
residents, the type of estate, the expected security
levels, and the quality of life of residents, while the
security service provider is the professional when
it comes to the actual security strategy.

“By working together both parties can then
device a thorough and effective security plan
while still keeping with the ‘feel’ of the estate
and the quality of life residents are accustomed
to, and expect.”

Stallion takes much the same approach.
Once estate-specific rules and job functions
are agreed upon, these are drafted into working
documents and signed-off.

Estates are a unique challenge. They may
seem like relaxing places, as they are supposed
to be, but that does not apply to the security
operations. Guards on estates are tasked with
the role of securing the estate and its
people, while being PR agents to the residents.
Choosing the correct service provider that
takes the time to understand your estate and
its intricacies while ensuring its staff do too, is
well worth the effort, time and money.

For more information, contact:
- Enforce, +27 (0)31 573 7600,
info@enforce.co.za, www.enforce.co.za.
- G4S Electronic Specialised Solutions,
+27 (0)10 001 4500, ess@za.g4s.com,
www.g4s.co.za.
- Stallion Reaction, +27 (0)11 533 8823,
daves@stallion.co.za, www.stallion.co.za.
Planning to install the latest and greatest technology in an estate to support the security function can be a daunting task for estate and security managers. Apart from being responsible for spending an enormous amount of money and being held responsible for the installation’s performance for the next few years, one has to make decisions about what products and partners to select. Not only do you have to choose wisely in terms of the installation, you also need to make a decision regarding ongoing maintenance and support, knowing that while you can point the finger when service providers make a mess, the homeowners’ association or body corporate is always going to point the finger at you.

In times like these, it is often easy to look at the cool and expensive things in your decision-making process, the cameras, storage, kilometres of fencing and so forth. Often, decision makers tend to forget the unseen parts of the security equation. One of these less fashionable bits is the communication solution you will need to make your security system work, in other words, your network. Most of us pay scant attention to the network, after all, it’s a cable transporting data that may be video or smaller amounts of data from electric fences or access control points, and a cable is a cable. Or is it?

Hi-Tech Security Solutions approached a few people in the know to ask them whether a cable really is a cable, and to find out what options there are when looking for a networking solution, or solutions for an estate. First off, we asked whether there was an optimal solution when it came to networking today, specifically when looking for a network that would not only transport video and other security data, but could also potentially link to the various residences. Naturally, fibre was a winner.

Fibre is it
Bronwyn d’Hotman Kotzen, brand manager at Datanet, says the optimal cabling solution for the whole estate would be fibre on the perimeter, gates and all connecting buildings. The advantage of fibre is that this network can also be used for FTTH (fibre-to-the-home). Tobie van Schalkwyk, business development manager at Duxbury Networking agrees. “Undoubtedly, the preferred and optimal cabling solution today is fibre optic cabling. One of the drivers is the fact that increasing demand for faster networking speeds is driving down the cost of networking equipment, supporting Gigabit and even 10 Gigabit fibre ports.”

“Fibre optic cabling has so many benefits, the knowledge of which is gaining currency in residential estates. Fibre cabling is faster, the cables do not easily break, they are unaffected by electromagnetic interference and the signal loss is significantly less than with copper cable.” Fibre is also the choice for Marco de Ru, Miro’s CTO. He says the main limitation of traditional copper cabling is that it can only support distances of up to 100 metres without repeaters. A passive optical fibre network, on the other hand, can support distances of up to 20 kilometres. Many estates support...
perimeters stretching over many kilometres, making fibre the only realistic and cost-effective option for the long-term.

In South Africa copper theft is, unfortunately, a reality we have to deal with, adds Van Schalkwyk. Most organisations will think twice before installing a copper-based infrastructure no matter what its specifications are. In a residential estate, copper theft has the potential to reduce revenues for the estate as it diverts budget from maintenance to repairs and the replacement of infrastructure.

In cases where estates need their network to cross roads or rivers and they don’t want large engineering projects, De Ru advises that low-latency, high-throughput wireless networks are the way to go. These will complement the speeds of fibre and can be set up quite easily to cross obstacles and ensure the whole network functions seamlessly.

Van Schalkwyk adds that in some cases, estates are also looking at wireless links from a central point to the perimeter or to/from residences as a service option. “Often fibre cabling and wireless links are considered together as a solution as the technologies are complementary.”

Is copper dead?

If fibre and wireless networks are producing such good performance without breaking the bank, can we assume there is no further requirements for copper network cabling?

While installers can set up any network without copper cabling today, it is not realistic to do so. In normal houses and offices, for example, De Ru says a 100 m copper cable run is more than enough and it can support the bandwidth required for video and so forth. Copper is also naturally still used in businesses around the world where it can support data networking and VoIP (voice over IP) telephony, according to De Ru. In most cases Cat5 copper cabling is acceptable, although Cat6 is somewhat more immune to electronic interference.

d’Hotman Kotzen echoes the usefulness of copper in homes and businesses, but notes that buyers should be aware of the differences in copper cables. For example, Cat5e was not designed for PoE (power over Ethernet), while Cat6 has higher operating margins. Cat6a does offer increased performance and will support up to 100 Watt PoE.

She says the brand of cabling used will not necessarily impact the transmission rates, however, well-known brands will conform to all the necessary standards and offer long-term warranties because of the quality built into the cables.

At the same time, she says your average end user will not be able to differentiate between good and poor cabling until they experience it in action, by which time it’s too late. The best guide to quality is the warranty offered, notes d’Hotman Kotzen. Insisting on a 15 to 25 year warranty certificate will determine how much faith the manufacturer and installer has in their cable.

Of course, Wi-Fi is a great option to extend copper infrastructures in homes and other buildings. De Ru notes that modern Wi-Fi solutions are even better than before due to the introduction of MU-MIMO (multi-user, multiple-input, multiple-output) technology. Put simply, this technology allows an access point to service more than one user at a time without having to share the bandwidth – which results in better performance for users.

For public hotspots, such as clubhouses, this will make a significant improvement to the Wi-Fi performance, and today Wi-Fi is something people expect to have wherever they are.

The CCA question

CCA stands for copper-clad aluminium wire. It is a cheaper alternative to copper cabling made up of an inner aluminium core and outer
copper layer. This type of cabling is used in many areas, including networking where it can replace traditional copper. However, some say that it is a cheaper and less reliable alternative as the aluminium core can affect transmission speeds. The argument is that aluminium has a higher electrical impedance versus copper and that aluminium is less flexible and tends to break more easily.

Of course, network cabling is not something that is moved around a lot, and so breakage may not be such a strong argument against CCA.

There are two sides to this story and d’Hotman Kotzen notes that inferior copper or CCA cables are prone to increased degradation over time. “This would mean you would not just replace the devices but the entire infrastructure over time. You will also not get the correct voltage or wattage required to run your equipment and this, in time, can damage your devices. Also, CCA cable is not specified in any international cabling standard.”

In any case, she does not recommend installing any metallic cable outdoors unless you have taken the necessary precautions with respect to earthing and lightning protection. However, she notes, “There is no guaranteed lightning protection system.”

De Ru says Miro is aware of the uneasiness around CCA and has conducted its own tests on these cables. What Miro found was that traditional copper is more susceptible to spikes than CCA, making surge protection a must. In addition, when it came to PoE transmission, the difference between copper and CCA cabling was so small it was negligible.

However, De Ru notes that you need to use a high quality CCA cable that is made up, for example, of 30% copper. This will ensure a similar transmission quality to traditional copper cables, but it will handle spikes better. (He notes that no matter what cable you use, it is advisable to always have inline surge protection.)

For those not convinced, De Ru refers to the ‘Skin Effect’ According to Wikipedia, “The skin effect causes alternating current to concentrate on the more-conductive copper cladding of the conductor, causing the resistance of the wire to approach that of a pure copper wire at high frequencies …. ” De Ru says this means at high frequencies, the current is concentrated around the outer copper layer, by as much as 80% in Cat5 cable at 100 MHz. So, with the right quality of CCA cabling, one can save on costs while getting similar performance to traditional copper.

Network decisions
Taking the above views into account, we asked the three interviewees to end off by providing our readers with their top three tips on what estates should consider when considering the challenges of networking their environments. Van Schalkwyk’s top three points are:

1. Determine the cost of cabling (both long term and short term). How much will it cost to install cabling now and maintain it for future years? Copper might be cheaper to install, but expensive to support. Fibre will be more expensive to install, but cheaper to maintain. Wireless networks, on the other hand, may alleviate many cost headaches in future.

2. Factor in reliability and scalability. Copper cabling might support today’s demand, but will it support the regular doubling of voice and data traffic in, for example, two years from now? Fibre supports much faster speeds than copper and will result in significantly fewer bottlenecks on the network.

3. Budget for on-going support costs. If an estate opts for copper cabling, there will most likely be future costs associated with losses due to theft and damage due to lightning strikes, to which copper is susceptible.

d’Hotman Kotzen recommends estates use a certified installer, one who can produce documentation to prove their certification. In addition, she advises estates to ensure they obtain a warranty certificate on all the cabling installed. And finally, although it should be a standard practice, only use reputable companies you can rely on and that will be around in future when you need assistance.

De Ru’s first recommendation is compatibility. When using wireless networking, make sure the frequencies of all your devices match (for example, 5.8 GHz), and make sure you obtain the latest wireless technology, not old stock that’s going cheap.

As noted above, the demand for bandwidth is always increasing so make sure you opt for a Gigabit switch. Even if you don’t need it today, you soon will. Moreover, the price difference between a Gigabit switch and a 100 Mbps switch is not extreme.

Finally, he recommends buyers don’t compromise for the sake of saving a few rand, the long-term costs can come back and bite you. He recommends estates stick to reputable brands that have a local support structure, and only work with service providers with a good reputation.

For more information contact:
- Datnet, +27 (0)11 990 6254, bronwyn@datnet.co.za, www.datnet.co.za.
- Duxbury Networking, +27 (0)11 351 9800, lparker@duxnet.co.za, www.duxbury.co.za.
- MIRO Distribution, 086 123 MIRO, lerize@miro.co.za, www.miro.co.za.
Simple but secure home security

Panasonic’s Home Network System provides a broad range of security measures for the home.

Home security is a priority for the majority in order to protect loved ones and the memories, mementoes and priceless items in the home. At the same time, cost is always a concern, with many people unable to afford private home security services. It is for these reasons that there is a growing trend towards home security systems which can be installed by the user and are much easier on the pocket.

Panasonic’s Home Network System, for example, allows you to create a wireless network of cameras, sensors and controllers, both in and outside the home. These can be controlled with a smartphone, via a single app, and offer many additional benefits over standard security systems.

For example, the system doubles as a complete and comprehensive baby monitoring device, enabling parents to check in on the child using live video footage, streamed directly to their mobile device. It is able to detect motion, sound and temperature and can immediately notify you of any unusual conditions. In addition, the camera offers a built-in microphone and speaker, enabling parents to talk to the baby, or play up to five different lullabies to help it fall asleep.

In a similar fashion, external cameras will allow users to monitor their pets at any time and from anywhere – perfect for those occasions where you have to go away for a day or two. The same outdoor cameras are also useful for assisting you in checking who is knocking on your front door.

These cameras not only deliver real-time streaming, but also offer a quad view, enabling the user to view up to four cameras simultaneously, as well as providing motion detection for specific areas of the garden where recording and notification are considered critical.

Moreover, because the solution is run by an app on your smartphone, you can control lighting and appliances remotely too, turning devices in a room on and off, at anytime and anywhere. This means you can make it appear as though someone is in the house, even when you are away.

Panasonic’s Home Network System allows you to decide what solutions you want and add these to the network as and when they are required. It includes external and internal cameras, smart plugs for controlling your lights and doors, windows and motion sensors that will alert you if anyone enters your property.

Not only is this an extremely cost-effective solution, it is also simple and easy to install. The system can be set-up in three easy steps, without any complicated installation. Simply plug in the hub, download the Home Networking System app – which is available on both iOS and Android – and ensure your mobile device is connected to your Wi-Fi network. The system is seamlessly integrated with Wi-Fi and has a range of over 300 metres.

