nzSecurity

Magazine

June/July 2012

A Vision of the Future with Hillsec
Merging Security with the IT Department
New Zealand Security Conference

NZ Fire Smokin' Ahead with Technology

Total HD surveillance
Uncompromising vision from Bosch

Integrate

Capture

Export

Analyse

HD

Search

Store

Compress

View

Transmit

Our **complete solution** guarantees the **highest quality HD** performance throughout the **entire surveillance chain** - from scene to screen.

Bosch HD takes image resolution to the next level
The level of detail in Bosch HD images captures extensive information throughout the whole scene. Our HD portfolio offers you a complete solution across the entire surveillance chain - from scene to screen. Every component is designed specifically for HD technology, so you can be sure that 'HD in' equals 'HD out'.

Ask about our Bosch HD product solutions today.

BOSCH
Invented for life

ZoneTechnology
Your Security Supply Partner

Email: sales@zonetechnology.co.nz
Web: www.zonetechnology.co.nz

Auckland
Unit 6, 25 Airborne Road
Albany, Auckland
Ph: 09 415 1500

Wellington
35 Abel Smith Street
Wellington
Ph: 04 803 3110

Christchurch
Ph: 03 365 1050

Hills® Reliance

Hills®
Electronic Security
New Zealand

SECURITY THAT TALKS

VoiceNav *Lite*

Personal voice Guide

ABC **Voice Labelling via Word Library**

Built-In User Manual

Encased in an elegant slim profile design with soft-touch illuminated keys, the Hills VoiceNav Lite uniquely offers a built-in interactive "personal voice guide", which enables users to control their security system with ease through the use of smart voice prompts. Users can also label zones, areas and outputs by voice, using the onboard word library.

Call or visit your local Hillsec branch for more information.

nzSecurity

Cover Photo
The advanced PTZ dome network camera works perfectly under bitter weather conditions on the Wendelstein Mountain, placed 1824 meters high altitude. Credit: Wendelstein Mountain, Germany, Camera: AXIS Q6032-E

CONTENTS

Security

Fire

For a FREE online subscription go to
www.newzealandsecurity.co.nz

Associations

NEW ZEALAND INSTITUTE OF PROFESSIONAL INVESTIGATORS INC.
www.nzipi.org.nz

ASIS INTERNATIONAL
Advancing Security Worldwide™
www.asis.org.nz

MASTER LOCKSMITHS
www.masterlocksmiths.com.au

NEW ZEALAND SECURITY ASSOCIATION
NZSA SECURITY
www.security.org.nz

Are you sure you want to permanently erase these items?

Yes   No

People expect more from technology today — or in other words, less. Less cables, less equipment, less hassle. Why should video surveillance be any different?

AXIS Camera Companion lets you offer cutting-edge network video also to customers with smaller areas to cover — giving them the advanced options they're looking for today. AXIS Camera Companion records all video directly on each camera's SD-card — so no need for DVRs, NVRs, extra cables, or even a computer during operation.

With superb HDTV image quality and remote and mobile live viewing, it's a no-brainer for your customers. And with its easy installation, low maintenance and competitive price, it's a dream come true for you.

AXIS Camera Companion — the easiest way to network video surveillance.

Get the Axis picture. Stay one step ahead.
Visit www.axiscameracompanion.com

HDTV image quality • Direct recording on SD cards (no DVR needed) • Viewing apps for iPhone, iPad and Android • Cameras powered over the network • No PC needed for operation • Free viewing client • Scales easily from 1 to 16 cameras • Encoder support for analog cameras • No single point of failure

AXIS
COMMUNICATIONS

Distributed by: CHANNELTEN
SURVEILLANCE SOLUTIONS   Hills
Electronic Security
New Zealand

A vision of the future

Hills Electronic Security (Hillsec), a division of Hills Holdings of Australia, is one of New Zealand's most successful distributors of CCTV, intrusion detection, access control, IP and fiber optics solutions and equipment. Hillsec has been in the industry for over 10 years where it has been able to truly establish itself over the years in the face of a changing industry and economic environments.

Their extensive range of electronic security products, provides solutions for various applications, ranging from simple domestic alarm systems up to a complex integrated surveillance system and fiber optic networks used in commercial and industrial applications. Furthermore, Hillsec's substantial product range and world-class brands has allowed them to offer customers the latest in the industry's technology – IP CCTV Solutions, intrusion detection and access control.

IP CCTV Solutions

Over the last few years, IP and Network Video has been knocking on our doors and is today regarded to be the future of video surveillance. Thanks to exciting new breakthroughs in technology, IP and Network Video surveillance are being widely applied in the security industry with technology that is more effective than ever before.

The systems are now far more cost-effective, flexible, and simple to operate, making it more accessible and user friendly for operators.

The Hills IP networking product range is one of most comprehensive and advanced in the industry also featuring world-class brands represented include

Panasonic WJ-NV200

DVTel, Panasonic, Axis Communications, Arecont Vision, Pelco, EVOnet and Pacom, to name a few.

"It's very exciting to have so many world class products and brands in this evolving technology. IP technology has advanced so much in the last few years. No doubt as the category and technology continues to develop, as will our product depth and breadth," commented Christchurch Branch Manager, Mike Clark.

One of the most exciting things about IP video surveillance is there's really no limit to the potential of the technology. The High Definition (HD) images that come from IP cameras and NVRs are now the new standard in the industry.

"By using an IP camera with megapixel resolution we get much clearer results with a higher zoom-in capability. In the case of identifying a persons face the megapixel camera will be far more effective as image clarity at close zoom is outstanding, when compared to previous technologies," commented Auckland Branch Manager, Graeme Cullen.

Recently released, the Pacom Network Video Recorder (PNVR) is an integral part of the Pacom IP solution. Available as a 16 or 32 input recorder, the PNVR provides monitoring of video from network cameras, network video encoders and the PDR range of Digital Video Recorders.

Recording of the network devices (cameras, encoders etc) is provided within the PNVR with the ability to show the live and recorded footage of the registered DVR's within the SiRiS Central Management Software. The PNVR is a unique device as it allows users to see the combined IP and Analogue systems as one. Furthermore it is compatible with most of the current H.264 and MPEG4 Pacom DVR's that we range, so where customers have invested in the current analogue technology, they now have the ability to enhance the existing systems by the inclusion of the latest technologies including Megapixel cameras and network recording devices, without the need to remove their existing systems.

The latest version of DVTel's award winning, Latitude NVMS, the Latitude NVMS V6.2 presents a new concept in the Security Video IP industry, allowing customers to use an Android Smartphone as a mobile video camera.

With this technology, users can take advantage of the new high-quality and cost effective consumer-grade devices and use the video capabilities they offer to capture events for evidence, or transmit them to the control room in real time, with the great advantage of being the camera-man who controls the location, the angle and the field of view.

DVTel Latitude NVMS V6.2

While traditional security cameras, in almost any site, are eventually limited in their ability to cover everything, this concept can add a new dimension to the role of video in security systems.

Latitude handles the TruWitness video from Android devices in a similar way to any video from a traditional IP Video edge device. It can record the video and allow users to view live, query for the video, playback from Archive, export and perform almost anything else that is available with traditional video scenes.

Another exciting features of DVTel's Latitude NVMS V6.2, is its new web client.

The new web client is a simple and thin video monitoring application, intended to provide quick and easy access to any user, by simply opening Microsoft Internet Explorer and typing the Latitude web server URL. The web client offers basic functionality and is easy to use. It supports live video monitoring, simple search of recorded video for playback, and PTZ control.

Axis Communications meanwhile have recently released their unique Lightfinder technology. Compared with any analog or network cameras, the Lightfinder technology produces more life-like colours, in low-light conditions.

The advantages of this technology are high light sensitivity, excellent image quality with low noise but a wealth of details, and better colour reproduction in low light. Cameras with the Lightfinder technology also have all the advantages of other network cameras, such as progressive scan.

The Lightfinder technology is featured in Axis' Q16 Series ranges from extended D1 resolution cameras to 1-megapixel Axis Q1604 and AXIS Q1604-E WDR cameras, which also provides HDTV 720p video.

Panasonic's IP Solution, the WJ-NV200K Network video recorder (NVR) is ground breaking in its simplicity to set-up, outstanding in its quality of images and HD Smart in so many ways. With no PC required for set-up, simply follow the setup wizard to get up and running with this great NVR. Connect up to 16 HD Panasonic IP cameras including PTZ's and encoder's via an ethernet switch. Record up to 30ips for all 16 cameras in HD resolution. The WJ-NV200K includes Face detection, built in browser for remote monitoring and downloading.

Intrusion detection

The continuous evolvement of the Hills Reliance suite has provided the product range with the reliability and technological advancements to become one of the most leading and trusted intrusion detection solutions in the security industry.

The newest member of the Reliance suite is the highly anticipated, Hills TouchNav, an intuitive touch screen code pad with an easy-to-use menu, so easy, it doesn't even come with a user manual (although one is available). The TouchNav offers a range of user friendly features including Quick Keys (for arming, stay and status), an in-built message centre and customised naming capabilities – all in a comfortable sized 3.5" colour touch screen.

Not only is the TouchNav user friendly and easy to use, it has the ability to control and expand to 128 zones, 8 areas and 16 outputs with 99 users, satisfying the requirements of most residential and commercial installation.

In keeping with the theme of continuous evolvement, Hills are expected to release the next edition of the TouchNav, called the TouchNav Pro. The TouchNav Pro combines security functionality with advanced features such as intercommunication functionality (between up to 8 TouchNav Pro/VoiceNav code pads) as well as video integration on each unit. The TouchNav Pro's video integration functionality allows users to take advantage of its monitoring capabilities (via a CCTV Camera) and comes supplied with the appropriately BNC connector for quick and easy installation.

With the Hills Reliance TouchNav's, security is just a touch away.

Hills TouchNav

Security Commander™

Access Control

For many years, Interlogix has been leading the way in proven solutions for access control, intrusion detection and video integration in the commercial environment. One of the most recognised and robust integrated security platforms, Challenger™, has now been enhanced with the introduction of a high scalable, user-friendly and feature packed management software called Security Commander™.

Managing your Challenger system with Security Commander has never been more user friendly with a simple-to-use menu system and intuitive control from a graphical map display of your building. Key features of Security Commander include; complete Challenger panel management, alarm monitoring, video management, access control badge/user management with photo ID, system device monitoring, access monitoring and a wide range of reports.

Security Commander is a highly-scalable multi-site application that can support up to 128 Challenger panels, over 6,000 intelligent doors and 32,000 alarm points. One of Security Commander's standout features is its client-server architecture, capable of allowing up to 10 operator workstations to manage the system simultaneously. Multi-site partitioning further enhances Security Commander's ability to manage geographically dispersed sites over an IP network or multiple tenant offices in the same building.

Security Commander is compatible with Windows 7 and is intelligently based on a SQL database, ideal for easy access to raw data for powerful database replication, information exchange and custom reporting. An XML-based API additionally allows integration to third-party HR or payroll systems.

Even more exciting news is Security Commander's video integration capabilities with supported GE/UTC DVR's, allowing Challenger alarms and other events to be linked to video footage for improved operator response and easier post-event investigation.

One key aspect of Security Commander which Interlogix have devoted their focus on is, its ease of use; easy for operators to use, learn and train, easy on your IT department, easy to get information and easy to deploy and configure.

Conclusion

Hillsec continuously aims to provide and educate the NZ security industry with emerging technologies and the latest products and services. This has consequently enhanced the knowledge base of the Hillsec team and as well them being able to provide customers with future-proof solutions in IP CCTV, innovative security systems and advanced access control platforms. Make Hillsec your solutions provider for your next install.

Surveillance cameras run 24x7. Capture it all with

WD reliability.

WD AV storage. The ultimate in reliability for surveillance applications.

Don't depend on anything less than WD's AV-class hard drives — built to thrive in the always-on demanding world of digital video surveillance. These drives are designed to support HD video from up to 12 simultaneous streams. They also minimize frame loss, which can pose a real problem when you use standard desktop drives for surveillance storage. For a solution that's a safe bet 24x7, you can count on WD reliability.

WD AV-Class Hard Drives

P U T   Y O U R   L I F E   O N   I T ®

Track and charge

A new system linking GPS to an online timesheet is helping security and delivery firms save money and work more efficiently

Tracking the whereabouts of vehicles using a GPS transmitter isn't anything new in security circles, but a South Island company has married up the technology with an online timesheet to help business owners calculate vehicle movements more accurately.

Ironclad GPS was launched last year and is led by Frank Ansell. His firm provides business owners with rock solid management of their drivers and vehicles, to take away human error with distance travelled, delivery times and time on-site.

Frank Ansell of Ironclad GPS

"Ironclad GPS offers secure management solutions for vehicle fleet operators," says Frank. "Our systems focus on presenting concise, relevant data via any web browser, it is intuitive and easy to use."

The main features of the Ironclad GPS system include:
• Keeping track of vehicles fitted with a compatible GPS unit by displaying their locations on an online street map
• Generating reports of where a given vehicle has travelled, rather than relying on paper timesheets and driver memory
• The system stores where your vehicles have travelled so you can retrieve the information when you need it
• In case of theft or emergency you can immediately locate your vehicles
• Monitoring and optimised delivery routes to save money on fuel costs
• Receive alerts when your vehicles are due for servicing or new RUC licenses

Ironclad GPS tracking is ideal for tracking any vehicle and transmits data via the cellular network, data is stored on a dedicated internet server.

"When a user accesses their Ironclad user account they can see all the information about the movements of their vehicles in an easy-to-read format," says Frank. "Historical data is stored should clients need to check back at any time in the future."

Frank comes from a background in security dispatch and subsequently worked in the engineering and construction industry.