For more information contact John David, Panasonic South Africa, +27 (0)11 312 7015, j.david@za.panasonic.com, www.panasonic.com.
The point of paying a premium to live in a secure estate is that it is secure. Most residents assume this means their responsibility to look after their own security is therefore transferred to the security team, which residents sometimes support by trying to allocate the minimum budget possible for security.

Of course, there will always be a conflict between security and residents. Residents want 100% guaranteed security, which is never possible, while the estate managers want more money to accomplish more in the security realm, to try and get as close to that 100% goal as possible.

Nevertheless, the idea of abdicating your security to someone else is appealing, but dangerous. Unless you can afford a 24-hour team of bodyguards, you are unlikely to be untouchable. And even with them, John F. Kennedy would tell you: there is still a risk. So what should estate dwellers do when it comes to their own home security?

The fact is, your security teams do a pretty good job of protecting the perimeter and controlling access to the estate. But criminal syndicates are not stupid; they will find ways to get in. The cliché remains true: your security needs to be functioning at 100% capacity all the time, while the criminals can fall 99% of the time and still profit from their 1% success rate.

One also needs to consider that more syndicates are setting up shop inside estates, either buying or renting property to give them unhindered access to upmarket homes and goodies. Added to that, there is also the problem of people who seem to think helping themselves to their neighbours’ stuff is fine, and there are kids who are sent out on their own into the safe estate that get up to mischief and vandalism. And the list of potential risks goes on.

So securing your home, even in an estate, is a must if you really want peace of mind. The benefit is that you won’t have to worry about perimeter and access control, only your own house. To find out what home security options there are for estate residents, Hi-Tech Security Solutions asked a few people for some insight into products and solutions designed for the consumer market.

Alarms are so 1999
In many homes, especially the more upmarket homes, the age of the Internet of Things has arrived and people want everything connected. The same will apply to security, and we can see the result of this consumer demand in products that are managed via a smartphone and which can be integrated with other home automation solutions. A simple alarm is simply not on the cards for the connected elite.

Rex Pennefather and Matt De Araujo from Inhep Digital Security (IDS) confirm this, noting that alarms have for many years been driven by the demand created by crime and insurance stipulations. “As the South African security market has developed to maturity, so we are starting to experience the challenges of globalisation, commoditisation and the Internet on our industry. Our customers are now doing their banking, social media, and a good portion of their browsing on their phones and are expecting a unified ecosystem for the management of devices, appliances and security in their houses.”

They add that, in the past, alarms have been a grudge purchase for most people, and the industry is now challenged to transfer the feature set of its solutions into tangible value for customers. “IoT is the perfect stepping stone to this with a large portion of data, control and storage now being housed in the cloud and accessible by GPRS or IP connections. Customers who have historically been presented with an outdated and complicated static keypad can now access, control and interrogate their home from a device of their choice, a device that is intuitive and designed for consumer applications.”

The benefit of being in an estate, some of which don’t allow home alarms because of the noise factor, is that alarms can be linked
to internal control rooms or guard houses. In addition, the owner can easily be alerted on a mobile device or email, and can even view home surveillance cameras from the same device, says Vaughn Tempelhoff from Forbatt SA.

He adds that most suppliers are moving to cloud-based applications where remote viewing and accessibility is quick and easy.

“TVT is a good example where it is as easy as enabling NAT, switching your DVR on, and scanning a barcode.”

**Alarm II**

While some form of alarm is always a good idea to alert residents to risks, today’s alarms allow for much more than linking a passive and making a noise. Hikvision’s senior technical engineer, Toby Chao, explains that access control, video intercom and smoke/water/door sensors can be added to a modern alarm control panel.

“Even our lights, TV and washing machine can be added. In my opinion, home security systems can easily and effectively be mixed with non-security technologies. It simply makes sense that all technologies work together to make a smart, simple and an all-in-one home security system.”

“The alarm is the perfect integrated box to offer not only the much demanded security application, but also heaps of value-adds for the consumers,” say Pennefather and De Araujo. “Abroad we have seen the likes of Intelbras in Brazil, 2G and Vivint in the US, Amazon Alexa and many others embrace this opportunity and start to incorporate cable, internet, solar and lighting into their home solutions. Most modern alarms do not require much more than a simple GPRS, Ethernet or serial device to create an open source or proprietary platform for remote control and panel access. IDS has gone so far as to develop and app-based solution that can control alarm panels that were sold and installed as far back as 2005, yet work with the latest iPhone or Samsung smartphone.”

They say it makes sense to use your alarm as the medium to blend in and control non-security applications, provided everything is managed and correctly installed. With the rapid expansion of CCTV in Africa and the massive cost lowering initiatives underway by dominant players in this space, the challenge for local manufacturers is not to try and compete with these players, but rather to develop and incorporate platforms and interfaces that allow exchange between services and devices.

**Product options**

When it comes to specifying what products they have available that fit the above descriptions, the respondents have a broad selection. Hikvision provides the EZVIZ product range, which includes alarm and CCTV equipment for the consumer market, as well as access control and video intercom devices. The company also acquired Pyronix, a producer of alarm and detector equipment to supplement its home security offering.

Chao says all products can be seamlessly integrated into one single platform so that every event is visible. “For example, when a visitor swipes a card to open a door or presses a button to phone the house owner, or even when an intrusion alarm is triggered, users are able to see what’s going on in real time on Hikvision’s client software or mobile app. This either can be a live-view pop-up or an app notification, whichever the user prefers.

Chao explains that products from Hikvision are engineered to be easy to install and use. For example, many products support POE (Power over Ethernet), which allows users to simply ‘plug and play’ the equipment. When cameras and an NVR are connected, the backend device automatically finds and
activates the cameras, automatically allocating an IP address to make it quite simple, even for users without much IT knowledge.

Forbatt offers the TVT range for home security. Tempelhoff notes that TVT is known for its robustness and ease of use. The product caters for a wide spectrum of clients, from domestic use through to commercial applications. “TVT’s analogue range supports all current analogue technologies in the market, including AHD, TVI and CVI, making the product a breeze to install even if you are unaware of the technology the customer is using.”

IDS has developed the HYYP Smart Home app which seamlessly integrates with any IDS alarm solution and now allows homeowners the ability to control and have visibility of their alarm status remotely and in real time. The HYYP app allows users to arm, disarm and bypass zones remotely, as well as get notifications should there be a violation, bypass, panic or trouble condition. “Through our proprietary trigger command embedded in the app, users are also now able to control a host of outputs and triggers for home automation solutions. Key applications at present include using your alarm to remotely control your gate, garage, electric fence or switch your lights on or off, geysers, pumps and motors,” state Pennefather and De Araujo. “Essentially we can control any one of the 51 available outputs on the IDS X-Series control panels.”

They continue that both the HYYP GPRS Hub and HYYP IP-Connect module are simple to install and do not require IT or systems integration knowledge. “We have maintained the standard alarm install process using a preconfigured and highly secure smart platform and switch as well as DHCP routing control to optimise control, security and simplicity. Our Smart app includes a multitude of features requested by our control groups, like the ability to view multiple sites on your phone, to control which notifications you receive and which you don’t, the ability to store and embed user codes for trigger and control, and the ability to add multiple users with your desired control levels.”

Today’s estate resident does not need to install security solutions that simply sit there and, hopefully, do nothing. You can gain the benefits of reliable home security while also entering the IoT and home automation world by accessing and controlling a host of other functions from your smartphone. In other words, you can still obtain value from your installation without the ‘grudge purchase’ idea so often associated with security products and solutions.

For more information contact:
• Forbatt SA, +27 (0)11 469 3598, sales@forbatt.co, www.forbatt.co.
• Hikvision South Africa, Evan Liu, +27 (0)10 035 1172, support.africa@hikvision.com, www.hikvision.com.
• IDS (Inhep Digital Security), +27 (0)31 705 1373, marketing@idsprotect.com, www.idsprotect.com.
Integrated layers of security

Integration is the key to effectively securing your estate.

As criminal operations become increasingly sophisticated, so too do the counter measures. In the past, securing a residential estate with a security officer at the gate and a paper-based book for visitors to sign in was sufficient, but now the need to integrate manned guarding and technology is not seen as a nice to have, but rather a necessity in protecting ourselves.

G4S understands the ‘secure village’ concept of lifestyle estate protection and has the knowledge and expertise to offer a range of integrated secure solutions based on a comprehensive risk assessment. We also believe that security is the responsibility of everyone within an estate and that it is imperative to have the support of residents who need to actively participate in securing their environment and making security related decisions. You can install technology and provide all the man-power in the world, but if the back door is left open, so to speak, nothing will prevent criminals from taking advantage.

Once everyone is on board, we believe that the safety of an estate relies on multiple layers of security.

Perimeter: Starting from the outside and moving inwards, perimeter protection needs to be addressed first. Ideally, this decision needs to be made in conjunction with the developer and a balance reached between a secure perimeter and development economics. In most cases, electric fencing is chosen as a solution and is very effective. A critical area to plan for is the maintenance of the perimeter fencing and must not be overlooked.

Access control: This is the next area to address and there are many new and innovative systems available. Biometric systems are an effective way to record access and egress details and to ensure that identity is not transferred – as can be the case with card or tag-based systems. Where your gatehouse is situated is also something to consider in an estate. Your security personnel are also at risk of attack and should be protected within the layers we are recommending.

Within the estate itself, there are a number of other security measures that can be implemented, including video surveillance in high risk areas; fire detection systems and public-address systems in communal areas, and vehicle and manned guarding patrols. A detailed risk assessment will help to identify areas of risk specific to your estate and these can be addressed in consultation with developers and residents.

Residents should also accept responsibility for the protection of their own assets and immediate surroundings by installing alarm systems and barriers. Many people are lulled into a false sense of security when purchasing property in a secure estate, and forget basic security measures like locking doors and gates, and not leaving valuables lying around. Work with your security provider to ensure that all areas of security are addressed.

There is still one area of concern and that is what we term the ‘threat from within’. Increasingly crime syndicates do not access estates from the outside, but go as far as to purchase property and operate from within the estate. To resolve this type of threat we believe the solution is the integration of systems and the analysis of resultant data. This type of service needs to be conducted by security personal trained to do so. You can proactively secure your environment by monitoring trends and unusual activity and issuing alerts before criminals have time to act. The monitoring of such systems can be done on- or off-site in a number of different ways, using technology and/or personnel.

We must not neglect the importance of people and positive human interaction. By deploying well-trained security officers who understand the intricacies of estate security, you provide the human touch one would expect in a residential environment. Ensure that the staff deployed at your estate have undergone training specific to the residential estate environment and do not overlook the importance of skills such as providing life support or fire-fighting and soft skills such as public relations and conflict resolution.

Tim Timmins, technical director for G4S Electronic Security Solutions, says: “We believe that securing those dearest to you must take on a multiple faceted approach and that integrated solutions benefit our customers through direct cost savings, improved efficiencies and better operational and informational processes.”

For more information contact G4S Electronic Security Solutions, +27 (0)10 001 4500, tim.timmins@za.g4s.com, www.g4s.co.za
There’s an app for that

By Johlene Selemela, ZKTeco South Africa.

The right technology can assist estates in better security.

Ensuring peace of mind in a residential estate is of utmost priority to the body corporate as well as residents. Property owners in estates often have a false sense of security due to the environment already having a level of security with guards, electric fences and the like. However, residential estates are increasingly being targeted by criminals and often having a security company manage the estate is not enough.

Alarm systems and armed response can only provide a certain amount of protection to deter intruders. In instances when an alarm is triggered, security companies often only conduct perimeter checks as they are unable to gain access to properties. Most often by the time the guards arrive, it is too late and goods have already been stolen.

This has highlighted the need for remote monitoring of security devices via mobile devices. The most effective way to secure a property is to install a range of products that can be monitored on one platform and via mobile devices, thus allowing residents, home owner and security officials within an estate to ‘check in’ periodically or if an alarm event is activated. With the correct placement and usage of various security products any residential estate or complex will be able to ensure that the people living within their properties feel safe and secure.