Ironclad GPS quick facts

Ironclad GPS offers one of the best tracking services in New Zealand and provides customers with the latest tracking technology, which is:
• Easy to use and install
• Easy to access – smartphones, computers, web enabled tablets
• Proven to get results and help businesses improve their efficiency and profitability
• GPS trackers are web-based – no need to install, download or update software
• Ironclad GPS` system stores all your historical data securely, so you can refer to any of your vehicles` fleet records at any time
• Improved scheduling and efficient route planning
• More accurate billing

Keep track of information such as:
• Vehicle location
• Distance travelled
• Speed
• Time spent at locations

The system also uses Geofencing to set up custom locations. See: www.ironcladgps.co.nz

The easy-to-use Ironclad GPS interface

He spotted a need for easy-to-use fleet management systems for companies operating vehicles, and so founded Ironclad GPS Tracking to see what could be done to bring the price of these systems down as well as develop the scope of the service.

"It was very expensive a few years back – but we have come a long way now," says Frank. "What we know is that it is very difficult to have staff, particularly casuals, to keep accurate time sheets. This new GPS system removes that worry for business owners.

"It not only solves a lot of problems, but can also be used to resolve disputes, such as when items were delivered, or who was where, and when. It is all about the time management of staff."

Frank says although businesses benefit with more accurate billing and saving time in handling time sheets, drivers appreciate the convenience too.

"After a long day the last thing drivers and security guards want to do is spend an hour filling out time sheets," says Frank.

"A simple mistake, human error, can cost a firm money in under estimated travel or cause issues with clients when it is over estimated, causing jobs to be charged inconsistently. Ironclad GPS delivers absolute transparency. With our system you don't need to rely on the driver to fill out timesheets."

Even though the tracking devices are concealed in vehicles, Frank already has an eye on the next step – real-time tracking

of people's smartphones (most of which already have GPS trackers built in).

"This idea is still in development," he says. "But that is where I see the whole industry going. Because people already have the phones and it reduces the capital cost of installing GPS units in vehicles. We expect to start launching this type of service within the next 12 months."

Frank says firms of any size can profit from the efficiencies of Ironclad GPS.

"Once the system is set up, including a client's list of their regular customers and their locations, users can download a statement of their vehicle's movements every day, once a week or once a month – to fit in with their billing requirements," he says. "Our clients simply log in to our website to access their data."

The system is also ideal for dispute resolution, should someone say a technician didn't arrive on time, or that three hours' work was claimed for ten minutes on site, then the Ironclad system can provide absolute verification of the facts.

"The system allows our clients to see when vehicles arrived at any address and how long they were there for," says Frank. "It protects everyone.

"And because the software is on the net (cloud computing) rather than on a client's computer, data can be accessed from anywhere – even with a web capable smartphone."

Charges for using the Ironclad GPS system is $30 a month for each vehicle fitted with a compatible GPS unit.

Apart from helping firms calculate vehicle usage correctly, the system also acts as a security measure should a vehicle be stolen.

"If a vehicle has been taken then you can find it almost instantly with our system – you just look it up on the map," says Frank.

"The trackers, which are concealed when we fit them, have a back-up battery installed, so if a thief disconnects a vehicle's main battery then the GPS tracker will continue to send out its location."

Frank says the team at Ironclad GPS is very pleased with the service they offer and are already seeing strong interest, despite the firm being less than six months old.

Ironclad GPS trackers are suitable for almost any motor vehicle

**For more information see
www.ironcladgps.co.nz
Phone: 03 423 1980
Email: Frank@ironcladgps.co.nz**

Interlogix releases the new Truvision range of IP Open Standard products

Interlogix has released the new Truvision IP Open Standard range of products. The range encompasses an extensive range of IP cameras including full body and indoor vandal domes as well as the new TVN 20 Network Video Recorder. TruVision Device Finder software assists in identifying the Truvision IP address and viewed using the TruVision Navigator Viewing Software.

"Interlogix have recognised the markets migration to cost effective IP solutions and have developed a comprehensive range of products that make IP installations a breeze," says Robert McDowell Sales Manager, Surveillance Technologies Ltd.

Truvision IP Open Standard Cameras
The TruVision™ IP and IP Megapixel Open Standards cameras bring state-of-the-art, high-definition pictures to the mass video surveillance market. With a wide variety of camera resolutions ranging from standard resolution through to 5 megapixels, these PoE enabled IP cameras represent a flexible video surveillance

Robert McDowell, Sales Manager, Surveillance Technologies Ltd

device to meet any need. Equipped with advanced technology and signal processing capability, they effectively capture video under challenging conditions.

TruVision cameras utilize H.264 compression technology with dual-streaming capability, making it easy to manage the camera's bandwidth usage. These cameras were designed to adhere to PSIA and ONVIF open communication standards and also support a CGI command set for simple integration into any IP system. Video streams can be set for high and low bandwidth and images can be streamed for live viewing or sent to a designated recording location.

Featuring an integrated browser and available SDHC memory card storage capabilities, TruVision IP and IP Megapixel cameras simplify remote, live monitoring/playback of edge-recorded video and audio. Recording on the memory card provides a level of redundancy in case of unforeseen network disruptions.

Select cameras also feature bi-directional audio and alarm inputs and outputs. Privacy masking conceals sensitive scenes and safeguards confidential areas from being observed during live view and recorded on the video file.

Truvision NVR 20
The TruVision™ NVR 20 (TVN 20) is a network video recorder designed to support video streams from IP video cameras. IP camera support includes resolutions from VGA/4CIF to 5 Megapixel from Interlogix and a range of third party IP camera manufacturers. The NVR 20 also supports the Interlogix UltraView™ Encoder 10 H.264 for integrating existing analogue cameras.

IP Open Standards 5MPX Indoor Vandal Resistant IR Dome

Up to 16 video inputs may be configured and internal hard drive capacity ranging from 2TB-16TB makes the TVN 20 ideal for extended storage or megapixel camera applications. Additionally, hard drives may be configured to provide redundant recording for multiple cameras.

Recording options include Continuous, Motion and Alarm or combined scheduled recording modes. Motion recording utilizes an IP camera's built-in motion detection events. Alarms can be triggered from any of the 16 on-board alarm inputs or from alarm inputs that reside on the IP camera.

Software connectivity allows remote access to the full capabilities of the recorder via Web browser or TruVision Navigator. The TVN 20 is easy to configure through IP device auto-discovery tools, and embedded processor technology allows device administration as a network appliance.

The Truvision IP Open Standards range can be viewed at the Surveillance Technologies Ltd showroom in Albany. Call the office on (09) 448-2366 to arrange a demonstration or visit the website: www.surveillancetechnologies.co.nz.

Security surveillance gets smarter
Merging security with the IT department

The days of the stereotypical 'doughnut eating' security guard blankly watching fuzzy images on a black and white TV screen are gone. New networked digital cameras combined with intelligent video analytics software are changing the nature of surveillance from reactive human-based monitoring and replays of past events, to sophisticated automated threat detection and rapid responses to more quickly identify and act on potential issues. As a result today's CSO and CIO must work closely together, says Scott Basham, Unisys's Asia Pacific Program Manager for Location, Perimeter and Surveillance Security.

New Zealand has come a long way since the first closed circuit television (CCTV) security cameras were installed back in the '80s.

In the thirty years since, those humble analogue installations have transformed into modern high resolution, networked-enabled, digital systems.

As technology has improved, and adoption rates have increased, the costs for modern CCTV systems have been significantly reduced, leading many organisations to deploy more and more cameras. However, adding more cameras is only effective if you can accurately and effectively monitor the images they generate. Just hoping that a security guard will happen to notice a change when an image cycles through a bank of monitors leaves too much to chance.

The advent of digital video cameras has allowed large numbers of high resolution cameras to be networked over existing ethernet networks (rather than expensive coaxial cable networks). When combined with powerful video management systems that incorporate video analytics software, it is possible to automatically detect potential threats in real-time, so that security personnel can take appropriate action as events occur. This transforms security surveillance from being a reactive tool for finding out what happened post incident, into a dynamic and proactive capability for live and real-time threat detection using the surveillance camera feeds.

One of the most interesting outcomes of this transformation is how the increasingly sophisticated security surveillance infrastructure is blurring the line between what was once strictly the domain of a physical protection specialist, but now the realm of IT department. As a result, today's IT and security departments must effectively combine their unique skills and abilities to deliver the security outcomes the organisation seeks to achieve.

An analytical look at today's security requirements and tools

For the last two decades, governments and commercial organisations in New Zealand, and around the world, have used video surveillance as the cornerstone of physical security capabilities.

Whether it was for national security, critical infrastructure protection, securing assets within the finance and banking sector or to protect private property, video surveillance has been universally accepted as the foundation upon which an organisation protected its people, assets and facilities.

Even though the cost of new cameras has decreased, organisations have faced continued pressure to further reduce operating costs. CCTV provides a convenient and efficient solution to manage and protect large areas at all hours, so many organisations have increased the number of cameras deployed but not the number of people monitoring them.

However, more cameras does not necessarily equate to increased security assuredness. The only relevant measure of the organisation's real-time enterprise-wide level of security situational awareness, is the number of constantly monitored feeds. Unobserved camera feeds only provide retrospective information – which helps to identify what happened, but does nothing to help stop an event occurring. What's more, even if someone is monitoring the screens, studies show that a person's ability to constantly monitor a screen rapidly decreases after just 20 minutes.

The solution to this false economy of equating quantity of cameras with quality of security is the advent of Internet Protocol (IP) enabled digital cameras. The video feeds from these cameras can be networked together and combined with video analytics software to automatically identify and respond to potential security threats as they happen.

Video analytics allow organisations to monitor and manage multiple video surveillance cameras by automatically recognising changes in activity on the screen to generate an alert or trigger

a response from the monitoring staff observing the feed, such as automatically locking a door, sounding an alarm or notifying the nearest security officer. This may identify a potential threat before it actually happens.

The action generated by these analytical tools can be as simple as on-screen alerts of suspicious or unwanted behaviours, or as complex as using biometric facial recognition technology to grant or deny a person access to a high security area. They can significantly increase the capabilities of what might otherwise be a very stock standard video surveillance system and turn it into a highly tuned, mission critical component of the organisation's entire operations.

Even the simplest of video analytics implementations can increase an organisation's security. These include motion detection (to notice when a person enters or leaves an area), virtual tripwires (to detect when someone or something enters a secure area), object recognition (which can identify when a particular object is removed or if additional objects appear), and licence plate recognition software to scrutinise cars entering and leaving a facility.

Specialist CCTV analytical tools can help government bodies and commercial groups put their security systems to other uses such as identifying regular patterns in human traffic to reviewing building plans in order to make work or public areas more efficient or safe. The possibilities are limitless.

Video Analytics

Face Matching

In the future, organisations will look to further leverage the capabilities of their CCTV network to incorporate specialist functions such as biometric identification and behaviour pattern recognition. Using facial recognition and gait recognition technologies, it is already possible to match surveillance subjects against a watch list of persons of interest. As these biometric technologies continue to evolve, we are likely to see even greater convergence between surveillance and identification.

Combining Security with IT

The IT department plays a critical role in assisting the CSO to economically and effectively respond to the physical threats and cover the gamut of security challenges faced by today's businesses. Understanding the role of technology, and how to use it most effectively, is now an integral part of managing an effective security surveillance system.

Complex IT skills are needed to support the surveillance systems, ranging from installing new hardware and software, integrating various network components, and managing the deployment of intelligent video analytic tools, through to managing the ever-growing back end server and storage infrastructure that runs and supports all of those edge devices.

Surveillance systems continue to evolve with the advent of new and better devices that are able to be integrated into the organisation's eco-system. As these capabilities grow, so too does the desire of security managers to fuse together all of that data from all of those various devices into a single, common operating picture that can provide them the most efficient and most effective means of monitoring and responding to security incidents and threats as they occur.

In such a mission critical environment as security, the search for innovation is constant. The advent of mobile computing devices, such as tablets and smart phones, enables security professionals to view real-time footage and other sensor information while on the move, releasing them from their desks and getting them out of their control rooms. This allows them to get closer to where the action is happening, which in turn better allows them to understand and respond to the nature of the security threats they face as and when they occur, regardless of where they are physically located, regardless of the time of day.

Scott Basham manages Unisys' location, perimeter and surveillance solution offerings within Asia Pacific. Starting as an officer in the Australian Regular Army more than 20 years ago, he has provided security and technology advice across both the public and private sectors, across a wide range of sectors including aviation, ports, critical infrastructure, border protection and defence.

Panasonic
ideas for life

104- Degree Surveillance with such Compact Size

Discreet D109mm x H47mm housing

Compact Dome Camera

WV-SW155   WV-SW152   WV-SF135   WV-SF132

- 720p HD images up to 30 fps [WV-SW155/WV-SF135]
- Horizontal angular field of view: 104 ° [WV-SW155/WV-SW152/WV-SF135]
- "Railway applications – Electronics equipment used on rolling stock" (EN50155) [WV-SW155/WV-SW152]
- IP66 rated water and dust resistant. (IEC60529) [WV-SW155/WV-SW152]
- Vandal resistant mechanism for high reliability [WV-SW155/WV-SW152]
- ONVIF compliant model

i-PRO SmartHD

Onvif

http://www.panasonic.co.nz

Life`s a breeze with Synology
The IP surveillance management system

Anyone who has moved across to using IP cameras for their surveillance requirements will already know how effective they are, particularly their high-resolution images – video and stills.

Using IP surveillance with Synology NVR is a breeze, all that needs to be done is to plug the camera and the NVR in to the existing network, and follow the instructions on the easy-to-use graphic user interface (GUI) and wizard for set-up.