Having a visitor management app will not only enhance efficiency within a residential estate or complex, but it ensures that visitors can be registered within seconds, with all necessary information captured. Such an app enables authorised personnel or even the residents within that estate to preregister visitors, thus helping to streamline the waiting process at the entrance of any estate or complex.

The app also ensures the handling of visitors is in accordance with the estate or complex’s policies and allows time for a watch check list before the visitor arrives. Visitor approval is sent to the authorised personnel via the app, which is connected to a mobile device and the proper access rights can be assigned. All information is stored in a secure database and can be conveniently retrieved for repeat visits.

Additional information can be gathered with visitor details to simplify future contacts. The visitor management app also allows the user to track visitors, assets and deliveries as they enter and exit the premises. It helps improve the efficiency, security and visitor service of any residential estate and complex.

In today’s world, with crime on the increase, biometric devices are gaining popularity in the residential security market. These devices can give accurate information as to who enters an estate’s premises, which can give a better indication of the events when an intrusion occurs.

Therefore, when buying products to secure any residential estate, body corporates need to consult with installers and system integrators on the best products available that will give their properties a comprehensive solution and ensure the residents have a clear outlook on the type of security they can look forward to.

For more information contact ZKTeco (SA), +27 (0)12 259 1047, johlene@zkteco.co.za, www.zkteco.co.za.
No sense of humour about security

By Andrew Seldon.

Louis de Jager has taken on the job of risk manager at Val de Vie to ensure residents live out the estate’s promise of a ‘life worth living.’

The Val de Vie Estate lies in the Berg River Valley in the Western Cape, about 35 minutes out of Cape Town. It is surrounded by the Simonsberg Mountains and is located on the banks of the Berg River. Val de Vie is a 1000-hectare estate divided up into various residential suburbs, including Pearl Valley with its Jack Nicklaus golf course.

Securing such a large estate is no small matter. Louis de Jager who incidentally also lives on the estate to ensure a 24/7 hands-on approach, has taken on the job of risk manager at Val de Vie. His job is to maintain an effective ‘thermal blanket’ of safety for residents within the estate, allowing them to live out the estate’s promise of a ‘life worth living.’

As can be imagined, the security team at Val de Vie has its work cut out for it in securing hundreds of homes and the families who live there. The perimeter of the estate is over 11 km long, which naturally poses an enormous risk and many opportunities for criminals.

The estate currently has 94 smart analytical thermal cameras covering the perimeter, all linked back to the security control room as well as Val de Vie’s offsite monitoring service provider – Thorburn Security Solutions.

De Jager says the estate has a well-trained team of outside perimeter tactical response officers who are armed and ready to attend to any attempted breach at a moment’s notice. Apart from being well trained, the team is equipped with the best available equipment as well as canine support. This team is further supported by unarmed response officers and guards on the inside who take care of the estate’s access requirements and other non-emergency situations.

De Jager says that the tactical team has proved its worth in various situations, describing them as ‘having no sense of humour and being capable of dealing with anything that needs to be dealt with’. They played a leading role in support and affecting arrests in a recent incident on a neighbouring farm when the manager was attacked by eleven machete-wielding individuals.

The primary aim and idea, which has been successful for many years, is to harden the outside of the estate to the extent of making it as visibly impenetrable as possible, keeping intruders away from Val de Vie and having potential intruders rather searching for softer targets elsewhere.

More than manpower

Of course, securing the estate requires more than only a modern perimeter security system and a well-trained team of tactical officers. De Jager says the estate’s security is intelligence driven and his team regularly interacts with other people and groups in the neighbourhood, such as neighbourhood and farm watches. Everyone cooperates in an all-inclusive and integrated approach to ensure the whole environment stays as safe as possible. The estate also makes use of a range of Online Intelligence products to manage and analyse data to make informed security decisions.

The estate’s access control is run via biometric technology which provides a more secure manner of controlling entry and adds to the intelligence in the form of an electronic occurrence book. The onsite guards, selected in cooperation with Thorburn, are also equipped with Instacom devices to allow them to work much smarter and if need arises, sound the alarm quickly and easily.

Moreover, contractors must register and undergo fingerprint-based criminal record checks before being allowed onto the estate. Domestic staff and tenants are also checked to ensure maximum safety for all. Naturally, before the estate employs anyone, a strict vetting and background check is run and the prospective staff member may even be required to undergo a pre-polygraph test.

Resident support

Critical to the success of the security function at Val de Vie is the absolute support the team gets from the residents. The security sub-committee is chaired by a resident and reports to the Homeowners’ Association. The sub-committee meets once per month with all concerned parties and assesses the security situation to decide on how to go forward with various initiatives.

There is no room for complacency and residents and visitors are constantly reminded that security begins at home and the less opportunist criminals the less the odds are that they will become targets and victims.

The hardening of the perimeter and the various security processes in place has paid dividends for residents as De Jager notes that there has been no penetration from outside for a number of years. Nevertheless, the security team can never rest as the criminal element is always planning something new and ready to test the defences again.

With professional criminals constantly adapting their modus operandi, security has to follow suit and stay on top of its game or face the consequences. The security sub-committee has therefore begun a process to ensure an eventual rollout of the best possible task and site-specific legal drone technology. This is no small feat as it is an extremely costly and arduous exercise sometimes taking up to two years to ensure all the legal aspects are covered and Civil Aviation grants all permits, pilot’s licences and so forth. It is an exciting prospect for all concerned though and one to look forward to.
Risk management approach to estate security

By Allyson Koekhoven.

Zambezi Country Estate takes a holistic viewpoint towards security.

Nestled virtually in the foothills of the Magaliesberg and in close proximity to the Roodeplaat Dam Nature Reserve in the heart of Pretoria’s Montana, Zambezi Country Estate is a secure haven for its residents.

According to the estate’s risk and security manager, Corné Meyer, the estate’s security portfolio needs to encompass more than just traditional guarding and boomed access gates. He emphasises that a risk management approach to security is essential to ensure that all elements work together for maximised protection of the residents, their assets and estate guests. However, although security is of the utmost importance within an estate, it in actual fact forms only a small part of the total risk management portfolio.

He quotes Thomas S. Coleman: “Risk management is the art of using lessons from the past to mitigate misfortune and exploit future opportunities – in other words, the art of avoiding the stupid mistakes of yesterday while recognising that nature can always create new ways for things to go wrong.”

The estate has identified that complete risk management needs to include the periodic changes in estate management as well as in legislation, such as the PoPi Act and the OHS Act. It is also important to factor in all requisite parameters and the budget when tenders to implement or upgrade security changes are requested. Furthermore, any changes in the implementation of a security system need to be undertaken in a manner that ensures the total safety of the system and its residents. This is coupled with the assurance that the contractor or sub-contractor has adhered to the OHS Act and all of the estate’s rules.

Eye-opener to risk

“We have strategically changed our approach to security by adopting a broader outlook and we noticed that there were loopholes in the systems, policies and procedures that were undertaken in an outdated manner. An example is that we were never quite sure if cloud-based surveillance footage was saved in a totally secure manner, or whether it was vulnerable to hacking. If you look at implementing risk management, this all creates a completely new security portfolio for estate security managers. Approaching security from a risk management perspective has been a total eye opener for us,” says Meyer.

While you still need security at the gates and patrolling of estate fences on a round-the-clock basis, there is, says Meyer, more to estate security than just that. One finds that the normal day-to-day running of estates includes the presence of visitors, contractors and other visitors, and school children after hours, all of whom are associated with their own inherent set of risk factors.

“Let us consider, for example, a child playing in a play area. They are hurt, so what are the procedures to follow when this event occurs? By having a risk management plan in place, we are now able to ensure that medical help is readily available. By communicating the risk management plan through to residents we are able to emphasise the fact that we are enhancing their safety and security and this gives them the peace of mind that they are well taken care of anywhere on the property,” Meyer explains.

Collaboration is essential

He says that it is important to have the backing of the HOA. This was achieved through a consultative process that outlined how the new risk assessment and management system’s outcomes would lead to an overall improvement in both the residents’ lives as well as adding reputationally to the estate, which would result in better property values.

“While we did encounter some initial resistance from some parties, once they were able to see the bigger picture they adopted the new system quite readily.”

When considering the most important aspects in an estate’s security operations, one needs to acknowledge that each estate is different. It is important to outline a vision and impress the importance of the security plan in terms of how it will positively affect the safety and security of residents.

There is an improvement within estates when residents work together with the HOA and security team on the development of a risk assessment and management plan. The majority of estates in South Africa have security systems and in general use a subcontractor or service provider who not only handles their security, but also the risk management.

“This is not a desirable situation and I would advise them to rather appoint somebody in the HOA office who is able to take all elements, including policies and procedures specific to the estate into consideration. A large reason for evaluating security on a site-specific basis is that you get to know the people on your estate and what their exact requirements are in terms of security,” says Meyer.
A primary reason for owners purchasing property within Zimbali is the safety and security offered by the resort. Not only does the estate have a full-time security manager – Albert Rode – who controls diplomatic-level security with unobtrusive systems and checkpoints, but he is also supported by a well-trained guarding and technical team.

This is a comprehensive, multi-layered perimeter-to-home system that begins with the electrified security fence, proceeds through access-controlled guarded gates and continues into the estate with a multitude of high-tech thermal and optical cameras.

“We have a holistic approach to security at Zimbali Coastal Resort. We have embraced the use of technology which enables our team to monitor who is on the estate at any given time. There has been a drastic change in our approach to securing Zimbali and we have had to evolve with our current crime trends and monitor the threats that gated estates are constantly face with,” says Rode.

The estate has upgraded its perimeter fencing by installing outriggers (V-brackets) that assist the team in fulfilling the ‘detect, deter and delay’ functions as well as in enhancing the mitigation of the over-under-through approach to intrusion.

“This fence is not just about aesthetics, but rather about providing an impenetrable barrier. The technology on our gates and booms has also evolved and we now use scanning devices at every entrance to the estate where all valid driver’s licences and motor vehicle licences have to be electronically scanned,” says Rode. Before entering the estate, visitors must use a pre-registered one-time code sent to them from the resident’s phone.

The estate also has many surveillance cameras, positioned in strategic locations. Rode points out that the estate undertook an upgrade programme in early 2013 and is currently in the early stages of embarking on the rollout of IP cameras to replace all existing analogue units and to supplement the existing IP cameras.

The move to IP has been made possible by the installation of a fibre backbone throughout the estate. All cameras are linked back to a sophisticated onsite control room with well-trained controllers, while system checks and maintenance are conducted by the dedicated technical team comprising an experienced technical manager and technicians.

Rode says that gathered intelligence plays a major role in the estate’s security. His intelligence background has provided a good grounding and he tactically uses this knowledge to gather intel from both internal and external networks, a tool he says is critical to mitigating risks. “Having knowledge on hand and looking at the things that will impact on the security of the estate and its residents is vital.

“I have used my many years of being exposed to all levels of crime and experience in law enforcement and security to benefit and safeguard the estate and my residents. A security manager needs to understand the geographic layout of the area (using statistics from the local SAPS), and since the residents’ needs are my first concern, personal interaction and communication with them plays an important role in my security operation on the estate. In addition, how involved one is in the local community and how the estate gives back to the local community is another factor to consider,” says Rode.

The addition of thermal cameras has resulted in Rode and his team being able to accurately monitor those people who are a possible threat to the perimeter. Before the introduction of thermal cameras, the estate employed a large complement of human resources on the 17 km fence line, but has been able to reduce this number with the feeds received from the cameras.

Rode advises those estates contemplating the implementation of security plans and processes to firstly conduct a comprehensive audit of the security that is currently in place. This, he says, includes manpower and technology, and should include an assessment of whether the security service provider is rendering a high standard of service as per the contract and service level agreement.

The Site Operational Procedures (SOPs) must be updated on a regular basis and the dynamics of the estate should be reassessed, since estates constantly change which impacts on plans and processes. “Weekly and monthly security meetings and detailed reports from the security service provider is essential to keep up to date with your security plans and processes. Secondly, you must have an immediate, short- and long-term vision for security; this allows you to budget correctly as this inevitably impacts on your security plans and processes.”

By Allyson Koekhoven.

Multi-layered estate security

Intelligence and technology protect Zimbali Coastal Resort & Estate.
Enforcing security at Izinga

Izinga Estates focuses on a tranquil lifestyle under the watchful eye of the latest security technology and best practices.

Izinga Estates is a grouping of residential estates situated in Umhlanga Ridge just north of Durban’s vibrant Umhlanga commercial and retail hub. Currently there are four estates that are developed or under development with further two developments to break ground shortly.

The key aspects of the security solution were to create a secure estate by providing effective security solutions and by using quality products to protect and manage security requirements of the estate and includes camera surveillance systems for the suburb entrances and patrols in open spaces and public roads.

Izinga Park falls within Izinga and is split into two gated entities that are divided by Herrwood Drive and is currently the only gated estate within the development. Access to Izinga Park is controlled by means of patrolled green Beta fencing and manned entrances. Electric fencing is included with the Beta fencing and monitored at a central control room. Each of the parks has two boom entries and two boom exits, as well as turnstiles for pedestrians on either side.

The security aspects of the estate was designed predominantly by Adamas Consulting and a formal technical security solution was created for tender purposes in conjunction with various stakeholders.

In respect to access control, an Impro IXP 400 access control backbone with Morpho Sigma biometric readers are installed. The access control system includes PT Guest as an integrated visitor management system.

The Cathexis VMS is used for CCTV surveillance and video management (VMS). Various cameras are installed, including 42 thermal cameras mounted on the fence line to protect against incursion along the perimeter. Furthermore, 62 optical cameras, including nine PTZ cameras are installed within the two estates, predominantly at the four access areas and at other critical locations. Over and above this, twelve ANPR (automatic number plate recognition) cameras are installed at certain points in the open estate to enable operators to ensure that vehicles that had been flagged on the database as suspicious could be tracked and reported. This is another method of crime detection and used to protect the area.

Security solutions selected by the relevant stakeholders were determined on the basis that they have been proven in environments of a similar nature and are, in general, products of choice used by the installation companies that install and manage security systems at other estates in the greater Durban area. As such, the level of expertise with respect to these products is high and due to local production and supply.

The Izinga Park security installation was done through a prescribed tender process designed by the appointed engineering security consultants. Enforce Security Services was awarded the tender; used internal installation teams that were managed through a strictly measured and controlled project process to ensure that timelines and quality standards were met.

Obstacles that were encountered during installation consisted of instances where new homeowners had excavated their sites too close to the fence line and certain instances jeopardised the secure foundation of some of the perimeter equipment and cable kiosks, and in some cases created obstacles which made it difficult for patrolling security officers to patrol the perimeter at these points. In all cases these issues were resolved and have not jeopardised the integrity of the equipment or patrol routes in any way.

Other obstacles included the topography of the area and some of the terrain had to be levelled and cleared to enable the installation to proceed. Monkeys, which are prevalent in the area, also provided a challenge in so far as they would sit on the perimeter camera housings causing the camera’s viewing arc to be changed. In some cases, metal spikes had to be installed on these cameras to stop this from happening.

Changing weather patterns also proved to be a problem and increased lightning activity in the area had to be taken into consideration after severe lightning strikes had damaged some electrical equipment. Increased lightning protection had to be added to protect against this.

On completion of the project, Enforce Security Services believes that the objectives set out at inception were met and that the installation standards required were achieved and exceeded. The result is a functional, effective and high quality security system has been installed and is being managed and utilised to full effect to protect the residents and their property.

The rate of change in technology is very high and if one lesson can be learned from this project it is that controllers and security personnel in key positions in this type of environment must undergo extensive and ongoing training to understand processes, cope with change and use the systems in place to their full capacity to ensure full value is obtained.

For more information contact Enforce, +27 (0)31 573 7600, info@enforce.co.za.
Is your water meter online?

Need better water management, there’s a device for that.

Is your water meter online?
VixNet Africa has launched a new way for estates to keep tabs on its residents’ and common property water usage. Connecting to current manual water meters, VixNet’s Water Meter Interface Unit (named Manzi), electronically reads water usage, on up to two water meters, and sends the information back to a central server every 24 hours, allowing for accurate, up-to-date billing and consumption reports.

According to VixNet’s Clinton Lemmer, Manzi reads water consumption on meters fitted with pulse outputs, such as magnetic reed switches. The Manzi counts the pulses, which are then converted by the back-end software into cubic metres for billing purposes. The device is powered by a replaceable battery which should last for at least five years under normal usage.

The pulse count values are saved in the onboard memory every hour, and the totals are transmitted once a day to keep battery drain to a minimum. Any unsuccessful transmission is retried at the next scheduled transmission.

The system works on VixNet’s Direct Sequence Spread Spectrum (DSSS) network, which is up and running in Gauteng and Cape Town. This is the same network VixNet uses to monitor alarms and transmit signals to guarding control rooms (www.securitysa.com/7715r). Using DSSS allows signals to be transmitted through normal obstacles, especially devices in awkward areas of transmission. In addition, VixNet’s DSSS network allows for bi-directional communications via the appropriate monitoring software.

Detection of excessive flow outside set parameters can activate the Manzi device to transmit this ‘alarm’ for action to be taken. The Manzi also has a tamper facility in case unauthorised access is gained to where the Manzi unit is installed.

Remote water control
On the back end, VixNet offers a management interface for estates which will allow estate managers to access the water usage from every meter whenever required. Moreover, the back-end functionality with Vixnet’s available incoming data can analyse for leaks due to pressure and or maintenance.

For example, Lemmer says water usage is normally limited between midnight and 3am. Through intelligent head end analysis trends in wasted water can be logged indicating possible leaks, especially during this period as usage is low and pressure is high. This will allow estates to find areas where there may be leaks without digging up pipes and ensuring a plumber is called only when they know there is a problem. Another cost saving feature is the ability to accurately measure water consumption without sending people to read each individual meter.

The system is easy to install, and it starts its work as soon as the batteries are inserted. Twenty-four hours later the first report will be transmitted (as long as the installation is within VixNet’s coverage area). The system has already been installed at numerous private and commercial installations successfully.

Manzi features
• Long range communication capabilities.
• No need for expensive concentrators.
• Licenced ICASA frequency and not in the unlisensed band.
• Secure and jam-resistant communication technology.
• Excellent signal penetration through urban obstacles.
• No SIM cards required.
• Adding in the meters specific pulse per litre in the head end, displays the litres used per hour.
• Tamper switch provides a signal when the meter casing is opened.
• Positioning of Manzi devices are possible via triangulation.
• No ICASA licence required by the end user.
• Self- powered using a replaceable battery pack.
• Low battery alarm.
• Programmable pipe burst alarm parameters.

For more information, contact VixNet Africa, +27 (0)11 100 1969, clintonl@vixnet.co.za, www.vixnet.co.za.
INTERNET OF THINGS

Keeping abreast of current trends is a critical element in the sustainability of any organisation. Comb Communications cut its teeth in the residential estate market as a pioneer in the adoption of GSM technology linked into the Internet. Numerous successful access control installations in a wide variety of estates throughout the country and abroad have provided the company with a vast footprint of residential customers eager to enhance their security.

While the term Internet of Things (IoT) was first mentioned in mainstream publications like *The Guardian*, *Scientific American* and the *Boston Globe* in 2003, the concept was actually born between 2008 and 2009 at the point in time when more ‘things’ or ‘objects’ were connected to the Internet than people (according to the Cisco Internet Business Solutions Group). IoT however did not become common until 2015 and has since accelerated at a rapid rate.

Comb Communications has taken its recognised hardware offerings and evolved each product line to encompass this growing trend that sees increasing focus on software development as well as Internet-based management solutions.

“Our customers are technologically savvy and all have a common goal in mind – controlling and monitoring access into residential or business estates in a safe and secure manner, while providing the highest levels of convenience for its users. By implementing strategic design changes, our product portfolio now includes a carefully orchestrated combination of standard and bespoke hardware elements integrated with a considered software offering in order to provide a holistic access and control solution,” says Comb Communications founder and CEO, Graham Wild.

**Portal to convenience**

Forming the hub of communications with Comb’s access control hardware, Comb Portal – an online integrated web platform – provides Comb’s customers with a secure means of managing access into their estates. Wild explains that the platform has a number of features that are geared around equipping estate managers with the tools to control the access environment.

When combined with Combware – Comb’s hardware offering – Comb Portal allows the user to register, add and invite users, as well as change their details in a simple and quick manner. It also provides a health check on devices, to ensure that uptime of the system’s components are maximised. Documents can be easily managed on Comb Portal and users are provided with a comprehensive selection of reports that include system usage, billing details and informative statistics. Portal also allows the user to undertake pro forma invoicing, linking/unlinking/deleting of connected devices, and access allocation management.

**Talk to me**

The new Comb intercom allows interaction with estate security personnel in an easy and hassle-free manner. The modular unit has a backlit keypad to ensure maximised visibility and is equipped with tamper detection to ensure that unauthorised users are unable to override the security system. The Comb intercom has built-in reset to ensure continued use even in inclement conditions.

Users are provided with peace of mind by using either the guard call or emergency call features of the intercom, ensuring that aid is simply a button push away. In addition, it has full integration with Comb’s keypad for seamless guest access and control.

The standalone Comb keypad is available in three different colour LED options. Ethernet and RS 485 communication protocols provide flexibility and a weatherproof housing ensures that the unit remains operable during the harshest environmental conditions. Operating on a 12 V DC input, on a single relay, the keypad provides consistent reliability over extended periods of time.

Comb is constantly updating and integrating with an array of third-party ware, including but not limited to biometrics, number plate scanners, CCTV, alarms and gate motors to ensure estate ecosystems are controlled and access is managed from a single point with Comb Portal.

For more information, contact Comb Communications, +27(0) 11 089 5800, info@comb-communications.com, www.comb-communications.com.
Apartment video intercom

As modern society develops, residents are looking for more advanced features in their intercom systems. However, old apartment buildings often do not have data network wiring in place to install an IP-based intercom system. The cost associated with rewiring has become a barrier in many intercom system upgrade projects. The Dahua 2-Wire Apartment Video Intercom System provides a cost-effective, fast, simple, and convenient way to upgrade analogue intercom systems.

Features

Simple wiring: The VTNS1006A-2 switch and the VTH5222CH indoor unit use a two-wire interface. The switch is connected to the indoor unit using any two wires, which are used for signal transmission and power. There is no polarity and the switch has a network interface to connect with external networks and communicate with IP devices. The maximum supported distance between the switch and the device is 100 metres, while the maximum supported distance between switches is 30 metres.

Large estates: With the VTO1210C-X large apartment outdoor station, each unit can support a maximum of 20 outdoor stations and 1000 indoor monitors. Each switch can support a maximum of six indoor monitors and only two series connections are needed between switches. The maximum number of switch connections is 30 and can satisfy the requirements for high-rise apartments.

Answer anywhere: Each household can install a maximum of five VTH5222CH indoor monitors which can be used for group calls, and calls can be answered anywhere within the household; within the household, users may communicate with each other through the indoor monitors.

Smart PSS management: SmartPSS is software that can be downloaded from the official website. It is convenient and facilitates smart management of entire areas.

Digital PIR detector

The BMD500 series of detection devices readies a security system for the unexpected by providing protection for every room, corner and corridor. The detector features intelligent signal analysis for reliable detection, pet immunity up to 25 kg and a slim design that complements any décor.

Advanced ASIC-based processing provides detection and false alarm rejection to help keep people and possessions secure. Quad Linear Imaging Technology provides sharp analysis of body dimensions and differentiation from backgrounds and pets.