This NVR is capable of overcoming the problems that traditional analogue systems have in regards to storage capacity, cool running temperature and scalability. It also comes packed with advanced features that are not common in the mainstream analogue systems.

For example, Synology's NAS unit was once used only for the back end storage. Synology was the first in the industry to implement free surveillance management software (Surveillance Station 5) into its entire range of NAS boxes turning them to NVRs.

Storage, of course, can be an issue as the days of using boxes of VHS tapes are long gone. Computer hard drive storage is the solution, but there are limits with older systems. For example to store the footage of four cameras with a resolution of 1.3 mega pixels for 15 days in MJPEG will need 2.5Tb of storage. With limited hard drive bays in older systems, users will quickly run out of space.

Douglas Leung, an account manager IT storage supplier VST says, "In general, traditional analogue systems will use direct attached storage (DAS), network attached storage (NAS) to overcome the limited storage capacity problem or even storage area network (SAN) for some of the higher-end solutions.

"However, adding back-end storage is not always as easy as it first appears, there are lots of factors to consider, such as compatibility.

Having wide experience in back-end storage, Synology is able to solve a lot of the once very difficult tasks that traditional

The most commonly used NVR is the DS412+ shown here

systems struggle with; limited storage space, drive redundancy, overheating, stability and scalability."

In the older systems there is normally a limited hard drive space available in the system, this can make it difficult for a user to add additional storage, let alone hard drive redundancy. Some older systems also rely on a single hard drive for storing video, but if that were to fail – typically without any warning – then the whole system is as good as useless until the drive is replaced with a new one. Even then, all the recorded footage will have been lost if not backed up.

Synology NVR units range from one to 36 hard drive bays and easily solve the storage problem users once faced. They also come with multiple RAID options that offer the user hard drive redundancy. If a single hard drive was to fail, the user will be able to recover their footage from other drives.

49 channel live view under one browser

The DS1512+ has a Hotswap Harddrive tray that makes it easy to add extra storage

Overheating is a common problem with the older analogue systems. As the drives stack up in the unit, so the heat builds up too.

"This adversely affects the life of the hard drives in the system," says Douglas. "Synology NVR units are designed to operate in a multiple hard drive environment with smart fan control that helps maintain a stable temperature in the system and takes the strain off the drives."

Another common problem with analogue systems is stability when under a heavy load. Even if the unit is capable of taking additional hard drives, the power drawn by multiple hard drives will increase the power load on the unit.

"This can lead to the hard drives being unstable and developing bad sectors which then build up to SMART errors and in the long run reliability becomes an issue," says Douglas. "This frequently leads to the drives needing to be swapped out by a technician at the user's cost and because this is a powering issue, it may continue to happen again in future.

"Synology NVR units are designed to have enough power to handle the amount of hard drives in the unit as well as coming with hard drive SMART (health) check.

The user can easily log in to the unit and check the hard drive status and see what is happening with their unit."

Douglas says swapping hard drives is also very easy, simply pull the drives from their hot swap unit and rebuild the RAID.

"This saves a lot of time and money for the user," he says.

Scalability is another problem traditional systems can face, with a PC based surveillance system once the maximum channel limit is reached the user will need to add an additional PCI card for more channels. However, the number of available PCI slots is limited.

With the Synology NVR solution, and depending on which model you have, up to 50 cameras can be attached to a single unit. The user can choose to run these entire 50 cameras on one unit or spread them out on different units and link them all under one management.

If the user has a company with multiple floors and would like to set-up more than 50 cameras, they can assign a unit to each floor, support 50 cameras each and chain all these units together under one management system. Therefore the amount of cameras under one management is theoretically unlimited.

Daisy chaining the units together gives the user the flexibility on storage space and spreads out the cameras to different units to flatten out the resource usage on the unit. It also gives the admin user 'department access control' rights, so that a user or department can have their own individual login to view the cameras they have access to in the system.

Although Synology have the hardware design to carry the large amount of hard drive that is required to deploy a modern IP surveillance solution, choosing the right drives is also important. For all our surveillance customers we suggest using Western Digital Surveillance Hard Drives WD AV-GP, these drives are engineered to thrive in a system that is running 24/7. With the combination

of WD's IntelliSeek, IntelliPower and IntelliPark technologies, WD has reduced the power consumption by up to 40% compared to other drives on the market. WD drives with GreenPower Technology™, consume less power during spin-up and operation, this minimises heat dissipation and vibration and provides the user long term reliability on all their surveillance applications. These drives also come in a 3Tb option allowing the user to record at a high level of clarity and at a broad range of resolutions and also storing the footage for a longer period of time.

As more people are starting to use Smartphone's and tablets, Synology NVR has created its own Smartphone application for Android and iOS devices.

"Again the Synology NVR is designed to allow users to do this without any special modifications or software, it just works," says Douglas.

"This feature enables the user to look at the live feed or recorded video and even control the P/T/Z camera functions via their Android or iOS devices.

"A security guard can use a Smartphone to look around a corner before they get there. Perfect for seeing blind spots and increasing safety. There is no need for a security guard to take a chance and risk an unnecessary or surprise confrontation."

Synology NVR is a solution that alleviates many of the problems that arise with the old analogue systems that are now long past their prime in terms of image quality, the ability to scale up and add more storage capacity.

"An IP solution is more than capable of overcoming the problems that occur with old analogue systems, but many of these are complicated and difficult to set-up and most require a computer IT background to implement," says Douglas.

"A Synology NVR system is a complete all in one IP surveillance solution with enhanced features that are designed to help the user to manage, view, record and handle all their surveillance requirement."

Chief Security Officer
Able to view & Control all 16 Cameras on network

Sales Dept — 4 Cameras
Manager — 4 Cameras
Marketing Dept — 4 Cameras
Warehouse — 4 Cameras

The Synology NVR daisy chain management system

Facts send a clear message

Here are the blunt facts that drive perimeter security in New Zealand. Over 16,000 business and other premises were broken into last year - on average 44 a day. With dwellings added the total climbs to 59,518 offences.

That is a staggering 163 offences per day and the highest number of any recorded crime except theft. As if that was not disturbing enough, the rate of resolving breaking and entering crimes is by far the lowest of any police category, at only 15 percent.

The message is pretty clear – you had best rely on prevention than with detection.

Still, there is some good news. Over the past decade the rate of burglary per head of population has declined by about 13 percent – and for that surely the security industry deserves some of the credit.

It was about 10 years ago that Chris Martin began looking in the New Zealand security industry for an opportunity, going on to start Xpanda Security.

He says at the time electronic security and manned services were well covered, cameras were rapidly developing, but physical security demands were not well catered for.

Chris Martin

Aluminium is too weak for first layer protection

"So I looked at the retractable grille market in South Africa and started bringing in a range of five or six different products and manufacturing custom products here as well," says Martin.

"Imported product off the shelf is very quick to install if people get burgled and they want a solution straight away. But if it is important how it looks and fits into the building, or they want something more niche with different colours, then we manufacture it.

"When I started a lot of people were saying that the products looked like bars in a jail. That thinking has all gone now, today people want strong security, good installation and a finished product that looks good."

Since those early days, the Xpanda product range has expanded to include customised solid steel doors, bars, steel gates, bollards, ram beams – all of which have to be made to size as each building is different.

Martin says the trend these days is for businesses to seek a complete perimeter solution built from a combination of different type products.

"At the front they might want an expanding grille, so it's inviting for the customer during the day, then on some of their side windows they might want fixed bars, then at the back they probably want ram beams with bollards," he says.

"The biggest clients like the electronics and computer retailers tend to bring us in during the store development phase and use the full range of what we recommend. They are probably the ones that get broken into the least, it's a direct inverse correlation to what they put in and for us it is a sign of success.

For example since we've been doing security for one large computer retailer they haven't had a successful break-in although there have been several attempts. Every door is three times protected, so there is

TITAN
TOUGH

The strength of the NUUO Titan is no myth.

Stories have been circulating for thousands of years about the fierce strength of the Titan warrior. Are they true?

Get up close and personal at your nearest Atlas Gentech and find out for yourself.

The NUUO Titan NVR utilises a redefined recording engine named File Ring Technology. File Ring Technology is engineered from scratch to handle high megapixel recordings by changing how hard drives store and retrieve video data. It can process large amount of data throughput boosting Titan's recording performance to 64 2 - Megapixel cameras (H.264, 15 fps, moderate traffic).

For more information on training or demo's call you local branch, email orders@atlasgentech.co.nz or visit us at www.atlasgentech.co.nz

ATLAS GENTECH
DATA | COMMUNICATIONS | SECURITY

NUUO
The Intelligent Surveillance Solution

FREEPHONE 0800 732 637   Auckland (09) 574 2700   Wellington (04) 379 7926   Christchurch (03) 477 9142

Managing Director, Peter Novosad

a very low chance of offenders getting through all three layers of protection."

Martin says he is a big believer in alarms and cameras – on top of good perimeter security.

"Alarms let a monitoring station know there has been a break-in and cameras record who did it, but that doesn't stop them," he says. On a bad Monday morning the company takes about three phone calls reacting to break-ins, despite most clients reporting that they have monitored alarms and security patrols that responded.

"That's when we can step in and help them by providing the first layers of perimeter protection," he says.

Steel only

Managing Director, Peter Novosad, says that the company only uses steel in its products, because the aluminium alternatives are too weak for secure first layer protection.

Steel mesh still intact preventing entry

"The level of the security you have is about how long it takes to get through the security barriers and that comes from a combination of things. It is partly the material that is used, that's why steel is very important, rather than using aluminium.

Then there's installation. We install bars on the inside because on the outside they can hook a vehicle up to them and maybe pull them out, whereas on the inside they have to smash the window and the sensor goes off while they attack the grille.

Then there is the thickness of material. Depending on the risk profile, round the back where nobody is going to see you, we might have 16 or 20 mm steel bars, whereas out the front it might be 12 mm. The welding and framing is important too. We weld every bar in place at every spot because if a bar is not welded in place it can easily be removed once it is cut."

Novosad says the same principle applies with the way grilles are constructed with many aluminium grilles being secured with a few pop rivets instead of welded at every join.

"The quality of the installation and the spacing, quality and size of the fixings, is vital too."

He says monitoring the types of break-ins over the years has led Xpanda Security to develop new products such as ram bars and roller door locks with specially recessed locks that make cutting with a bolt cutter impossible.

"But again quality is important, we use good quality hardened locks, because some cheap locks are insecure imitations," says Peter, producing two identical looking door locks.

"These locks look very similar and people think it's just a lock and the cheap one which maybe made in China will be the same. However one of these locks can be

Insecure pop riveted Aluminium

Welded Steel Mesh

Similar looking locks: one can be opened from the back without a key and one can't

opened from the back without a key and one can't. That's what you are paying for."

Consequences

Martin says its worth doing the job properly because the consequences if you do get broken into are severe and it's not just the value of stolen goods.

"You feel violated and you can't put a price on that," he says. "And even if you don't lose high value stock, the costs are high. I've seen liquor stores get broken into and lose three bottles of whisky, which is say $120, then have to get a police number, wait around without touching anything, replace the broken glass, replace doors and windows and everything else and it all costs much more than the value of the stolen stock."

But physical security is more than just stopping forced entry – Martin says the deterrence factor is also important.

He says US research on commercial break-ins shows that the decision to commit burglaries is premeditated but the decision as to which place to break into tends to be opportunistic, and he believes the same applies here.

"Most offenders are going to drive around and find an easy target. If they are more professional they will wait for a security patrol to go by, then they break in. These days it would be very surprising to find a commercial building that was not alarmed and monitored and they still break-in because they are easy targets and they know that security response takes time," he says.

"Putting grilles and bars on identifies the premises as a hard target and that is the psychology of deterring break-ins – by making offenders not even look at your place."

Now, the future really is wide open.

Introducing iCLASS® SE™, enabled with the Secure Identity Object (SIO) model.

More portable, more flexible, and more secure than ever before. iCLASS® SE™ — the platform that simplifies everything.

HID®

Learn about SIO.
hidglobal.com/sio
or scan this with
a QR reader

iCLASS® SE™ protects the integrity of your identities, regardless of the card platform. It's also amazingly flexible — use multiple form factors with an access control solution to create your ideal product today, then change it down the road as your business needs evolve by simply re-programming it.

Powerful, adaptable and designed to be energy efficient, iCLASS SE is truly the next generation in access control. **For more information, visit hidglobal.com/future-NZSec**

New gate set to secure farms

The kind of heavy duty security taken for granted in urban business yards is now available to farmers, thanks to a new strong remote operation gate specifically designed to bolster security of farms.

These days farms are often substantial agri-businesses with valuable machinery, tools and live-stock which is vulnerable to increasing amounts of theft, but tight security on a farm is often in conflict with the freedom to be able to move to and fro around the farm. While alarms and cameras can help, it is better to keep intruders and unauthorised visitors out in the first place, says Leaweld, the company that designed and manufactures the new gate.

"An ordinary farm gate – even with a padlock – is no deterrent to an intruder with bolt cutters and in any case, it can easily be lifted off its hinges," says Director Darryl Tuck.

When the team at Leaweld uncovered the extent of the problem in rural areas, they set out to solve the problem and the result is a robust, remotely operated security gate to keep unauthorised people and vehicles off the farm and away from the homestead, the yard and implement sheds.

"Farms will always be difficult to secure completely, but if intruders can't drive their vehicles onto the farm, they will go some-where else for easier pickings," says Tuck.

However security gates designed for urban business yards are not useable in locations where connecting to mains power is impractical.

"Our new gate is solar powered, saving the cost and hassle of mains wiring," he says.

"The solar panels charge a heavy duty 24v battery, so that it will perform even on rainy days - essential in winter and if you need more capacity, you can install back up batteries."