Effective motion detection is dependent on a sensor’s ability to identify intruders and provide true false alarm resistance. The LC series of detection devices pinpoints intruders through digital signal processing. Digital information is more accurately analysed using software and is not subject to signal degradation caused by amplification, noise, distortion or signal clipping.

Once the detector is installed at the recommended height, installers simply conduct a brief walk-test, to make any necessary adjustments, and the unit is ready to perform. LEDs can be viewed at a glance and help the installer identify the detection range from any distance or angle within the coverage pattern.

The detection range of the motion detector is adjustable to about 3 m to 12 m. A potentiometer can be adjusted clockwise or counter-clockwise to increase or decrease the range respectively. For optimum performance, range should be adjusted so that it effectively protects the dimensions of the intended area. The LC-100-PI is factory-set for 84%.

When choosing a location for the detector, be sure to consider the following:

• Do not aim the detector at reflective surfaces.
• Avoid locations that are subject to direct high air flow.
• Do not locate the detector in the path of direct or reflected sunlight.
• Do not place next to large obstructions that may limit the coverage area.

For more information contact Provident Technologies, +27 (0)82 4451 541, info@providenttech.co.za, www.providenttech.co.za.
**Video entry system**

The IP360 video entry system enables the integration of audio and video intercom, CCTV and home automation, with the possibility to use standard communication devices such as SIP handsets or tablets, smart phones or PCs. The system gives freedom from worrying about distances, cables and the number of devices to be included.

It is possible to monitor the video entry system at any time, from anywhere, via the Internet. A smartphone can be used to receive audio/video calls from the entry panel, open the gate or view CCTV feeds remotely, simply by downloading the XIP Mobile app.

At the core of this technology is Came Connect, a cloud service which is extended to all gate and door automation of the Came Group. This fully integrated platform allows complete control for the user and an easy maintenance tool for the installation company. The set-up is done in two simple steps.

For more information, contact Came BPT South Africa, +27 (0)11 616 3222, info@camebpt.co.za, www.camebpt.co.za.

---

**ViRDI fortifies visitor management**

Visitors have historically been a major security risk for residential estates. The ability to manage their access and egress has been a difficult and costly task until now.

ViRDI’s visitor-oriented solutions including Mobile Key and Visitor Register, which are available from Regal Distributors, makes it possible to issue and manage secure temporary access tokens to visitors or contractors in addition to scanning South African identity documents and vehicle licence discs.

The management and issuing of the secure tokens with a full audit trail of the visitor’s entry, exit, time, date and access points is accomplished with ViRDI’s UNIS 4.0 Security Management Software.

Gone are the days of the unsecure One Time PIN and tedious, manual visitor log books.

For more information contact Regal Distributors, +27 (0) 87 802 3800, info@regalsecurity.co.za, www.regalsecurity.co.za

---

**Gate Manager for visitors**

Easy Systems and Taggit SA have developed an easy-to-use, client-branded and customisable web and mobile application to manage visitors to companies, business parks and estates.

By now, we have all spent time filling in our details in those books passed through our vehicle windows, trying to fit our details into a space that is never big enough. It just doesn’t make sense. And while there are some scan-in systems available in this space, the Gate Manager solution has been developed to allow for easy operation by the guards, providing accurate and timely information for the clients and at an attractive price point.

**Features:**

- System administration set-up.
- Ideal for single-occupant site, multi-occupant site or residential estates.
- Configure multiple-contact persons per business.
- Configure regular visitors authorisation for immediate access.
- Customisable guard checklists to confirm the correct procedures are being followed.
- Driver’s licence and vehicle licence scanning capability.
- Image capture capability.
- Visitor information captured on screen.
- On-screen display of terms and conditions of entry with on-screen signature of acceptance.
- Configure SMS alerts to hosts on arrival.

- Custom reports of visitors and duration on site.
- Accurate data of who is on site at all times.
- POPI compliant.
- Customisable reports.
- Includes an IP68 all weather smartphone device with 13 MP camera, WIFI and 3G connectivity.

For more information, contact Taggit SA, +27 (0)31 560 0101, craig@taggitsa.co.za.
Perimeter challenges with CCTV

Effectively securing perimeters visually versus remaining in budget has always been a challenge. Risk and security managers have a challenge with the solutions, and security operators have to monitor a few cameras at one time and still miss most intrusions unless they are monitoring the camera when and where it is taking place.

For the past few years, various brands and types of video analytics have been available, and in conjunction with thermal imaging have made it possible to go from 25 m between cameras to up to 1 km per camera with cost-efficient thermal cameras. The problem with this is that the video analytics only function properly at a fraction of the distance, so we still rely on the operator to monitor most of the time.

We now have a more cost efficient and effective visual solution with accurate and advanced self-learning video analytics that function at 250 m, even in total darkness.

The operator now simply needs to watch a blank screen and focus on cameras and alerts that pop up, and escalate if he does not act. At the same time, the client has high quality video recordings that can be used as evidence and can be easily monitored from various locations without wasting bandwidth, and without requiring expensive networks thanks to Avigilon’s patented High Definition Stream Management (HDSM).

The system can be configured to ignore guards on patrol, or give the operator the opportunity to also monitor that the guards are on their patrols and receive alerts if the guard loiters in an area for too long.

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

Stafix Electric Fence and Security Centres, the South African distributors of the JVA Security electric fence range of energisers and monitoring systems, is now also providing users with the latest JVA Perimeter Patrol software packages for standalone and piggyback electric security fences.

Starting with the JVA Mimic Perimeter Patrol panel, a plug-in-and-play package that interfaces with an existing JVA network system and gives a geographical layout on a single screen, to the JVA Perimeter Patrol advanced which adds PC connectivity, TCP/IP communications, SQL database and client/server options, these products provide solutions for virtually all challenges.

JVA also provides a High Level Integration Program (HLI) which, in conjunction with a JVA GSM communicator, allows users to take control of multiple Perimeter Patrol sites from virtually anywhere around the world. The HLI system allows one to customise, monitor and control JVA security electric fence systems from within one’s own environment, the software connecting to the JVA Perimeter Patrol over an encrypted TCP/IP connection.

All systems are capable of customised event logging making it also a valuable tool for monitoring security guards vigilance, alarm conditions, the voltage status of the fence lines, the battery condition status, gates, Roboguards, and any other devices that may be included in the system and which need attention.

For further information on this monitoring system visit www.jvasecurity.co.za.
Two-way radio is here to stay

By Brett van den Bosch.

In today’s world of nearly ubiquitous cellular coverage and smartphones that can transmit voice, data, images and video with ease, it is only reasonable to question the relevance of that old stalwart, the two-way radio. According to local specialist, Global Communications, two-way radios are still the choice of first responders such as the police, ambulance services and fire brigades, and that won’t be changing any time soon.

One of the main reasons for this preference is that these applications communicate primarily by means of voice, and whereas cellular devices are geared more for one-to-one communication, two-way radios can broadcast to large groups of up to 1000 users. And although two-way radios have been around for decades, the technology powering them hasn’t stood still. Analogue technology has been surpassed by digital advances that produce better audio clarity, especially in fringe areas of coverage, and extended range that can be up to 12% better than analogue.

Ongoing data and cellular costs run the risk of getting out of hand, and cellular connections are not always as reliable as a dedicated radio network since they are at the mercy of a service provider – a dropped call during an emergency could prove disastrous. While the initial cost of a digital radio is more expensive when compared to analogue, once the device is acquired it can be used without limitations with no further costs. As the industry continues to migrate to digital radios, they have become more affordable and should continue to do so as analogue is further phased out. It is worth noting that most two-way radio manufacturers are withdrawing legacy analogue technology which is now being superseded by digital.

Modern digital radios have some other tricks up their sleeves too, such as GPS tracking which has become a staple for portable and mobile users. This allows small businesses, for example, to track their members on a regular desktop computer – a feature that’s invaluable in the security industry.

All communication can also be recorded for reference and later reviewed and audited, and is admissible in a court of law. Kenwood has taken this one step further and added a SD card to its NX-5000 series of radios, allowing the device to record all conversations as well as save its GPS coordinates. This is very useful in situations where operators in mission critical environments are separated from the device and the organisation wants to review the last location and conversation, much like a black box in an aircraft. Short data messaging is also invaluable, along with status messaging for those who don’t like to type. Encryption is standard with digital devices, which prevents casual eavesdropping.

TDMA (DMR) and FDMA (NXDN) have emerged as the de facto standard protocols for digital radio. TDMA (time division multiple access) boasts two time slots in a 12.5 kHz carrier wave, which allows two separate groups to operate in an analogue carrier wave. This gives the advantage of doubling up on the number of users on a community repeater. FDMA (frequency division multiple access) is unaffected by time and thus provides better communication range.

The ideal protocol depends on the specific application, and the decision-making criteria sometimes have the unfortunate effect of making users reluctant to move into the digital realm. To overcome this, Kenwood builds portables and mobiles that support both formats in one device, in the form of the NX-3000 series. This device can also transmit pre-recorded audio files and transmit at the push of a button. This functionality can, for example, be beneficial in the case of a pensioner with a heart condition. Should they experience any difficulty, they could press a predetermined button on a portable which would send a pre-recorded emergency audio message of their identity, address and information on allergies to any types of medication. This can also be done via a preset data message and sent simultaneously to a control room.

Global Communications has had success with the South African National Defence Force (SANDF) with the same product which is now available to the consumer, regardless of the size of their organisation.

For more information contact Global Communications,
+27 (0)12 621 0400, info@globalcomms.co.za, www.globalcomms.co.za.
Forensic WDR technology

Axis Communications has introduced Forensic WDR, an enhanced Wide Dynamic Range (WDR) method that focuses on achieving high forensic value, in a number of new cameras. WDR is the term commonly used for the art of balancing both very dark and very bright areas in a scene. It is also known as HDR (High Dynamic Range).

In the surveillance industry, the aim is to capture the forensic details at all times. Until now, the WDR methods on the market have not been able to add sufficient forensic value to ultra-high resolution cameras or surveillance scenes that feature a significant amount of movement. In launching its Forensic WDR, Axis has addressed both issues in several new cameras.

“Current WDR methods on the market struggle to capture the forensic details needed, especially in challenging scenes with a great deal of movement and where high resolution is needed,” explained Johan Paulsson, CTO at Axis Communications. “With Forensic WDR, the benefits of WDR can be realised even in such scenarios.”

“Forensic WDR pushes the borders and even allows for multi-megapixel cameras to reveal the details in scenes with difficult light conditions,” added Petra Bennermark, global product manager, Axis Communications. “With our new wide range of fixed domes offering from 5 megapixel resolution up to 4K, we make this technology available for both customers with limited means and for applications exposed to the harshest conditions.”

The new AXIS P32 models offer cost-efficient cameras that require a minimum of effort to install. These fixed domes deliver outstanding video performance with multi-megapixel resolution in full frame rate up to 4K, featuring Forensic WDR, OptimisedIR and Zipstream.

The new AXIS Q35 cameras offer a comprehensive feature set, including power redundancy. Electronic image stabilisation and the IK10+ rating that makes them ideal for harsh environments. They address the need for monitoring in multi-megapixel detail at full frame rate, including Forensic WDR, Lightfinder, OptimisedIR and Zipstream.

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

it all comes together … in the …

CONTROL ROOM

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

Integrated surveillance solutions

IndigoVisions’ products all work together to provide a high level of security in residential estates through its end-to-end security management solution, from cameras to software to storage. Indigo Vision offers IP surveillance solutions and the intelligent BX camera range.

With BX cameras, you get connectivity and flexibility, combined with HD or 4K video, audio and analytics to create the most effective security solution for your needs. With the GX camera range, you get more camera than you bargained for, and lastly, an Ultra camera range that uses SMART.core technology that has Activity Controlled Framerate which offers you up to 90% savings on storage costs.

IndigoVision’s enterprise recording solutions and open platform video management systems are there to achieve the best results for residential estate security. IndigoVision products integrate seamlessly with MASS video analytics, which indicates everything from intrusion detection, average speed exceeding or below a defined threshold, LPR for vehicle licence plates for access control management, to stationary vehicles within virtual areas for longer than a defined time. Everything is integrated into and managed by the IndigoVision Control Centre.

For more information contact Management and Supply of Security Solutions (MASS), +27 (0)12 142 0000, info@mass-solutions.co.za, www.Mass-solutions.co.za.

Your safety in sight

The Active Eye wireless IP camera system does not require a professional to install it, or a large capital spend to acquire it. Depending on your specific requirements, a Wi-Fi IP camera set includes a minimum of four and a maximum of eight high-definition wireless cameras and a wireless NVR. The advanced wireless design of the system and pre-configured cameras make this a true plug-and-play system.

In the case of a home or office, the cameras can be placed up to 300 metres from the NVR. Since every camera acts as a repeater, you can place a camera up to one kilometre from the NVR, thereby catering for a vast range of property sizes.

The system is controlled via a free smartphone application. The simple, user-friendly application transforms your smartphone into a monitoring centre. Alarms and parameters can be set on the NVR in such a way that a signal or notification is sent to your smartphone in the event of breach of a parameter. You will be able to visit the footage at the time of the alarm to determine what triggered the breach, and take the appropriate action if necessary.

You can also rewind, pause and fast-forward footage, and download it the form of video clips or screen-shots. By being alerted to a potential security breach in real-time, you are equipping yourself to respond swiftly to threats against property and life.

The wireless IP camera system is available on various rental and purchase options.

For more information, contact Active Eye, +27 (0)11 058 1049, info@activeeye.co.za.

Integration and communication are essential

Integration and communication are two essential features when considering security systems and access control in a residential environment for both the security and convenience of residents. There are a few questions which need to be answered when investigating this field.

• What access control measures are in place and how integrated are they with CCTV and the intercom facilities?
• What features are available to allow the resident to monitor the situation from a remote location, using modern devices like laptops, tablets or smartphones?
• And if they are available, how complicated are they to implement and to maintain?

The answer to these and many other security-related questions is in technology that allows for the complete control and communication to, from and between different devices and systems from a web application. Connection is the key word and the Came Group has developed Came Connect. The benefits for the user and the installer are significant. Here are some examples of what is possible.

For the end user
• Status of the installations.

For the installer
• A dedicated installer interface to view installations.
• Map location of installations.
• After a support request from an end user, the installer will be able to access the end user interface with all the same functionalities.
• Remote assistance.
• Schedule of maintenance activities.

For more information, contact Came BPT South Africa, +27 (0)11 616 3222, info@camebpt.co.za, www.camebpt.co.za.
**OnGuard Mobi**

Innovation is what keeps security companies everywhere ahead of criminals. First, it was the walkie-talkie and then the more advanced push to talk technology. Today it is all about the adaptation of existing digital technology to suit the security industry and improve the services provided to clients.

Blending innovation and technology, OnGuard Mobi is the next step in tour guard technology that can assist any security company in improving its patrol services. The product is a security guard patrol system that is designed to be built into a touch screen mobile phone. The device eliminates the need to have paperwork while it also makes the collection of data a tamper-proof process.

With its smartphone technology, these systems are designed to provide real-time communication between the guard and the security company, ensuring that the company is always aware of the patrol route the guard is taking while knowing they can easily get in touch with the tour guard on duty.

One of the most important features of OnGuard Mobi is that it improves the reaction times when an incident occurs. As it also improves accountability and reporting, it becomes the ideal security system to have. With this device, guards can produce highly accurate records of incidents and they can use the device to take photographs which can be included in such reports.

**Features of OnGuard Mobi**
- Bluetooth Technology.
- Automatic connectivity.
- Hidden checkpoints.
- Access control: OnGuard Mobi has built-in access control system capability. With this system, there will be more control over who will enter the property.

OnGuard Mobi can be paired with numerous operating systems by using a QR code and the system can be used along with existing security patrol systems. Using a variety of security options, along with OnGuard Mobi, can improve the services that you are providing for your clients.

For more information contact OnGuard , +27 (0)21 701 7777, richard@onguard.co.za, www.onguard.co.za.

---

**Outdoor access terminals**

Many residential estates need rugged, dust and weather-proof devices that offer exceptional durability in extreme conditions.

Suprema offers seven access control terminals that are suitable for outdoor use, namely BioStation 2, BioLite Net, BioLite Solo, BioEntry W2 and BioEntry Plus – which provide card, PIN and finger authentication and Xpass and Xpass S2, which operate with card only. These devices feature IP65-rated protection, meticulous sealing, and extra protective engineering. The BioEntry W2 also offers IK-08 vandal resistance.

A large number of users are supported, with a maximum of 500 000 on some of the devices, with no additional licences. BioStation 2 and BioEntry W2 are fitted with Suprema’s next generation optical sensor, which captures and processes much clearer fingerprint images under less-than-ideal conditions. The new sensor offers excellent wet and dry fingerprint capture performance, allowing these devices to be used even in harsh environments. The W2 achieves matching speeds of 150 000 matches per second, offering high-speed authentication in even the largest estate.

Xpass S2 operates in extreme cold temperatures as well as extremely hot environments (operational temperature -35°C to 65°C). The S2 features innovative multi-smartcard support, allowing it to read multiple card formats from Mifare, DesFire, ISO 14443A, ISO 15693, to Felica.

Suprema devices host a number of different communication interfaces providing higher flexibility and multiple installation options. They are easy to install and easy to operate.

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

**Face recognition for access**

Recently launched, FaceStation 2 brings fast, accurate hands-free access control to the luxury high-rise apartment market. It offers a massive memory capacity and can accommodate up to 30 000 users, 50 000 face image logs and 5 000 000 text logs making it ideal for any site, large or small.

FaceStation 2 can recognise a face even in an environment with 25 000 lux, which is equivalent to full daylight (not direct sunlight). This allows for indoor installations at locations near windows, lobbies and building entries. FaceStation 2 performs equally well in total darkness.

Enhanced security is provided through Live Face Detection: IR-based image analysis to prevent spoofing by printed images and LCDs, enhanced security by Android 5.0 Lollipop and high quality image logging.

Ergonomically designed, the angle and position of the cameras on FaceStation 2 ensures that even tall users are comfortable using the device and an optional tilt-bracket can be used to accommodate wheel-chaired persons and children. FaceStation 2 can work as a video intercom, eliminating the need to install a separate intercom system, giving residents control over their visitors.

The device makes use of multi-band RF reading technology and supports the latest RFID standards. FaceStation 2 now also boasts mobile credentials, using NFC or Bluetooth Low Energy. This means that smart cards can now be loaded to any new generation mobile phone supporting NFC or BLE, totally eliminating cards where multi-factor authentication is required.

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

**Integrated access control**

Ideal for securing residential estates, Suprema’s access control platform is intelligent, fast, accurate and easy to use – efficiently controlling access for residents, visitors, domestic and facility workers as well as contractors.

Suprema’s range of access devices can be installed in a variety of environments, from outdoor installations to luxury high-rise apartments. Suprema’s product range provides a rich range of features to choose from, such as PoE, Live Finger Detection, vandal resistance and ingress protection, as well as various authentication options, including face, finger, PIN and card. BioStar2, Suprema’s access control platform offers a cloud-enabled mobile access control application with real-time reporting, alarm notifications, remote access and monitoring.

Alternatively, Suprema is integrated into more than 25 access control platforms, many that directly address the residential security vertical, such as Gallagher, Honeywell ProWatch, Avigilon, Paxton and many more. BioStar 2 now also boasts mobile credentials for its new terminals, using NFC or Bluetooth Low Energy. This means that smart cards can now be loaded to any new generation mobile phone supporting NFC or BLE, totally eliminating cards where multi-factor authentication is required.

Further, Suprema integrates into popular VMS platforms such as Milestone, NX Witness, Arteco, Cathexis Vision, Hikvision and Indigo Vision. These integrations bring to the table integrated number plate recognition for multi-factor access control, efficient visitor access and vehicle black listing. It also adds forensic intelligence to video by linking video to access events with an undisputable video trail.

Suprema hardware also allows for external intrusion and perimeter security input signals, feeding it into the access control and video management platforms, allowing for a unified view of security for estates or personal residences.

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

**Smart video servers**

Regal offers two video management servers from Hikvision, namely the Blazer Pro all-in-one server and the Blazer Express intelligent VMS station.

The Blazer Pro Series combines a powerful VMS with storage capabilities for 128 or 256 network cameras. VMS add-ons include licence plate recognition, POS integration, business intelligence, GIS mapping and access control management. Blazer Pro is an all-in-one server that provides storage and advanced centralised video management.

The Blazer Express is a 16 or 32 channel intelligent video management platform combined with preinstalled operating system and VMS software. Blazer Express allows for the connection of multiple Blazer Express stations at remote sites with the use of the Blazer Express Client to offer centralised management.

For more information, contact Regal Distributors, +27 (0)87 802 3800, hikvision@regalsecurity.co.za, www.regalsecurity.co.za.
Directory of estate security products and service providers

**Disclaimer:** The information in this publication is furnished for the exclusive use of subscribers and is based on the most reliable data available to Technews Publishing. However, the information was obtained from sources which Technews Publishing does not control and, although every effort has been made to verify it, the data is volatile. In furnishing this information, Technews Publishing in no way assumes any part of the users' or suppliers' risks, does not guarantee its completeness, timeliness or accuracy and shall not be liable for any loss or injury whatever resulting from the use of or reliance on the information, or from negligence.

**AcoustAlert**
Manufacturer
Distributor

**Contact:** Cliff Rose  
**Tel:** +27 (0)83 456 9542  
info@acoustalert.com  
www.acoustalert.com  
**Branches:** Port Elizabeth, Johannesburg  
**Distributors/resellers:** Modular Communications, Stafix Security, all leading perimeter security companies

AcoustAlert is an advanced acoustic Perimeter Intrusion Detection System (PIDS). Up to 2 x 300 metres of sensor cable can be attached to the perimeter fence fabric, which is connected to the field processor which effectively analyses the connected cable for fence disturbances. The field processor can be integrated to 3rd party systems directly or using the SDK soft interface for management and security systems.

**Active Eye**
Wireless

**Installer**  
**Distributor/supplier**  
**Service provider**

**Contact:** Chantal Lubbe  
**Tel:** +27 (0)11 058 1049  
info@activeeye.co.za  
www.activeeye.co.za  
**Branches:** Nationwide

Active Eye supplies plug-and-play wireless IP camera systems with HD resolution. The system can be controlled, footage can be viewed, and alarms can be received, in real-time via your smartphone. An extremely competitive and affordable solution for home or office, with no hidden maintenance costs or fees.

**Adamastor Consulting**

**Service provider**

**Contact:** Rob Anderson  
**Tel:** 086 099 5269  
info@adamastor.co.za  
www.adamastor.co.za  
**Branches:** Durban, Ballito

Adamastor Consulting provides consulting services for security and electrical engineering.

**Avigilon**
Manufacturer

**Contact:** Charntel Loftus  
**Tel:** 080 099 0920 / +27 (0)79 079 6528  
charntel.loftus@avigilon.com  
www.avigilon.com  
**Branches:** Gauteng and surrounds, Cape Town, KwaZulu-Natal, sub-Saharan Africa  
**Distributors:** Rediton, VCAM Sakasa Security Distributors

Avigilon provides trusted security solutions to the global market. Avigilon designs, develops and manufactures video analytics, network video management software and hardware, surveillance cameras, and access control solutions. Its solutions have been installed at thousands of customer sites, including school campuses, transportation systems, healthcare centres, public venues, critical infrastructure, prisons, factories, casinos, airports, financial institutions, government facilities and retailers.

**Axis Communications SA**
Manufacturer

**Contact:** Roy Alves  
**Tel:** +27 (0)11 548 6780  
roya@axis.com  
www.axis.com  
**Branches:** Cape Town, Durban  
**Distributors/resellers:** ADI Global Distribution, Pinnacle, Duxbury Networking

Axis Communications’ perimeter protection solutions are the ideal fit for securing a residential estate. Its thermal cameras with built-in video analytics software can ‘see’ in complete darkness and provide automatic alerts when a person enters a predefined area within the camera’s field of view. This makes it possible to acknowledge suspect activity already before intrusion, and to visually verify what’s going on before taking relevant action.