Because it is not linked to mains power, and requires no ground track, the entire gate assembly can be relocated if necessary around the farm and double as a remote stock management tool in corporate style farming operations with shared milking sheds or other shared facilities.

The new gate installed at an Matamata organic dairy farm

"Because it doesn't have a ground track, it will operate without problems over rough tracks and gravel," says Tuck. "The rollers have been designed with Nylon encapsulated steel and sealed bearings, so that gravel and stones will not disrupted the mechanism."

Authorised

But busy farms have legitimate visitors, who may arrive when the farmer is elsewhere on the farm and for them the answer lies in the GSM mobile network, explains Leaweld Head Technician, Nelson Harris.

"You and your family would use remote key fobs but for a regular authorised visitor you give them a mobile phone code number to unlock the gate," he says.

The gate can also operate by timer or from a keypad, but GSM technology allows up to 64 authorised mobile phones to operate the gate with SMS texts or free calling with authorised mobile numbers added and removed by SMS text command to the control unit. People who try to use another mobile number to generate the command will be refused entry.

"If you have a one-off contractor, you can talk to them by mobile then release the gate and grant access," says Harris.

This makes the technology also suitable for other applications that require security

clearance before entry but do not have access to mains power, like remote water supply facilities or monitoring stations. Where GSM has low signal strength, an extension antenna can be fitted to the gate.

Variety

Leaweld produces a wide range of security gates and Harris says the focus is on good design and manufacturing.

"For example, the gate can be outfitted with wrought iron options and if the gate is damaged a new standard agricultural gate can be fitted to the frame. We make them strong and reliable and we hot dip galvanise them for maximum corrosion protection.

"But safety is even more important. A lot of gates out there are dangerous and there are several instances of children being killed. Even full size wooden gates are heavy and can crush a child, so we make sure all our gates have stops that prevent them falling out of their tower and we have employed independent risk assessors to evaluate our products.

"I wish I could say the same for the whole industry, but there are gates being installed today – especially heavy duty security gates – that can escape their tower and fall over."

He says the new gate also helps with occupational health and safety compliance by reducing the risks from allowing unauthorised access to sites.

Schlage Technology meets Legge reliability

Schlage's latest range of commercial electronic locks has now expanded with the introduction of the Schlage CO Series with mortice lock.

Launched in 2011, the Schlage CO Series of electronic locks gives you the additional security and convenience of electronic access control without the cost or complexity of a networked solution. The CO100 and CO200 now have the added security of the hugely popular Legge 990 mortice lock.

Especially designed for the needs of the New Zealand market, the Legge 990 mortice lock is one of the most trusted names in the market for security. The new CO Series with mortice lock is easy to retrofit into the existing mortice cut-out of the Legge 990 or other major brands.

Available in keypad, proximity card/ FOB and/or magnetic strip cards, the Schlage CO Series is open platform, providing users with more choices and freedom from proprietary technologies.

They can be used in a variety of applications for convenient offline access control of schools, healthcare facilities, plants, commercial buildings, retail outlets, apartments, and more.

For more information contact Ingersoll Rand on 0800 477 869 or visit www.ingersollrand.co.nz.

Trends 2012: IP Video for All
New tech trends that move the question from "Why IP?" to "Why not?"

by Johan Paulsson, CTO, Axis Communications

The adoption of IP-based surveillance continues to increase annually, capturing market share across virtually all industry segments. The most recent IMS Research forecast indicates that IP video revenue amounts to about 30% of all installations in 2011 and will be more than 50% of the world wide surveillance camera market by 2015. Integrators and consultants, along with security practitioners, have long-since realized that the trend towards IP has by far surpassed the point of being a niche offering. It's moved to the class of required knowledge.

With each passing year, performance improvements of electronics in the IT and consumer worlds enable manufactures to address demands that they couldn't have done with earlier product generations. Looking at trends that shape the physical security world for the year ahead the question remains: What has the market been asking for that we'll finally see in this year?

Clarity: Seeing better than the naked eye

Image usability is the most critical success factor for the security professional who deploys video. It is vital to cameras to provide outstanding image performance and image clarity, even in the most difficult environments.

The defined objective of a surveillance application dictates the quality of the video required. Whereas the conditions or environment it is mounted in dictates the camera type selected. This is surveillance 101 for the integrator and/or consultant.

Recent advances in video processing chips (sometimes referred to as a system-on-chip, SOC) combined with the latest image sensors give security professionals broader product portfolios to choose from. For the past two years, manufacturers have been in a race to deliver the highest resolution cameras. While the chips and processors can render high multi-megapixel images, the lensing marketing is currently topping out at about 5 MP performance, although in reality lenses above 5 MP are rare and difficult to find. Since camera imaging technology must wait for the lens market to catch up, manufacturers will concentrate on products that provide more clarity, specifically in low light scenarios.

The most light sensitive camera on the market is an IP camera delivering colour imagery down to 0.05 lux without the need for auxiliary light. Known as "Lightfinder," this technology will find its way into all types of cameras – from box to dome to PTZ dome – and provide increased resolution enabling colour images in scenes that traditionally only delivered black & white. Adding colour to video shot in virtual darkness only increases the usability of that video, giving the security practitioner enhanced situational awareness. This capability is available in cameras that are outdoor ready, powered by Ethernet, and rated down to -40 F° right out of the box.

Wide dynamic range (WDR) is a feature available in some network cameras that incorporates techniques for handling a wide range of lighting conditions in a scene. WDR enables clear identification of people and objects, even in highly variable lighting conditions.

In a scene with extremely bright and dark areas or in backlight situations where a person is in front of a bright window, a typical camera would produce an image where objects in the dark areas would hardly be visible. Wide dynamic range solves this by applying techniques such as using different exposures for different objects in a scene to enable objects in both bright and dark areas to be visible.
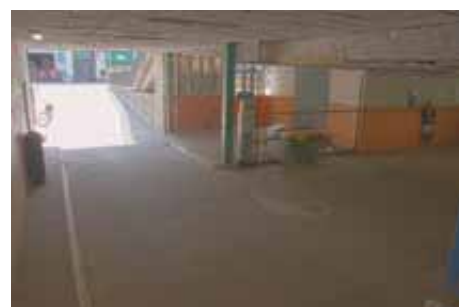
City Library Parking

Too Bright

Too Dark

Additionally, for the past 70 years we have lived with the analog standards of NTSC and PAL. Today, nearly everyone has HDTVs in their homes. HDTV is perfect for surveillance because the SMPTE standard guarantees frame rate, resolution, colour fidelity and aspect ratio. The HDTV might not be standard to last for 70 years, but 15 years from now it's believable that the majority of cameras will be HDTV compliant.

Chips for Analytics: Killer apps are coming

The "killer app" for video surveillance products is the ability to apply rules to a condition and initiate predefined actions as a result. Otherwise known as analytics, applying intelligence to the edge (i.e. in the camera) offers new options for solving some common problems faced by security professionals in basically all industries.

Over a relatively short period of time, humans experience physical fatigue that impacts their effectiveness at monitoring video. Computers, on the other hand, do not have this disadvantage and will continually process events in the manner that they were programmed. The challenge is programming them. With each new advance in processing power brought on by newer generation of in-camera chipsets, capabilities increase, giving us new opportunities to do more at the edge while increasing ease of use.

The power is there today for more on-board analytics, so expect to see software developers leveraging the camera as a platform in the way the iPhone drove the app movement.

Convenience: IP is everywhere

The trend of easy installation products will certainly continue throughout 2012, with surveillance made as convenient as possible through technology innovation and ongoing education in all sectors. The end goal is to decrease the time it takes to physically install devices so more time can be spent on configuration and improved use. Year-by-year we've seen IP video products becoming easier to install and now the industry has its eyes on making them easy to install in any environment.

Out-of-the-box ready products are hitting the market. They can be installed in any temperature, extreme cold, or with active cooling, hot; from -40°F (-40°C) to 165°F (75°C). Ease of installation now allows cameras to be hung and connected in a matter of minutes, installers can focus on more value added configuration practices including image quality settings, which will be the ultimate judge of the system's success.

Educating yourself and/or your staff on camera configuration practices is a wise move. The industry is at the point where the majority of integrators can sell, install and maintain a functioning IP surveillance system with easy to integrate solutions but one major distinguishing factor will be the ability to obtain the best quality image from the camera selected – default settings are not always the best choice.

Convergence: IP isn't all-or-nothing

Despite the many undisputed advantages of network cameras (image quality, scalability, TCO and functionality), analog still has its place at the table in 2012 and will be an uninvited guest for many years to come… for those of us who strongly believe in the IP world, anyway.

Kidding aside, analog cameras still provide a workable solution for certain installations and continue to amount to 70% of new camera installations in 2011, according to IMS Research. But the shift from analog to IP video surveillance continues to accelerate, and that's because the shift isn't an all-or-nothing proposition.

The continued development of video encoder technologies, which act as a bridge between the analog and digital world, enables practitioners to leverage working analog cameras they purchased

and integrate them into the future IP surveillance system. Like the analytics market, encoders too are benefitting from improved chip (SoC) technology.

One of these benefits is the ability to better de-interlace video captured by analog cameras. For example, analog cameras produce video in lines of resolution which are either designated as "even" or "odd." Combined, they produce the entire picture – but there is a 17 millisecond delay between the odd and even lines. When there is movement, the delay creates an interlaced effect that causes degradation in the image quality. De-interlacing reduces this effect and thus provides a clearer image. You're still stuck viewing recordings at NTSC or PAL resolution because of the analog camera, but it won't have the jagged lines associated with interlaced cameras.

Finally, the form factor of encoders is typically identified by two criteria: (1) the number of analog video channels it can convert; and (2) whether it is either standalone or rack mounted. Current offerings start at single channel offerings and go up to enterprise rack mounted solutions that can encode 84 channels of video. Performance enhancements of SoC provide the capability of multi-channel video ports on one chip – the end result is a lower cost per port of video encoders. The world is full of analog cameras and with each performance increase the reality of converting them to a digital solution becomes more affordable.

From the introduction of the first network camera in 1996 and video encoder in 1998, the convergence to digital video surveillance has been driven by value-added, open-source functionalities.

Cloud: Flying high in 2012

The final trend pushing IP surveillance into the realm of small business has been buzzing for the last two years: hosted video. During 2011, major national system integrators including ADT, NAVCO, Niscayah, Siemens and Stanley, launched hosted video applications that offered customers a range of business choices. Now customers can opt to purchase cameras and pay a monthly fee for the off-site storage of recordings. Some companies offer complete turnkey solutions – cameras included – for a monthly fee.

This changes the traditional DVR-based business model of purchasing all the equipment upfront and relying heavily on maintenance and service, which can be cost prohibitive for small businesses. It also offers new avenues for monthly recurring revenue for integrators of all sizes, since some hosting providers offer private labeling of the service, giving qualified companies the opportunity to offer hosted video services under their own brand. Together, edge storage and hosted video might just sing the final swan song for the DVR.

But the hosted video trend is not solely focused on small businesses. For instance, national retailers with a number of dispersed locations might deploy thousands of hosted video channels across their retail operations in malls or shopping centers. They receive the benefits associated with IP video, but aren't purchasing separate storage devices for each location. And for those who do not have the time or resources to monitor all these video channels internally, Central Monitoring Stations will embrace this opportunity as it becomes more widely accepted.

And for those customers who are hesitant to consider hosted video because of the need for high resolution video, the consumer market is playing a major role. Ever-increasing bandwidth pipes from Internet Service Providers will give us more resolution options in the future. In areas where bandwidth is lacking, network attached storage devices – the same ones that consumers use to store backup photo, video and music files – can be used to record multi-Terabytes of higher quality video locally in a cost effective manner.

As technology evolves, so do the expectations for the best results from all surveillance solutions. A network camera provider should embrace these changes and make continual innovation paramount in their surveillance offerings.

IP (really) is for everyone

Technology innovations in network video have made it so IP is for everyone, regardless of the installation size or location. There are so many more storage, installation and functionality options today that it will be hard to turn down an IP system – as long as the end-customer is properly educated on the benefits. Finding a trusted, credible partner to distributors, resellers and system integrators will help decipher what IP system is most suitable to any installation. Use this year to learn all you can about IP. It will be everywhere you look.

GET MORE OUT OF YOUR
INTERCOM

KOCOM

Hills® Electronic Security New Zealand

Kocom KCV-D374SD

| | Multimedia Centre | | CCTV Interface | | On Screen Display (OSD) |

The Kocom KCV-D374SD sets a new benchmark for all communication systems. Together with its optimal intercommunication features, the KCV-D374SD offers more, with a built-in multimedia centre and CCTV interface, allowing users to record and store motion detection videos, as well as, view their favourite photos and listen to music (mp3) directly from a SD card.

Call or visit your local Hillsec branch for more information about this ultimate communication solution.

Hills® Electronic Security New Zealand

www.hillsec.co.nz

Auckland
Unit 1, 30 Greenpark Rd
Penrose Auckland
Ph: 09 525 8007
Fax: 09 525 8009

Wellington
124-128 Hutt Rd
Petone Lower Hutt Wellington
Ph: 04 939 9355
Fax: 04 939 9366

Christchurch
Unit 5, 235 Waltham Rd
Sydenham Christchurch
Ph: 03 374 6277
Fax: 03 374 6287

Beating price objections

So you've created a strategy that is not just about offering the cheapest price, your sales approach focuses on convincing the customer they want your product or service and not just dollars, but when you go to ask for the order, the customer starts looking at the floor and the ceiling - anywhere but in your eye.

After skirting around the subject for a bit, they finally reveal what is bothering them.

"It's too expensive."