**Betafence South Africa**
Manufacturer
Distributor/supplier

**Contact:** Dan Edwards  
**Tel:** +27 (0)21 868 7300  
info@betafence.co.za  
www.betafence.co.za  
**Branches:** Paarl, Midrand  
**Distributors/resellers:** Conrite Walls, Impi Wire, Clinton van Dyk Technologies

Betafence is a global leader in perimeter security solutions. Its fences have been trusted for over 135 years to secure what matters. 100% of Betafence products are manufactured in South Africa and tailored to meet the needs of South Africa.
BetaTrac Telematic Solutions
Service provider

Contact: Keith Lawrence
Tel: +27 (0)11 782 5335
keith.lawrence@betastrac.com
www.betastrac.com

Supplier to the security guarding industry of AIMSS (Analytical Intelligent Mobile Security Systems), a powerful management tool offering auto daily autonomous guard reporting, detailed reporting, weekly and monthly performance reports with charts. The system provides a unique playback breadcrumb trail including speed and non movement by bar graph. Ideal for incident follow-through and the improvement of services rendered.

BioMaster
Manufacturer
Distributor/supplier
Service provider

Contact: Bradley Cabral
Tel: 0861000228
sales@biomaster.co.za
www.biomaster.co.za

BioMaster is a provider of revolutionary IP-based access control, identity management and biometric matching technology. Its product range is an advanced suite of innovative products, with a common theme of identity management. BioMaster’s solutions are comprehensive, and include important access control features such as LPR, OHS training platform, visitor management, mobile clocking, staff information storage, criminal and identity checking, and much more.

Blacklight Integrated
Installer/system integrator
Service provider

Contact: Kelly McIntock
Tel: +27 (0)11 026 7582
kelly@blacklightconsulting.co.za
www.blacklightconsulting.co.za

Blacklight Integrated specialises in systems design, sales, installation, offline monitoring and maintenance of IP surveillance, access systems, boom, turnstiles, fencing, networking and integrated systems, as well as Internet of Things (IoT) and IT security.

Boomgate Systems
Manufacturer

Contact: Andre Rossouw
Tel: +27 (0)11 674 4441
boomgate@global.co.za
www.boomgatesystems.co.za

Branches: Cape Town
Distributors/resellers: Domestic and export network.
Contact for more info.

Boomgate Systems is a manufacturer of vehicle and pedestrian access control equipment and high security anti-terror equipment. Its range of products includes traffic barriers, billboard advertising barriers, spike barriers, turnstiles, revolving doors, speedstiles, road blockers, mantrap cubicles, reusable rubber traffic islands, bollards (hydraulic and static), anti bandit doors and cantilever gates.

CAME BPT South Africa
Distributor/supplier

Contact: Riccardo Battaini
Tel: +27 (0)11 616 3222
info@camebpt.co.za
www.camebpt.co.za

Branches: Johannesburg, Pretoria, Durban, Cape Town
Distributors/resellers: Contact company for details

CAME BPT South Africa is a subsidiary of CAME Group which incorporates companies like CAME, BPT, Urbaco, Parkare and GO. A wide range of access control technologies are available: gate and door automation, parking systems, turnstiles, access control systems, audio and video intercoms, CCTV and automatic bollards.

Cathexis Technologies
Manufacturer/Vendor

Contact: Ross Joughin
Tel: +27 (0)31 240 0800
rossj@catafrica.co.za
http://cathexisvideo.com

Distributors/resellers: Cathexis Africa, Compass Security

Cathexis is a leading video management software developer, specialising in surveillance solutions for the international market. Through its flagship product, CathexisVision, Cathexis has demonstrated how the intelligent use of surveillance software can go beyond security management - as a comprehensive business intelligence tool to enhance operational efficiencies.

Clearline Protection Systems
Manufacturer
Distributor/supplier

Contact: Vernon Kyzer
Tel: +27 (0)11 848 1100
vernon@clearline.co.za
www.clearline.co.za

Branches: Johannesburg
Distributors/resellers: Regal Security, MIRO Distribution, Nashua, Netfusion-Botswana, PABX, Infinitron, Bytes Technology, Telkom

Clearline Protection Systems specialises in the design, manufacturing and sale of lightning and surge protection products. Its product range includes Powerline Series, Data Series, Telecoms Series, CCTV and Security Series.

ClickOn Communications
Manufacturer
Installer/system integrator
Service provider

Contact: Mark Watt
Tel: +27 (0)12 803 6783
mark@clickon.co.za
www.clickon.co.za

Branches: Pretoria

ClickOn Communications specialises in the design and implementation of electronic visitor and resident access control solutions including integrated dialling systems, card and biometric solutions, driver and vehicle licence scanners, cloud based access control portal and reporting facilities, bulk email and SMS communication, visitor preclearance access codes, and rental and maintenance services.
From pioneering the use of groundbreaking technology in the market to a track record spanning over ten years and more than a million gate openings daily, Comb Communications provides smart access and control solutions through current technologies and web-based applications, with the backing of a design focused development house.

DEHN Africa offers a broad range of systems, products and services in the surge protection, lightning protection and earthing as well as safety equipment sectors. DEHN Africa reliably protects persons, buildings and systems as well as electrical and electronic devices from the potentially devastating effects of lightning and surges.

Doculam is a South African company, based in KwaZulu-Natal, which has serviced the identification, security and safety sectors through its national footprint for the past 38 years. The company continues to grow its network of customers and distribution partners throughout southern and central Africa. It offers both local and imported products to its target market and prides itself on its technical backup and after sales service.

Elf Rentals started in 1995 as a specialist security provider of full maintenance operating leases of electric fences, CCTV, access control and related power supply and network equipment. The offering includes a 24-hour service solution with a guarantee on all equipment and insurance cover for the duration of the agreement.
Forbatt SA
Manufacturer
Distributor/supplier

Contact: Gino
Tel: +27 (0)11 469 3598
sales@forbatt.co
www.forbatt.co

Distributors: ADI, Elvey, TPA Security Distributors, Communica, Rull Technologies, VCAM, Pentagon, Eurobyte, Pinnacle

Forbatt SA is the sole agent for a range of energy products, video surveillance technology, security peripherals and home automation, and imports exclusively from its network of distributors.

FSK Electronics SA
Manufacturer
Distributor/supplier

Contact: Natasha Loubser
Tel: +27 (0)11 477 2600
sales@fsk.co.za
www.fsk.co.za

Branches: Johannesburg, Cape Town, Durban, Port Elizabeth

Distributors/resellers: All security monitoring companies

FSK Electronics SA designs, develops and manufactures a wide variety of innovative wireless security solutions. These include alarm communicators, guard monitoring and alert systems, alarm panels and remote control devices - all designed to keep you safer and provide you with peace of mind.

G4S Secure Solutions
Installer/System integrator

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

Branches: Centurion, Boksburg, Witbank, Port Elizabeth, Cape Town, Durban, Klerksdorp, Bloemfontein

Distributors/resellers: Access and Beyond

G4S understands the 'secure village' concept of residential estate protection, resulting in an exclusive blueprint for estate protection. The company offers a range of integrated secure solutions to protect you and those dearest to you. Services include manned security services, secure monitoring and response, electronic specialised solutions and risk consultancy.

Gallagher
Distributor/supplier

Contact: Morne Grobler
Tel: +27 (0)79 494 9147
morne.grobler@gallagher.com
https://security.gallagher.com/
Branches: Johannesburg

Distributors/resellers: Contact company for a list of accredited and certified channel partners

Organisations face complex security challenges and business risks. Understanding these challenges and responding with innovative solutions is the cornerstone of what Gallagher does. Gallagher creates and delivers integrated security solutions to meet the varying needs of customers, from basic access control, to critical sites with some of today’s highest security requirements.

Gatebook
Distributor/supplier

Contact: Dave Rampersad
Tel: +27 (0)71 887 3619
dave@snipr.co.za
www.gatebook.co.za, www.snipr.co.za

Branches: Durban, Johannesburg

Distributors/resellers: JKS Security

The Gatebook visitor management solution keeps control of visitors, contractors etc., and reports in real-time. Its easy-to-use mobile app, scanning devices and cloud based platform make the system very intuitive for security personnel. SNIPR is a national database of suspicious vehicles, which can be loaded on an LPR camera or the Gatebook scanner.

GIS-SA
Manufacturer

Contact: Roston Sadie
Tel: +27 (0)71 560 4151
roston@gis-sa.net
www.gis-sa.net

GIS-SA offers custom perimeter lighting solutions to residential estates, encompassing both infrared and white light. Its lights are highly directional to offer enhanced privacy to residents, and their long range provides savings on installation and integration.

IACT-Africa
Service provider

Contact: John Cato
Tel: +27 (0)10 500 1038
johnc@iact-africa.com
www.popisolutions.co.za

Branches: Johannesburg as well as agents in Cape Town and Port Elizabeth

IACT-Africa offers a unique and comprehensive set of PoPI Act-related products and services designed to enable organisations to prepare for compliance with the Act. It also offers cinformation security products and services to complement these, and has experience in assisting residential estates in these areas through implementation projects.

Identiscan
Installer/system integrator
Distributor/supplier
Service provider

Contact: Jamie Bell
Tel: +27 (0)21 701 7777
jamie@onguard.co.za
www.onguard.co.za

Branches: Johannesburg, Pretoria, Durban, Cape Town

Distributors/resellers: Elvey

With the implementation and roll out of the Protection of Personal Information (PoPI) Act, paper based access control registers are no longer compliant and will soon become obsolete. Identiscan has developed a modern solution for its replacement called Identiscan, a handheld mobile data terminal effective in scanning both motor vehicle and driver’s licences.
Impro Technologies
Manufacturer
Contact: Mike Kidson
Tel: +27 (0)11 469 5568
info@impro.net
www.impro.net
Branches: Johannesburg, Durban
Distributors/resellers: Access & Beyond, Elvey, Powell Tronics

Impro Technologies specialises in an array of access control solutions for residential estates. The company offers off-the-shelf solutions that can be tailored to specific needs with seamless integration including mobile offerings, long range readers, biometrics and more.

MASS Solutions
Distributor/supplier
Contact: Ettiene Swanepoel
Tel: +27 (0)82 552 4339
info@mass-solutions.co.za
www.mass-solutions.co.za

MASS Solutions provides a highly professional, functional and reliable security solution through a combination of over 60 years experience, expertise and knowledge, coupled with a superior product range and mastery of unusual challenges in a highly competent matter. The company is directly involved in every stage of the projects for managed and integrated security systems.

MiRO Distribution
Distributor/supplier
Contact: MIRO Sales
Tel: +27 (0)12 657 0960
sales@miro.co.za
www.miro.co.za
Branches: Johannesburg, Cape Town, Durban, Nelspruit

MiRO is a leading supplier of best-of-breed IP convergence products and services to the ICT and security market. MiRO can assist with planning, training and supply of the latest in IP surveillance, wireless access control, biometrics, network infrastructure and wireless connectivity technologies.

Ndlovu Fencing t/a Stafix Electric Fence and Security Centre
Manufacturer
Distributor/supplier
Contact: Shaun Williamson
Tel: +27 (0)11 397 3507
shaun@stafix.co.za
www.stafix.co.za
Branches: Extensive branch network throughout SA

Ndlovu Fencing is the sole southern African distributor of various ranges of electric fence energisers and accessories, CCTV cameras, wireless beam systems as well as automatic gates and access control systems. All systems are COC and LOA approved.

Nemtek
Manufacturer
Distributor/supplier
Contact: Ray Wilsenach
Tel: +27 (0)11 462 8283/4
ray@nemtek.co.za
www.nemtek.com
Branches: Randburg, Edenvale, Cape Town, Port Elizabeth, Pinetown, Nelspruit

Nemtek is a manufacturer and distributor of a high quality, comprehensive range of electric fencing products, offering a full spectrum of energizers and fencing products for industrial, commercial and residential applications.

Powell Tronics
Manufacturer (software developer)
Distributor/supplier
Contact: Mike Austen
Tel: +27 (0)21 448 0156
marketing@powelltronics.com
www.p-tron.com
Branches: Cape Town, Johannesburg, Durban, Port Elizabeth

Powell Tronics is the industry’s chosen distributor for market-leading, innovative, access control related technologies. The company provides access to leading access control brands, and combined with its vastly experienced development team and regional support teams, has the ability to implement and scale these solutions within any business environment.

Oberthur Technologies (OT) and Safran Identity & Security (Morpho) are joining forces to create a world leader in digital security and identification technologies with the ambition to empower citizens and consumers alike to interact, pay, connect, commute, travel and even vote safely in ways that are now possible in a connected world.
Progroup
Manufacturer
Installer/system integrator

Contact: Angelique Roos
Tel: +27 (0)11 493 1545
angelique@progroup.co.za
www.progroup.co.za

Progroup manufactures and sells custom-designed control and security room consoles, specialised desks and interior fittings. The company also provides an installation service for control and security consoles and interior fittings.

Progroup Manufacturing
Manufacturer
Installer/system integrator

Regal Distributors SA
Distributor/supplier

Contact: Regal Distributors SA
Tel: +27 (0)87 802 3800
info@regalsecurity.co.za
www.regalsecurity.co.za

Branches: Johannesburg, Pretoria, Cape Town, Bellville, East London, Port Elizabeth, Durban, Pinetown, Vanderbijlpark, Nelspruit, Witbank, Polokwane, Bloemfontein

Distributor of electronic security equipment from leading international brands including Hikvision, Planet, Utepo, Wisnetworks, DMP, Crow, Securi-Prod, Paxton, ZKTeco and VRDI plus many other popular local brands. Regal Distributors SA is a one stop security shop, nationwide.

Provident Technologies
Distributor/supplier

Contact: Frank Fowles
Tel: +27 (0)82 445 1541
frank@providenttech.co.za
www.providenttech.co.za

Branches: Pretoria, Johannesburg, Cape Town

The name Provident has been synonymous with security for several decades, having been founded by Geoffrey Fowles, an ex Spitfire pilot from World War 2. His son Frank and grandson Luke proudly represent the Provident brand with the integrity of its original founder. Today Provident represents leading brands, distributing products in South Africa and exporting to African countries.

Provident Technologies
Distributor/supplier

Radio Data Communications
Manufacturer & service provider

Contact: Gert Venter
Tel: +27 (0)11 452 1471/2
sales@radiodata.co.za
www.radiodata.co.za

Branches: Edenvale. Representatives in Cape Town and Durban.

Distributors: Eley, IDS – Inhep Digital Security, Nemtek, Platico (Cape Town), SecuLogix (Nairobi), TPA Security Distributors

Established in 1978, Radio Data Communications has supplied over 1,5 million VHF transmitter units and has over 400 radio networks located in South Africa and around the world. GSM and SMS based systems for alarm communication are available, offering expanded features and coverage for alarm communication. In keeping with the focus on personal service, RDC offers a number of value added services including 24 hour, 365 days a year technical support.

Radio Data Communications
Manufacturer & service provider

Reditron
Distributor/supplier

Contact: Jacques Bester
Tel: +27 (0)87 802 2288
jacques@reditron.co.za
www.reditron.co.za

Branches: Cape Town, Durban, Port Elizabeth, Nelspruit

Distributors: Regal Exports

Reditron’s range of CCTV surveillance solutions includes thermal perimeter cameras with human target recognition products. It also offers access control solutions which include fingerprint access terminal products with high capacity and fake finger detection.

Reditron
Distributor/supplier

Risk Diversion
Distributor/supplier

Contact: Peter Fryer
Tel: +27 (0)12 941 9202
hello@riskdiversion.com
www.riskdiversion.co.za

Branches: Pretoria

Risk Diversion proudly distributes internationally recognised Axon Technologies products. The company provides the latest products such as Taser X2 and body worn cameras to law enforcement and the security industries. Taser devices are safe and effective, and can reduce injury to an officer or suspect. Axon Body 2 can record and stream unlimited HD on-officer video with enhanced security features.

Risk Diversion
Distributor/supplier

Secusystems
Installer/system integrator

Contact: Charles Harrison
Tel: +27 (0)11 794 8330
charles@secusystems.co.za
www.secusystems.co.za

Branches: Johannesburg

Secusystems is a security technology company focusing on high value strategic sectors where security technology is of paramount importance. Being hardware agnostic, the company will design an effective solution that meets your requirements. Combining Flir thermal technology with movement target indicators, solutions provide situational awareness up to 20 km radius.

Secusystems
Installer/system integrator

SAIDSA
(South African Intruder Detection Services Association)
Employer organisation

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

SAIDSA is the representative employer body for the electronic security industry, encompassing service providers of basic alarms to sophisticated electronic intruder detection systems and CCTV, and incorporating signal monitoring as well as the provision of armed reaction services.

SAIDSA
(South African Intruder Detection Services Association)
Employer organisation

Secusystems
Installer/system integrator

SAIDSA
(South African Intruder Detection Services Association)
Employer organisation

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

SAIDSA is the representative employer body for the electronic security industry, encompassing service providers of basic alarms to sophisticated electronic intruder detection systems and CCTV, and incorporating signal monitoring as well as the provision of armed reaction services.

SAIDSA
(South African Intruder Detection Services Association)
Employer organisation

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

SAIDSA is the representative employer body for the electronic security industry, encompassing service providers of basic alarms to sophisticated electronic intruder detection systems and CCTV, and incorporating signal monitoring as well as the provision of armed reaction services.
Stallion Reaction
Service provider

Contact: Bevan Herwill
Tel: +27 (0)11 533 8888
bevanh@stallion.co.za
www.stallion.co.za
Branches: Johannesburg, Durban, Port Elizabeth, Cape Town, Bloemfontein, Kimberley, Pretoria, Witbank, Vaal Triangle, North West

Stallion Reaction is a holistic service provider with an impeccable track record and a brand within the top five companies in the industry. Incorporating estates, complexes, churches and residential homes, the company’s focus remains on improving its client security benefits and it is one of the select few security companies which is able to finance electronic security and therefore provide solutions for enhanced residential security.

Suprema
Manufacturer
Distributor/supplier

Contact: Chris Lelicanin
Tel: +27 (0)11 784 3952
enquiry@suprema.co.za
www.suprema.co.za
Branches: Johannesburg
Distributors/resellers: Network across Africa. Contact company for details.

Suprema supplies some of the world’s best matching performance access terminals and software, suitable for residential estates and exclusive homes, and distributed through its trusted partner channel. Leading edge APIs, device SDKs and development support allow for easy integration into existing or new access platforms. SA-based training, device repair and support enable superior service.

Syscontrol Secure
Installer/System integrator
Service provider

Contact: Rudolph Nothling
Tel: 086 111 4453
info@syscontrol.co.za
www.syscontrol.co.za
Branches: Johannesburg

Syscontrol Secure supplies, installs and maintains most CCTV, thermal imaging camera, access control, intruder detection, electrical fencing and access automation system brands. It also offers off-site CCTV monitoring services, LPR street surveillance solutions, estate visitor management systems and physical guarding services.

Thorburn Security Solutions
Service provider

Contact: Julie Redman
Tel: +27 (0)21 880 0015
jredman@thorburn.co.za
www.thorburn.co.za
Branches: Extensive national footprint

Thorburn Security Solutions specialises in estate security, with the majority of its estate clientele classified as top 5-star establishments. Its ability to assess risk, evaluate safeguards, design and provide holistic and integrated solutions puts us at the forefront of this industry sector. The company is a Level 1 B-BBEE contributor, wholly owned by the Tsebo Solutions Group.

Zhejiang Dahua Technology
Manufacturer

Contact: Zhejiang Dahua Technology
Tel: +86 571 8768 8883
dahua.saiglobal.dahuatech.com
www.dahuasecurity.com
Branches: Johannesburg
Distributors/resellers: Elvey, IDS, Redtriton, Security & Communication Warehouse

Zhejiang Dahua Technology is a leading product and solution provider in the global video surveillance industry. With more than 10 000 employees all over the world, Dahua solutions, products and services are used in over 160 countries and regions.

ZKTeco South Africa
Manufacturer

Contact: Hendrik Combrinck
Tel: +27 (0)12 259 1047
hendrik@zkteco.co.za
www.zkteco.co.za
Distributors/resellers: Regal Distributors, Blue Chip, ERS

ZKTeco is a globally-renowned provider of security, access control and time management solutions. The company controls manufacturing, product design, component assembly, logistics/shipping, research and development – all under one roof. ZKTeco develops biometric technology in the mass commercial market in a cost-effective method to ensure efficient usage of biometric technology and provide effective solutions to help organisations improve management efficiency.

Vixnet Africa
Manufacturer
Distributor/supplier

Contact: Clinton Lemmer
Tel: +27 (0)11 100 1969
clinton@vixnet.co.za
www.vixnet.co.za
Branches: Pretoria, Cape Town
Distributors/resellers: Sabertek, C-Track, Vixnet

Vixnet offers the most cost effective way of switching from old to new security service providers’ offering of offshore alarm monitoring to estate residents. The estate owns the Vixnet radio alarm transmitter and can switch the signal traffic to the new security provider within seconds. Vixnet has also introduced the Manzi water usage transmitter to inform the estate of its daily water consumption.

Xone Integrated Security
Installer/System integrator
Service provider

Contact: Ian Downie
Tel: 0861 65 65 65 / +27 (0)82 906 7600
ian@xone.co.za
www.xone.co.za

Xone specialises in providing turnkey security services to residential estates. These include the construction of control rooms, designing process, provision, maintenance and installation of technology as well as the physical guarding force, control room staffing, management and off-site remote monitoring. The company works on more than half the top estates in the country, and specialises in off-site remote monitoring, thermal installations and video analytics.
Index to advertisers

ActiveEye ................................................................. 47
Axis Communications ............................................. 67
BioMaster ................................................................. 41
Boomgate Systems ...................................................... 75
CAME-BPT South Africa .............................................. 37
CatheXis ................................................................. 55
Clearline ................................................................. 45
Comb Communications .............................................. 43
DEHN Africa ............................................................... 13
Elf Rentals ................................................................. 9
Excellerate Services ..................................................... 3
Forbatt SA ................................................................. OBC
G4S Secure Solutions .................................................. 57
Gallagher ................................................................. 61
Gatebook ................................................................. 59
GIS-SA ................................................................. 11
Hi-Tech Security Solutions ........................................... 108, IBC
Impro Technologies ..................................................... 35
MASS ................................................................. 71
MiRO Distribution ......................................................... 31
Modular Communications (Acoust Alert) ....................... 73
Morpho SA ............................................................... 5
Naxian ................................................................. 33
neoMetrics ................................................................. 29
Nemtek ................................................................. 65
Onguard ................................................................. 39
Powell Tronics ........................................................... 19
Progroup Manufacturing ............................................. 97
RDC ................................................................. 15
Reditron ................................................................. 51
Regal Distributors ....................................................... 83
Stafix ................................................................. 95
Stallion Reaction ......................................................... 79
SecuSystemS ............................................................. 69
Suprema ................................................................. 29
Xone ................................................................. 27
Zhejiang Dahua Technology Co ...................................... IFC
ZKTEco SA ............................................................... 7
The journal for decision makers who solve today's security challenges

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

Available in the following formats

The Print Magazines
Monthly issues: 10 issues from February to November

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

The Hi-Tech Security Solutions website www.securitysa.com
The place where professionals search for products, services and suppliers. With access to every article we have published since 2002, this is the ultimate security reference site.

Contact us to order your free* subscription
(011) 543 5800 or subs@technews.co.za

*The publisher has the right to refuse a free application if the respondent does not qualify in terms of our target audience.
Recognitive IP Video Solutions

enhancing the security & safety of people’s lives and assets