If you haven't prepared and practiced for this moment, then all the 'value added' management theory in the world will fly out the window as you try and retrieve the sale. It doesn't matter if you are a sales representative or the CEO negotiating a big contract, the consistency with which you and your colleagues handle price objections has a lot to do with the health of your company's bottom line – it is just simple arithmetic.

Peter Parnham is an Auckland based business mentor and freelance writer

Contact:
peter.parnham@paraphrase.co.nz.

For example, if you sell for $100 something that cost you $80, it doesn't seem like much to give away a mere 5 percent discount, but in truth you are giving away a full 25 percent of your gross profits ($5 out of $20 gross profit).

Price objections are not the only objections you'll encounter, but they seem the easiest to solve - you just drop the price and hey presto, you'll get the sale.

Fortunately, if you understand what is going on, with preparation, training and practice you don't have to erode your own pricing regime every time you close a sale.

The first thing to accept is that a price objection might not be about price at all – it may simply be the easiest way for the client to avoid telling you something you don't want to hear.

For example, if there is something about you or your company the customers doesn't trust, they are pretty unlikely to tell you to your face, because that would be awkward, rude and would invite a confrontation. It is much easier to get rid of you by saying you are too expensive.

Likewise if there is some technical feature they don't believe is worthwhile or some hyped performance figure they don't trust. After all, if they object directly, you might just bamboozle them with facts or numbers – it is much easier just to try and get rid of you with price.

To uncover the real sticking point you need to ask open ended questions – questions that cannot be answered with a conversation stopping 'no.'

It can be as simple as starting with: "What makes you say that?"

This is where the preparation and training comes in, because you need a stock repertoire of open questions and follow ups ready because they are pretty hard to make up on the fly.

When you do ask questions acknowledge the objection rather than dismissing it or arguing with it, however silly it seems. Don't interrupt – listen patiently and carefully to tease out the problem.

If the customer does have a genuine price objection it probably falls into one of a few broad categories.

The first one is a simple push from a customer who wants to buy, but just wants to make sure they are getting your best price. Most customers like to know they have got a special deal, or some sort of bargain, and so it often pays to leave a little wiggle room before you get to your normal price level.

Other objections are based on the customer's own comparisons with other products, and the basic technique is to ask questions that draw the customers' attention your comparative advantages. It is important during this process not to disparage competitor products or services because that makes you seem untrustworthy.

If your customer genuinely can't afford your product or service, it is not worth slicing a few percentage points off your price – the exact price won't make any real difference if they are going to struggle to pay. Refer them to a finance company, or let them go and cause your competitor a money headache.

Of course none of this will succeed if you don't believe in your own mind that the price you charge for your products or services are fair. If you can't convince yourself, you won't convince anyone else.

Look for another job.

But mostly, if you have a reasonable product or service at a reasonable price then sales is about technique and skills that can be learned. Invest in some good sales training that runs role plays. This is vital because lectures and book learning are by themselves not enough, it is practice makes perfect.

For all that, sometimes you will not get customers across the line. This is an opportunity for feedback - but don't just ask bluntly what they didn't like about your offer - they will probably just tell you it was too expensive.

New Zealand Security Conference & Exhibition 2012

The New Zealand Security Conference 2012 is to be held at the Rendezvous Hotel, Auckland on 22nd & 23rd of August. A two day security exhibition will be held alongside the conference. The event is staged by the New Zealand Security Association in association with ASIS.

The conference is the single largest gathering of security professionals in New Zealand, attracting between 180 - 220 delegates and over 140 security organisations coming together in one location.

In addition to this the NZSA will be advertising the event on national radio with over 11,000 commercials airing to a

A great time was had by all at last years conference Awards Dinner

Key Note Speakers

Master of Ceremony
Michele A'Court, Commedian & Writer
Winner of "Female Comedian of the Decade" at the 2010 NZ Comedy Guild Awards, Michele A'Court is a full time professional stand-up comedian and freelance writer.

Michele has a weekly spot reviewing the news on TVNZ's "Good Morning" show; she is a regular guest on TV3's award-winning comedy show, "7 Days;" on Radio NZ National's "The Panel" with Jim Mora; and "9 to Noon" with Kathryn Ryan and Te Radar.

Her international experience as a stand-up comedian includes shows in Edinburgh, Glasgow, Melbourne, Adelaide, Vancouver and NZ. Michele also performed for the international troops in East Timor back in 2001.

Wednesday 22nd 0730
Jane Turner, Economist ASB
Jane joined ASB in 2008 as an Economist. Her role involves monitoring, analysing and forecasting trends in the New Zealand economy, financial markets and monetary policy. Prior to joining ASB, Jane spent 5 years working for the Reserve Bank of New Zealand in Wellington, spending most of this time in the forecasting team as a Senior Economic Analyst.

Session Outline:
Jane will provide an insight into the current economic conditions.

Wednesday 22nd 0930
Graham McGregor,
International Marketing Expert
Graham McGregor is an internationally recognised marketing expert and the creator of "The Unfair Business Report," www.TheUnfairBusinessAdvantage.com which has now been read by business owners in over 27 countries.

This presentation is called: *"How to get an Unfair Sales Advantage in your security business..."*

Session Outline:
• An easy way to turn your best clients into your unpaid sales team.
• Two magic words that will increase your sales and referrals by at least 15% a year.
• A simple technique to make sure your customers, prospects and centre's of influence keep you 'top of mind' at all times.

total audience of over 1.4 million listeners from June to August, which is expected to increase visitor numbers significantly, providing companies with an excellent platform to promote their products and services.

The conference & exhibition will provide information on the latest trends relevant to the security industry and a forum to build networks of security practitioners by interaction with hundreds of executives and decision makers from general industry.

The conference and exhibition will appeal to a wide range of security industry and associated organisations. These include, but are not limited to:
• Security Managers
• Government Security Advisors
• Security Consultants
• Security Trainers
• Risk Managers
• Facility Managers
• Private Investigators
• Security Systems Providers and Installers
• Police
• Insurance Companies
• IT and Intelligence Professionals
• Emergency Managers
• Business Continuity Consultants
• Fire Protection
• Senior Managers from General Industry

Exhibition Opportunities
A wide range of stands are available to the industry and interested parties, (see graph opposite).

Sponsorship Opportunities
Sponsorship opportunities, for the Security Conference 2012, offer a unique and highly valuable opportunity to target security professionals from business and government, they include:

Cocktail Reception Sponsor
The Cocktail evening will commence immediately after the last session of the first day. It will run for two hours and will be held inside the exhibition where guests will be able to view the exhibits.

Lunch Sponsors
This is an opportunity for sponsors to participate in one of the two lunches.

Awards Dinner Sponsor
The Security Industry Awards Dinner is a special and popular event, with many of the industry's leaders attending. Session Sponsor

This is an opportunity for sponsors to participate in the proceedings of one of the sessions. If you wish you can introduce the speaker.

Keynote Speaker Sponsor
This is an opportunity for sponsors to participate in the proceedings by sponsoring one of the Keynote speakers. If you wish you can introduce the speaker.

Conference Floor Plan

Booths 1-26 are 3.0 x 2.4mtrs Unless Otherwise Stated

Booths 27-31 are 3.0 x 1.2mtrs Unless Otherwise Stated
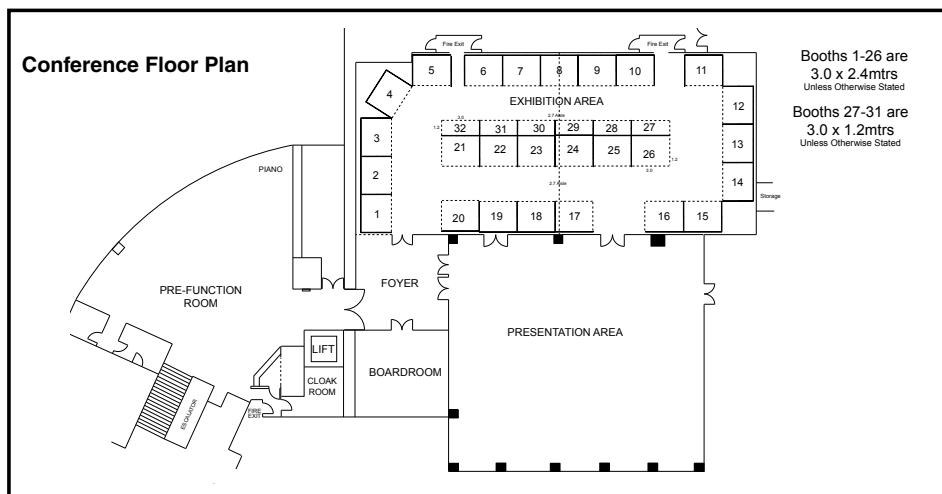
Wednesday 22nd 1100
Bill Butler, Chief Executive SIA
Mr Butler has been Chief Executive of the Security Industry Authority (SIA), the body responsible for the licensing and regulation of the private security industry throughout the UK, since July 2009. He has worked with ministers in the Home Office and key players in the industry to develop the Government's proposals for a new regulatory regime. http://sia.homeoffice.gov.uk/Pages/home.aspx.

Session Outline:
• The original objectives of the SIA and how it has performed, including an assessment of the various roles of fit and proper checks
• The proposed changes to the regime and the move to business licensing.
• SIA's expectations for the new regime, including our approach to customer service.

Wednesday 22nd 1330
Dr Warren Tucker, Director NZ Security Intelligence Service
Dr Tucker was appointed Director of the Government Communications Security Bureau with effect 13 December 1999. He took up the position as Director of Security, New Zealand Security Intelligence Service, on 1 November 2006.

Warren is a founding member and Patron of the New Zealand Institute of Intelligence Professionals (NZIIP) and is Chair of the recently formed Strategic Advisory Board, Centre for Defence and Security Studies, Massey University.

Session Outline:
Dr Tucker will reflect on the changing National Security landscape in New Zealand in his time as Director of the New Zealand Security Intelligence Service.

Wednesday 22nd 1415
Chris Budge, CFE, Forensic Services, KPMG
Chris is the Forensic Technology leader in New Zealand within KPMG's Forensic practice. With over 28 years investigative experience, with the last 12 years focused on technology offending and cybercrime, Chris brings a wealth of experience to the conference.

Chris is a Member of ASIS NZ, ACFE and on the CPPF Committee sponsored by the NZ Police as the ACFE Representative.

Session Outline:
• Trends in both the public and private sector fraud within New Zealand over the last year as compared with the last three years
• Prevention strategies; what is being done? Is it working? Where to next?
• Global trends and where do we fit in the world?

Wednesday 22nd 1530
Steve Mark – Australasian Register of Security Professionals

In January 2010 Steve Mark was appointed Australasian Register of Security Professionals, which was established to set competencies and criteria for the registration of security professionals in Australia and New Zealand. In 2011 Steve Mark was appointed Technical Committee Member to the International Standards for Security Agencies Technical Committee.

Session Outline:
The forced movement of peoples through war, government action, food politics and now climate change presents one of the greatest threats to identity, culture and community. This session will explore the impact of climate change as a result of rising sea levels on vulnerable communities, particularly those located on low lying Pacific islands and in the Asia-Pacific river deltas.

Wednesday 22nd 1615
Tony Ridley
International Security Advisor

Tony Ridley is a leading international business and security expert with specialties in online marketing and business intelligence tools. http://tony-ridley.com

Session Outline:
Business travellers are becoming more aware, even demanding. Technology abounds in the travel management and information space and Security managers are trying to do more with less. This has made the task of travel risk management even more demanding ,but many are still making critical errors or wasting valuable time and money in the wrong areas.
In this session we discover new and effective solutions to solving these problems, developing high-end training and information for travellers on a budget and identify what threats and hazards really await our valuable business travellers.

Thursday 23rd 0900
Professor Grant Schofield
Neuroscience of Leadership

Grant is a Professor of Public Health at AUT University and a consultant in Neuroscience of Leadership. Grant has over a decade's experience in teaching psychology and being involved in elite sport, including representing NZ in triathalons.

Session Outline:
• Demonstrating the latest that neuroscience research has to offer us with regard to how the body and brain interact and function under pressure.
• The single best technique for getting on with others
• The one thing you can start doing immediately that will make you smarter......much smarter!
• A powerful idea about how to live an engaged and meaningful life

Thursday 23rd 0945
Tony Ridley
Social Media Expert

With years of experience in social media and online marketing, Tony helps companies understand the strength, threats and weaknesses of social media.
Using his experience with online marketing, Tony educates and develops companies security, risk, marketing and communications on the benefits of using social media and other online marketing tools and processes.

Session Outline:
• Research
• Management
• Monitoring
• Implementation
• Tips from the professionals

Thursday 23rd 1100
Andy Hays
Interfnational CCTV Specialist

Andy Hays is an international specialist in CCTV systems and was a finalist two years running for UK Security Consultant of the year 2009/2010. He was the keynote speaker at Tourism Safety and Security Summit in India and Tourism security conference in Malaysia, actively promoting CCTV standards and best practice to Asia-Pacific countries.

Session Outline:
• Future technologies that will impact on our industry.
• Demonstrating the results of detailed testing of mega pixel and HD cameras and discuss the potential mistakes and misgiving the new technology may have for the end user.
• CCTV Operational Requirements
• How to draw up operational requirements, use them to evaluate systems and how to test systems to Secure By Design standards.

Thursday 23rd 1330
Laurie Gabites
Regional Director CPTED Association
Laurie is a Regional Advisor for the Safe Communities Foundation of New Zealand (SCFNZ) and a recognised CPTED practitioner. Laurie is also a Trustee and Board Member of the Safe Communities Foundation of New Zealand (SCFNZ) and a New Zealand Delegate on the Pan Pacific Safe Community Network (PPSCN). He is currently the Regional Director of the International CPTED Association (ICA) covering New Zealand, Australia and the South Pacific.

Session Outline:
CPTED is a crime prevention philosophy based on proper design and effective use of the environment, leading to a reduction in the incidence and fear of crime, as well as an improvement in quality of life. This session explores how to design and implement CPTED in today's environment.

ASIS New Zealand 25th Anniversary Seminar

The Security Business: A Management Perspective

ASIS New Zealand celebrates its 25th Anniversary during 2012. As part of our celebrations we will host a special one day Seminar at the InterContinental, Wellington on Thursday 28 June 2012. Register now at www.asis.org.nz/seminar2012.

Connect with your peers from across New Zealand. Share experiences and exchange ideas. Gain valuable new insights and perspectives on security challenges faced within New Zealand, as well as those that extend beyond our shores.

**Eduard J Emde CPP
President,
ASIS International**
Eduard J Emde is the first non-US President of ASIS International. He is the principal consultant for BMKISS Europe, an independent security support organisation based in the Netherlands. He received a master's degree in Organisational Analysis & Behaviour from Lancaster University in the UK and degrees in Business Administration and Dutch Law from Erasmus University Rotterdam. He holds CPP and CISSP certifications.

**Sir William Gallagher
KNZM MBE Hon D
Doing business globally**
Sir William is renowned, recognised and rewarded for his skills as a motivational, pragmatic and hands-on businessman in and outside of the industry in New Zealand and abroad. His reputation both as a dynamic leader and one of NZ's most astute businessmen springs from the way in which he conducts his business – and therefore his working relationships – with customers and staff.

**Dr Warren Tucker
New Zealand's threat environment**
Dr Tucker is the Director, New Zealand Security Intelligence Service. He was educated at Nelson College and the University of Canterbury. He graduated BE (Hons) and PhD (both in Electrical Engineering) in 1973 and 1978 respectively and qualified as a Registered Engineer. Dr Tucker joined the NZ Army (RNZ Sigs) in 1979, retiring in 1982 with the rank of Major. He joined the Government Communications Security Bureau (GCSB) in 1982 and was appointed as its Director in 1999. He took up the position as Director of Security, New Zealand Security Intelligence Service, on 1 November 2006.

**Professor
Stephen Cummings
Creative Strategy**
Stephen Cummings is Head of School and Professor of Strategic Management at Victoria University of Wellington, New Zealand. He also holds visiting or adjunct positions at Warwick Business School, United Kingdom; ENPC, Paris; Ecole Hassania, Casablanca; Stockholm University and Trinity College Dublin. He has twenty years of teaching, executive development and public speaking experience in the UK, New Zealand, Belgium, Morocco, France, Sweden, Ireland, Malaysia and China and is the author of a number of books on strategy. He has given addresses on creative approaches to strategy development for many leading organizations, including Philips, HSBC, The Financial Times, Wellington City Council, GKN Westland, Prudential, Air Services Australia, Petronas, SCION and IRL.

Also presenting will be, Warren Cornor CPP, head of security for Customs New Zealand, Dr Chris Roberts of the Government Communications Security Bureau and Chris Budge CPP of KPMG. Note: speakers are subject to their own operational requirements and may be changed without notice.

**Register now at:
www.asis.org.nz/seminar2012**
A day of high-level security education for only: All prices are exclusive of GST.

Cost:
Member:	$295
Member Early Bird Rate:	$245*
Non-member:	$355
Non-member Early Bird Rate:	$295*

* (if paid before 31st of May)

Win a new iPad
Join ASIS to receive member benefits including the monthly 'Security Management' magazine, a reduced seminar entry fee and, entry into the draw to win a new iPad on the day.

For further information or comment, please contact Carlton Ruffell Chairman of ASIS New Zealand

**Carlton Ruffell CPP
carlton@clruffell.co.nz
Phone: 021952810**

Five ways criminals use facebook

Facebook went public on the 21st May 2012 in one of the most anticipated IPO's in history. With more than 900 million users, Mark Zuckerberg's expanding social media empire has become a part of the online experience.

A by-product of its success is that millions of people around the world are now far more exposed to a number of cybercrimes that result from criminals having access to this media.

The modern Private Investigator needs to be savvy and up to date with the most modern technology to combat this on-going trend involving the cybercriminal.

Cybercrime has been around for a long time but the presence of social media has made many crimes easier to commit. In social networks people often make 'friends' without knowing the person and make their personal information easily available.

None of the networks present more opportunity to criminals than Facebook and its hundreds of millions of users.

Recent studies have identified some of the most common ways criminals use Facebook to their advantage.

1. Hacking accounts

When criminals hack a Facebook account they typically used one of several available 'brute force' tools, which cycle through a common password directory and try commonly used names and dates, opposite hundreds of thousands of different email ID's. Once hacked, an account can be commandeered and then used as a platform to deliver spam, or – more commonly – sold. Clandestine hacker forums are crawling with ads offering Facebook account ID's and passwords in exchange for money. In the cyber world, information is a valuable resource.

2. Commandeering accounts

A more direct form of identity theft, commandeering occurs when the criminal logs onto an existing user account using an illegally obtained ID and password. Once they are online, they have the victim's entire friend list at their disposal and a trusted cyber-identity. The imposter can use this identity for a variety of confidence schemes, such as a popular one that has become known as the London scam in which the fraudster claims to be stranded overseas and in need of money to make it home. This scam has a far higher success rate on Facebook, and specifically of commandeered accounts, because there is a baseline of trust between the users and those on their friends list.

3. Profile cloning

Profile cloning is the act of using unprotected images and information to create a Facebook account with the same name and details of an existing user. The cloner will then send "friend" requests to all of the victim's contacts. These contacts will likely accept the cloner as a friend since the request appears to be from someone they're familiar with. Once accepted the criminal has access to the targets personal information which they can then use to clone other profiles or to commit fraud. By doing this they exploit a person's account and postulate as that person to extract information. The scariest aspect of this offending is its simplicity as hacking acumen is unnecessary to clone the profile; the criminal simply needs a registered account.

4. Fake Facebook

A common form of phishing is the fake Facebook scam. The scammer's direct users via some sort of clickable enticement, to a spurious Facebook log in page designed to look like the real thing. When the victims enter their usernames and passwords, they are collected into a database, which the scammer will often then sell. Once scammers have purchased a user's information they can take advantage of their assumed identity through apps like Facebook Marketplace

Michael Campbell is the Vice Chairman of the NZIPI and he has operated his business as a self-employed Private Investigator in New Zealand for the past 31 years.
www.advancedinvestigations.co.nz

and buy and sell a laundry list of goods and services. Posing as a reputable user lets the scammer capitalise on the trust that person has earned by selling fake goods and services or promoting brands they have been paid to advertise.

5. Mining unprotected information

Few sites provide an easier source of basic information than Facebook. While it is possible to keep all personal information on Facebook private, users frequently reveal their emails, phone numbers, addresses, birth dates and other pieces of private data. As security experts and hackers know, this kind of information if often used as passwords or as answers to secret security questions. While the majority of unprotected information is mined for targeted advertising, it can be a means to a more devious purpose such as profile cloning and ultimately, identity theft.

These are but a few of many examples of computer related crimes the modern investigator needs to be aware of.

New Zealand legislation has been updated in recent years to prohibit behaviour when criminals access computers for a dishonest purpose or without the authority of the computer owner. Offenders who commit computer related crimes are often surprised to discover the serious consequences they can face upon conviction for breaches of sections 249-252 Crimes Act 1961.

2am!

What is that ringing sound? Blast, it is my phone again. Yep, you got it. They want me to jump out of bed and go and sort out their locks now! And of course only charge the daytime hourly rate that the cut price guy around the corner charges. Of course he is not answering his phone at this hour of the night. In fact, when I last did a check-up, I found that he was very hard to find after 9pm. Even more alarming is that the job he did at 4pm for $40, he wanted $170 when asked to do it at 5:15pm.

Where as once those late night calls tended to come from people who were out too late, I have been noticing an increasing trend for the calls to be in response to someone who is working the "night shift." Increasingly people are finding burglars have caused damage or stolen the keys while they were sleeping. They no longer feel safe to spend the rest of the night insecure. They want the locks changed then and there. Or maybe it is the aluminium window that has been jemmied and they need it secured until they can get the aluminium company to replace the window completely.

Obviously it is up to each company to choose whether they want after hours work. If they do choose to accept these sorts of jobs then they need to carefully cost the charges. When you allow for vehicle running (don't get started about the fuel costs), the overtime, public holidays, inconvenience to you family life, the costs, stresses and strains add up. Sooner or later you will need to face up to them. Many a keen locksmith has ended up in hospital with medical conditions because he thought he could do it all.

Personally, I think Locksmithing is the best job out. When I wake up in the morning, I have no idea of the details of what the day will bring. For instance, because I'm a specialist with safes, I often have to travel around the country in response to problems that people, companies and Government Departments face. These may be quite serious problems and need urgent addressing. So recently on one day I woke up in the morning at home. By 10am I was heading south 2 hours to open one safe. As I left that job with a successful resolution (it was open and working again), another call came in for me to attend another safe, 4 hours north. That required an overnight stay before returning home. (Of course I got that one open too... did you need to ask)?

So if you are in need of a Locksmith, bear in mind that we are constantly contending with emergency situations for other people as yourself. We are in locksmithing because we care enough to try and solve your problem and make you secure or to get back into your car or house. Give us room to move based upon who has the biggest emergency. Next time it might be you that needs us to drop the job we are on.

Allowing the right amount of time for a job is very difficult. A large part of our time we are doing what the manufacture says is impossible. Sometimes we are able to work pure magic and more often we have to fight every challenge on the way.

Recently I had a junior colleague get stuck opening a door that should have been only moderately difficult. They had succeeded in picking it, but the contrary thing still wouldn't open. I called around to see what the problem was. Recognising the only possible issue, I used a spinner to reset the lock in around 20 seconds. Needless to say the owner was highly impressed with my skill. The truth is that my colleague had done all the hard work, and I was just left to fill in the missing link. But hey, I don't mind getting the credit.

That is why I am recognised as being a Master Locksmith. Years of experience helps sort out the issues. And with having recently had the Master Locksmith Training Weekend in Rotorua, all the other members will be better equipped to solve the security issues of their clients.

Fraser Burns is a member of the New Zealand Branch of the Master Locksmiths Association of Australasia Ltd.
Email safe@safemasters.co.nz

Contact:
the Master Locksmiths Association of Australasia Ltd.
Web: www.masterlocksmiths.com.au
Email:national@masterlocksmiths.com.au

Ph: 0800 652 269

Water and electricity do not mix

By Peter Calvert

It is well known that water and electricity is an unwise combination and whilst lethal considerations are hardly likely to be issues with 12 or 24v DC, reliability most certainly is.

Consider the door and frame. Electric locks are often used on perimeter doors and many of these doors have aluminium frames. It appears to be common for doors to be open at the top of the vertical section, see the photo below. You may need to seal this void!

Even if a door is set back under a soffit, the driving rain experienced more or less throughout New Zealand will inevitably find its way down this section which you can regard as an unobstructed conduit to any lock mounted in the door.

Electric mortice locks are the obvious products to consider in this regard and can easily succumb to water ingress. However, do not overlook those installations where electric strikes are used on a pair of counter-hinged doors without a mullion or even a pair of French doors. Generally one of the pair will be mechanically locked with a flush bolt or similar device and the electric strike will be fitted to this door.

Peter Calvert is the Managing Director of Loktronic and can be contacted on 09 623 3919

Even if this door is fully protected at the top, the weakness lies in the active leaf which if open at the top will allow water to enter, fall down to the latch which then may act as a bridge and transfer water into the electric strike with failure eventually occurring.

A similar failure can occur with the ever popular V-lock, when water transfers across the thrown bolt and seeps to the PCB.

Water can enter a door frame in various ways including from window washing and house cleaning with the garden hose.

However the major brickbat must go to misusers of the ubiquitous water blaster. Doesn't everyone seem to have one? Even the smaller domestic models deliver water at pressures from 100 to 150 bar whereas the larger models designed for commercial use will deliver water at pressures up to 275 bar. (Note 1 bar = 1 atmosphere or 14.5 psi). Imagine the nooks and crannies that water delivered at these pressures will be forced into; and no, resulting damage will not be accepted by the manufacturers as a valid warranty claim.

Remember also the phenomenon of capillary attraction. Water can track considerable distances against the forces of gravity!

It seems that lock manufacturers have not accepted that conformal coating of moisture sensitive electronics and PCBs is a routine which they should follow; more's the pity!

Is it possible to use proprietary compounds such as CRC 2049 or CRC 2050 which may more than adequately protect the electronics, but some words of caution are necessary. Firstly, opening the lock case is regarded by some manufacturers as reasonable grounds to refuse any subsequent warranty claim. Secondly, the use of the CRC products mentioned must be undertaken with care. Avoid spraying any adjacent mechanical components which may quite literally be stuck together by the compound; and avoid coating any electrical contact points where wires should be attached as these will be insulated and no electrical contact will be made.

Water blasters

Door design

External doors

Indoor locks used outdoor

Stainless steel construction does not mean that weatherproof qualities apply

Capillary attraction

Tracking from latch to strike

Conformal coatings

Correct product choice is essential so do ask your supplier for their recommendation and do give the fullest description possible of the planned end use. Your supplier is here to help you make the right choice, so please help them to help you. If a product is described as approved for internal use only or is not specifically recommended for outdoor use, then do not use it in non-weather protected areas.

Most importantly, look carefully at the chosen product's construction and the materials that have been used to make it. Much of what goes into the product will be visible from an outside examination without running the risk of voiding the warranty through unauthorised disassembly. A product may well be made of corrosion resistant materials such as stainless steel but this in no way confers either suitability or approval for use in an outside environment.

Most manufacturers exclude deterioration of plated and decorative surfaces from warranty cover when their products are used in other than benign interior environments. Although New Zealand has a temperate climate it does experience extreme temperature variations and atmospheric conditions can vary widely from the sulphurous to the maritime. In this regard it pays to bear in mind that much of this country's major population centres experience maritime conditions.

It will pay to fully disclose the potential for problems to your client; they will appreciate your openness and honesty, as they in turn can then make an informed decision as to what product is most suitable for their need.

Surveillance Technologies Ltd announces the appointment of a Northern Regional Account Manager

Jack Downer, Surveillance Technologies Northern Regional Account Manager

Surveillance Technologies Ltd Sales Manager, Robert McDowell announced Jack Downer as the new Northern Regional Account Manager. "Due to steady growth in our business during the last 12 months we have decided to bring on board an experienced Account Manager in order to maintain the high level of customer service we strive to achieve," said Robert McDowell. Jack Downer has extensive Account Management experience operating in a variety of business sectors including security. Jack's role covers the Northern Region of New Zealand from Taupo north. "The opportunity to represent two well-known and respected brands of CCTV products is an exciting prospect and I look forward to representing Surveillance Technologies Ltd," said Jack Downer.

Surveillance Technologies hold the exclusive agency for Dedicated Micros and Interlogix products. The Interlogix range of products includes the Truvision and Ultraview range of CCTV products as well as the IFS range of fibre, UTP and network products. Visit the Surveillance Technologies website for more information on the products they offer: www.surveillancetechnologies.co.nz

More help on offer

Stewart O'Reilly, Managing Director of Training Systems and Solutions Ltd (TSSL)

Other security companies have offered assistance to students caught out by a scandal involving fake security qualifications.

Managing Director of Training Systems and Solutions Ltd (TSSL), Stewart O'Reilly says his company offered to help after he was contacted by TVNZ for the first of their stories reporting on a 26 week bogus security course.

Genesis Eight International College of Security is now being investigated by the Commerce Commission and the New Zealand Qualifications Authority after One News reported students had enrolled for a national security qualification course that was unregistered and had filched course materials from legitimate providers including TSSL.

O'Reilly says he was contacted by TVNZ when they were preparing the story.

"I gave them a statement, but I could not do an on air interview as I was delivering training in Samoa at the time.

When I got back I contacted local companies through New Zealand Security Association and gained agreement that the affected students would be offered employment (provided they met normal hiring requirements) and could gain their qualifications on-job while getting paid."

O'Reilly says he contacted TVNZ with the offer, but to date has not heard back from them.

Axis announces small network cameras with support for edge storage and ASIS Camera Companion

The neat and affordable AXIS M10 Network Camera Series have support for edge storage and AXIS Camera Companion

Axis Communications has announced the affordable and indoor AXIS M1013 and AXIS M1014 Network Cameras, with small design and support for edge storage, making them suitable for securing locations such as small businesses, boutiques, restaurants, hotels and residences.

"With their superb video quality in both SVGA and HDTV, and support for edge storage and AXIS Camera Companion, AXIS M1013 and AXIS M1014 are perfectly adapted for retail and other industries that require dependable video surveillance at an affordable cost," says Wai King Wong, Country Manager, Axis Communications. "These cameras allow store and home owners and other users to experience the resolution, full frame rate, and colour fidelity of HDTV surveillance – without compromising the budget."

At full frame rate AXIS M1014 offers HDTV 720p / 1 megapixel resolution, while AXIS M1013 offers SVGA resolution. The small, affordable and indoor AXIS M10 Network Camera Series come with practical features that help installations with cost restraints: H.264 compression that reduces storage and bandwidth needs, and edge storage, which includes support for storage on MicroSDHC cards as well as recording to network shares such as Network-Attached Storage (NAS). This allows users to build cost-efficient and reliable recording solutions, and can for example be used to achieve redundancy in a system.

Thanks to the support for MicroSDHC cards in the cameras, they are ideal for AXIS Camera Companion, the recently launched intuitive and cost-effective IP video solution designed for small installations. Recording the video to a MicroSDHC memory card in each camera reduces cost, simplifies installation and ensures that there is no single point of failure in the system.

AXIS M1013 and AXIS M1014 models are supported by the industry's largest base of video management software through the Axis Application Development Partner Program, and AXIS Camera Station. The cameras include support for AXIS Camera Companion, Hosted Video and ONVIF for easy camera system integration.

AXIS M1013 and AXIS M1014 Network Cameras will be available in second quarter of 2012.

Card security questioned

Entry card systems have come along in leaps and bounds in recent years. Steve Hart discovers that this speedy evolution could mean some business owners are more vulnerable to an unwelcome visitor than they imagine

Up to 90 per cent of access control systems in use today are no longer secure due to their encryption having been compromised.

That's the view of Stephen Blakey of HID Global, a firm that offers secure identity systems across the world.

Of course, Blakey has a vested interest in getting people to look at their security systems, but he makes a compelling case that too many firms – clients of security equipment providers and installers – have forgotten the age of their systems and frequently don't think to update them until it is breached.

Blakey says too many format keys that are relied upon to keep people out of buildings, are no longer robust enough to do the job.

"The codes, or format keys, have been un-encrypted by post-graduate engineers in universities around the world," he says. "They have written papers proving how they have broken 26 bit, 35 bit and 128 bit encryption codes that too many firms are relying on for their security. This means the format keys people use are not secure.

We live in a world where people don't put a zebra crossing outside the school until an accident happens. And it is the same with security, people don't upgrade until they suffer a catastrophic event.

> *"We live in a world of zeros and ones, and there are a lot of smart people out there."*
>
> *Stephen Blakey, HID Global*

Companies need, at the very least, to move away from magnetic stripe cards to proximity cards with the SIO (secure identity object) capability. Cards with RFID chips might be okay, but you need to find out if the code in the chip has been broken."

Blakey says because we sit on the bottom of the earth, far away from most of the world's troubles, too many business owners have become complacent – believing no one is interested in hacking their security systems.

"This is a mistake," he says. "Too many people think there's nothing wrong with a good old fashioned Yale lock. But the world has changed. We have seen people coming from Europe with devices to put on the front of bank Eftpos machines, to scan customers' cards, send the details overseas and wipe out people's bank accounts. So it does happen. We live in a world of zeros and ones, and there are a lot of smart people out there."

Blakey has worked in the security industry for more than 30 years, 15 of which have been in entry management.

"The early cards came out in 1991 and they were really basic – a fourth former could break the code of the magnetic stripe card if they tried. Lots of clubs used them as well as companies who wanted to allow access to their lobby area after hours."

Newer breeds of cards that allow entry and store data have computer chips built into them.

"These are a lot more secure and safer," says Blakey. "You can't add data to them once they have been programmed. Once you get one, they are what they are.

But smart cards are not the end of the road, this area of card security is constantly evolving – access controls have gone from your magnetic stripe to your 13.56Mhz RF chip – which emits a tiny radio signal."

What makes a good assessor?

Training in the security industry is gaining momentum, and having skilled assessors to guide trainees through their qualification has never been more important. By making sure assessors keep their skills fresh and up-to-date, the security industry can be confident it's delivering the most efficient and effective outcomes possible.

There are a number of simple steps assessors can take to ensure they're making the most of work time and trainee time. From the little details right through to the most important decision-making, ETITO has clear guidelines on how assessors can stay on top of their game.

☑ Remember the basics

- Know the qualification – it might sound obvious, but do you know the qualification and the unit standard you're assessing inside out? If you do, you will be more confident in your decisions. Putting in a little legwork at the beginning will make the road ahead much smoother.

- VSCARD is key – Valid, Sufficient, Current, Authentic, Repeatable, Direct. When assessing a unit standard, VSCARD should be every assessor's mantra. It spells out the basis for checking a trainee's competency – so be prepared to justify your decision.

☑ Time savers

- Rather than assessing trainees separately, look for opportunities to group them together, e.g. Five candidates can complete the same written test in a 20-minute timeframe.

- Use naturally occurring evidence as much as possible. Unit standards often include elements that can be observed during a normal day's work. If you make the most of these moments, extra time for assessing will not be necessary.

- You can assess more than one unit standard at a time. Sometimes the same skill can be applied to another unit standard – there is an example of integrated assessment practice on ETITO's website.

☑ Prepare yourself [and the trainee]

- First things first – schedule pre-assessment meetings to work out ahead of time which units can be assessed together. Doing this before you reach the assessment stage helps both assessors and trainees to have clear objectives right from the get-go. Then plan exactly when and how each assessment will happen.

- Keep the candidate in the loop. Make sure they know what to expect and are familiar and comfortable with the process. Prepare them for the assessment by letting them know what they're up against and what evidence they need to provide.

☑ NZQA best practice

Assessors will be familiar with ETITO's guidelines, but NZQA also has a similar set of best practice principles that are just as important and relevant. These include:

- Assessors asking, "Am I confident the candidate knows or can currently do what is required by the standard[s] being assessed?" A thorough check of the criteria will help make a decision that, if needed, can be justified in the appeal process.

- Being wary of over-assessing, or requesting more than the sufficient evidence needed to demonstrate competency. This can just frustrate trainees and make the process harder for all involved unnecessarily.

The full NZQA Best Practice Principles document is available in the assessor support materials on the ETITO website.

☑ We're your experts

ETITO is your expert on everything you need to know about assessors. If you're unsure about anything, we're on hand to help you out. Contact Lindy Martins on (09) 583 1307 or email lindym@etito.co.nz with any queries.

Cards that feature RFID chips have a small copper aerial and their own security protocols. The system is called 'prox' for proximity cards. Instead of swiping them through a reader, you simply wave them in front of it.

"A card with an RF chip can be up to half a metre away from the reader and still be recognised. Then the door will open or, in a belt and braces situation, the holder will be asked to enter their unique number or verify themselves with a thumbprint. The thumbprint image can be stored on the card as well.

Smart cards take it to another level with features such as active identity. These cards can store data such as access control, hold funds – such as pre-loaded money for the staff canteen – and biometric information too."

For secure computer access, these cards can be used to logon to IT networks.

Blakey says: "For example, you can pop the card in your laptop, do some work on a cloud service. Remove the card, go to a different desk, put the card in and carry on where you left off. These cards are ideal for IT staff who move around working on different computers."

Blakey says another paradigm shift is on the way, particularly with access control.

"There is a convergence happening right now with smart cards," he says.

Pick a card, any card

The days of rubbing clean the magnetic stripe on our swipe cards to get them to open doors, raise car parking barriers or pay for goods are slipping away.

These cards were invented in the 1960s, under a US government contract by engineers at IBM. By the 1980s the idea had been adopted by the banks and plastic cards were given to customers so they could withdraw cash from machines and latterly to pay for shopping at Eftpos terminals.

A German, Helmut Grottrup, invented the first smartcard in 1968, although his patent was only awarded in 1982.

Smartcards feature a read-only tamper-proof computer chip that stores far more information than a stripe of magnetic tape can. The first smartcards to be used by bank customers came out in 1994 and have been under continued development to increase security.

Contactless cards, that only need to be waved in front of a sensor, have been around for years too. But the technology is being transferred to smartphones.

"Companies such as Tyco, ADT and the Chubbs of this world are looking for integrated solutions – so people don't need to carry around a dozen cards.

"These companies are starting to ask for a one card solution for computer access, building and floor access, for the same card to hold biometric information as well as money.

This is where the logical – or active identity card – comes in because it can do all this type of stuff. But apart from this convergence, a new disruptive technology is starting to emerge, technology that is starting to turn all these format keys into mobile keys.

For example, a simcard is in every cellphone, it is effectively the same technology as in a smartcard. So now people in our industry are saying 'why don't we take all the information from these plastic cards and put it on a person's smartphone – using their sim card?' There is an application coming out called NFC (near field communication), or ISO (secure identity object) and this will wipe away any need for plastic cards in the future."

One firm that is in the process of adopting the NFC system is Vodafone in Auckland. In an announcement last month, the Smart Card Alliance, an industry association for the promotion of the near field communication (NFC) system says more than 100 million mobile phone handsets containing NFC technology will be introduced this year alone.

Randy Vanderhoof, executive director of the alliance, says: "Many think of payments when they hear NFC, but the technology opens the door to many industries for innovative applications, such as ticketing, digital content exchange, secure identification, social networking, and communication between electronic devices.

"The mobile and NFC council will provide a bridge between NFC technologies and the industries who want to adopt NFC-enabled mobile devices to discuss and promote common standards and best practices."

Karenza Boyd, MD at ISCS, an Australian company with offices in Auckland that supplies access control products, says NFC readers – which can read the signal from the new breed of smartphones – are already being installed in readiness for the roll out of the technology.

Goodbye cards?

In another sign that our trusted plastic cards are being overtaken is the TSM system that's been adopted by Kiwi electronic payments provider Paymark and phone operators Vodafone, 2degrees and Telecom.

The four companies have launched what it calls a trusted service manager (TSM) that allows owners of smartphones to make secure payments, collect reward points and pay to use public transport.

Vodafone says the technology delivered by the TSM will enable many of the cards held in your wallet – such as bank cards, loyalty cards or bus tickets – to be replaced by applications securely stored in a virtual wallet on a mobile phone.

The service uses near-field communications (NFC) technology to transfer payment information stored on the customer's phone to a retailer's NFC-equipped Eftops terminal.

At a shop check out, customers will be able to make payments by holding their mobile phone next to an NFC terminal and entering a code number.

Paymark's CEO, Simon Tong, says: "Our priority is to ensure the technology adheres to the most rigorous global standards so customers have a safe experience."

The TSM system, says Vodafone, is being built with the intention of providing a single open-access system to encourage wide-spread uptake.

Eric Hertz, the CEO of 2degrees says: "Over the past decade, our mobile phone has swallowed our newspaper, our map and our camera to become an essential all-in-one device.

The logical next step is to make it even more convenient by having it swallow our wallet and making it the only thing you need to grab when you leave the house in the morning."

Vodafone CEO, Russell Stanners, says it won't be long before people can "leave their wallet at home for good."

building, a smartcard system is future proof. It will allow the clients to add on cashless spending, log the user on to the photocopier and PC logons etc.

But I also promote it because it does have the higher security capabilities."

Blakey says the option of using smartphones instead of smart cards won't necessarily mean card manufacturers will be put out of business; 'not the smart ones anyway.'

"Instead of firms having to buy a plastic card for their staff, they'll need to buy the SIO – that is the mobile key," says Blakey.

"So if a company wants to put it on a hundred phones, then they'll need one hundred SIOs.

But there will still be room for smartcards in any case, not everyone will have a smartphone such as an Android or iPhone. It is also worth remembering that if a phone goes flat, then it is useless. So this is where the HID smartcard can be a lifesaver – they don't need a power source.

These cards will never go flat and they have the same level of security as the chips in a smartphone."

Blakey's advice to any firm using a card system is to investigate its security features and consider upgrading to a more secure system if they feel at risk.

Steve Hart is a freelance reporter at SteveHart.co.nz

"At the moment we are still waiting on the phones to work with the NFC readers," says Boyd. "That app – for access control – isn't up and running yet. But we expect it to be here by the end of the year. Some existing readers can be rejigged to read (NFC) signals from smartphones.

"But cards are still going to be used – absolutely. Because people will still need a physical ID card with their photo on it. But the one-card solution, for logging on to your computer etc will remain – so there is still a use for a physical card."

Like Blakey. Boyd cautions companies to be aware of the limitations of magnetic stripe cards.

"The security features on a magnetic stripe card are not high," she says. "They can be easily skimmed (copied). But a smartcard is a different matter because the chips have different sectors and each can be encrypted. They are harder to read and copy – having said that, even a 125Khz proximity card is a pretty open format."

Boyd says although smart cards have been around for years, it is only during the past year that suppliers and service technicians have started to promote the technology to their clients – people who may still be using much older card access systems.

"It does come down to education," says Boyd. "When clients come to me for information I always promote the smartcard technology. Even if they only require a system to access a

Chips with everything

A smartcard is a plastic card that is embedded with either a microprocessor and a memory chip or just a read-only memory chip that can't be altered.

The microprocessor card can add, delete, and manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation. The host computer and card reader communicate with the microprocessor.

Some cards can contain programming and data to support multiple applications and others can be updated to add new applications after they are issued.

Types of smart cards include: memory cards, processor cards, electronic purse cards, security cards, and JavaCards.

One of the common uses for smart card readers on notebooks is to authenticate a user for security applications. For example; secure logon and authentication of users to PC and networks, storage of digital certificates, passwords and credentials, encryption of sensitive data, and wireless communication subscriber authentication.

A smart card is inserted into the reader and then a personal identification number (PIN) is required to log onto the notebook or network. No card, no access.

Microprocessor cards (also referred as chip cards) offer greater memory storage and security than a traditional magnetic stripe card. Chip cards can process data on the card. The current generation of chip cards has an eight-bit processor, 16KB read-only memory, and 512 bytes of random-access memory.

Optical memory cards look like a card with a piece of a CD glued on top - which is basically what they are. Optical memory cards can store up to 4.9MB of data. But once written, the data cannot be changed or removed. This type of card is used for medical files, driving records and travel histories etc.

While the optical cards are comparable in price to chip cards, the card readers use non-standard protocols and are expensive.

Smart cards: life begins at 40

Sixty six year old Roland Moreno passed away in Paris during late April, an event unremarked in the mainstream media headlines, perhaps because they were unaware of just how he is beginning to influence our daily habits.

Moreno wasn't the first to think of the idea of smart cards but he was the one that took out the first patents in 1974 and is credited with getting the first business systems established in his adopted country France, opening the way for the rest of the world to follow.

But that was almost 40 years ago and although they have been used for public transport tickets in London for years, smart cards are still pretty new in this country, (for instance, out of eight various cards in my wallet today, only one has an onboard memory chip, earning it the title 'smart').

Despite 40 years and the inherent security advantages of smart cards, in access control applications they have yet to completely squeeze out older technology, says Steve Bell, Security Software Development Manager at Gallagher.

"We can probably say that magnetic stripe access control cards are dead and gone, but worldwide, the predominant installed technology is probably still 125 kilohertz proximity cards, although if you are looking at the security on them, well, they've pretty much got none and anybody can clone them," he says.
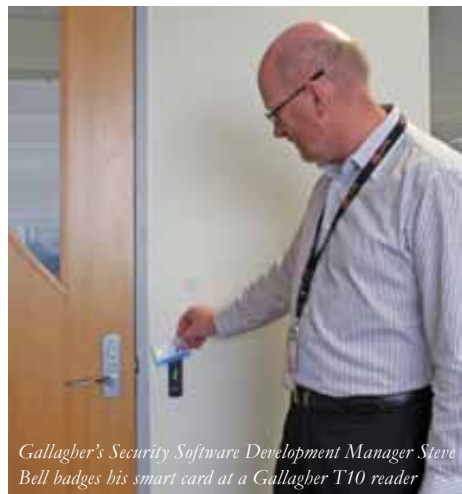
Gallagher's Security Software Development Manager Steve Bell badges his smart card at a Gallagher T10 reader

It's a situation that Gallagher, known for its access control platform Command Centre (formerly Cardax), is doing its best to change. The company believes smart cards leap frog the best 125 kilohertz proximity cards have to offer.

The most widely adopted smart cards are the Mifare series of smart cards originally developed for public transport ticketing. They are powered wirelessly from the reader over 13.56 megahertz frequency band and because they have extra memory capacity they can be used for multiple applications and accessed by different systems. For example, a university or polytechnic may use them for access control, student photo copying, and in a Rotorua example, the same student cards may be used for public transport as well.

Hacked

But the original Mifare smart card, now called the Mifare Classic, was hacked back in 2008. To be fair to Mifare's original designers, it took a high level German researcher and a doctoral candidate at the University of Virginia a long time and they did it by taking the chip itself to bits in a painstaking microscopic process. But as collateral damage of proving to the world how smart they were, the researchers made it easier for subsequent hackers, although today it still takes a determined effort by computer experts to get illegitimate access into a Mifare Classic card.

Since then Mifare variants with better security have been introduced. Mifare DESFire EV1 cards are more secure but cost more, while the more recent Mifare Plus card is designed to directly replace Mifare Classic with a more secure card.

"Mifare Plus is still pretty new, but since we bought out a new range of readers we've got some clients like universities insisting on it now," says Bell.

High security

Above Mifare there is a newer level of secure smart cards based on a United States federal government standard, FIPS 201 (Federal Information Processing Standard Publication 201) which specifies United States Federal Government Personal Identity Verification (PIV) requirements for federal employees and contractors.

"The US is pretty much leading in this area," says Bell.

"They still are working through it all, but they do have lots and lots of these cards issued and one of the things we are doing is implementing that type of functionality in our system for the US market.

"Implementation is pretty much all in the software and PKI (public-key infrastructure) encryption. It is very standards based and we have to go through test labs to get certification – we are in that process at the moment," says Bell.

"There is definitely nothing like that adopted in New Zealand yet, but in Australia we're just starting to see a desire for some higher security smart card standards in some circles."

But FIPS201 is not the only system at the high security level. In the US a system called Opacity (Open Protocol for Access Control, Identification and Ticketing with privacy), has been set up and in Australia PLAID (Protocol for Lightweight Authentication of ID) has been proposed, leading Bell to caution that competing systems are incompatible.

"From the customer's point of view, having one access token and having it being able to be used in many systems, should be the goal," he says.

"Unfortunately standardisation is not really happening. It would be good if there was just one or two standards for the world, but at this stage we don't know which standards will come into use in which markets."

A single standard with interoperability would offer practical benefits says Bell, pointing to the example of the Queensland Government's transition to smart card drivers' licences, a project that commenced in late 2010 (after a cost blow out and delay that seems to often attend these kinds of government schemes).

As well as usual vehicle classes, the smart card licence includes an adult proof of age card, a marine licence indicator and

industry qualifications such as dangerous goods or escort vehicles certifications.

"It has various protocols to access the various classes of information," says Bell. "One example is if you go into a pub, you can present your smart card and the machine at the bar will ask the card if you are over 18 years old. The machine simply says yes or no, without revealing how old the person is."

Other ways

But for all the options and possibilities in the future, a two stage authentication process is a simple way to boost access control security on existing Mifare based systems.

With Gallagher Command Centre's Challenge feature, when you present your access control card at the reader, then and at the operator's workstation in the control room, your picture and all the other information turns up on the screen. The workstation operator then visually identifies you using CCTV covering the access point and grants or denies access.

"The Challenge feature would normally be used in military or defence and it is used quite a lot on some of our ports, including the truck gates. They might use it all the time or just at times of elevated security risk," says Bell.

"The system works a bit like a biometric, except with the verification done by the guard. Any time you have got a smart card plus biometric, then that is definitely a higher security level. Fingerprints are generally the most common biometric and we have integrated Morpho biometric fingerprint readers with our systems, giving people the option of either storing the biometric information in a database, or storing it on the Mifare card itself, if they have privacy concerns."

Competencies

But for Gallagher smart cards have now gone past simple access control authentication and time keeping, a process helped by the company making its own readers.

"Not many access control companies make their own readers and most of the generic readers on the market don't make it easy to get to some of the higher security levels," says Bell.

"But we have built a good encrypted protocol between the reader and the controller so that gives us a much more secure environment and we can also add more value through it.

A lot of what we do these days is around health and safety. For example as people are passing through we can check what we call competencies. If you visit a site that has some sort of requirement that you've done a safety induction before you go on the
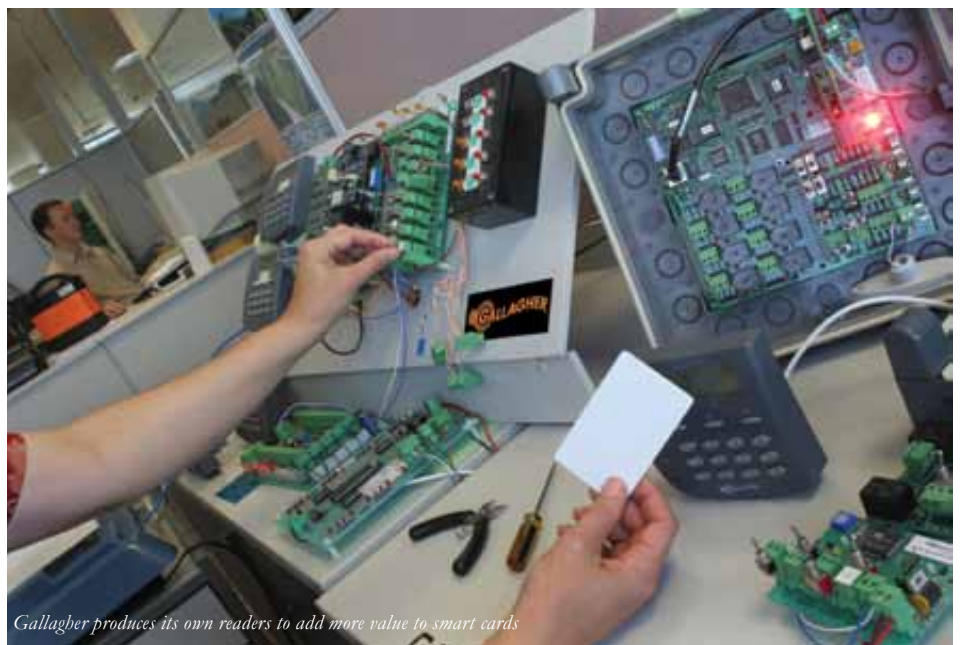
Gallagher produces its own readers to add more value to smart cards

site, then we will check at the access point to see if that person has done that safety induction. We also check to see when it is going to expire and if it is using a reader with a display, it will warn you when the site safety training is going to expire. We can also set the system up to help with random testing of cardholders for drug and alcohol."

The ability to control detailed health and safety programmes on top of access systems is ideal for mining and other large operations, but Bell says smart card technology is flexible enough to be useful to small companies as well.

"We have starter kits with just a few readers, that make electronic access control affordable for smaller businesses too," he says.

The future

Secure smart cards may have been slow to take over our wallets, but there are more mobile phones than people in this country and smartphone penetration is growing rapidly with estimates of perhaps one million of them in New Zealand already.

In Wellington advertisements suggest you can use your mobile phone as a smart card alternative on the smart card 'touch and go' bus ticketing system called Snapper, which also works in many stores, taxis and coffees shops. Another slick television advertisement for a bank shows a similar phone app can even be used to allow debit money transfers between phones with a flourish and a bump.

For access control and security systems this kind of functionality represents an opportunity – once the market shakes down to one or two reliable technologies and back end systems and enough phones become NFC (near field communications)

capable. NFC mobile phones mimic contactless smart cards and potentially have more processing power and capability than can be loaded on smart cards.

"I think in the next two or three years you'll find that people will want to use NFC on mobiles for medium security access control and if it is all done properly they do have the security required for that," says Bell.

"Smart phones allow software applications to be loaded by the end users but hackers can gain access to data stored on the phone. The most secure way to store user credentials on the phone is a special hardware chip often called a 'secure element.' The SIM card in your phone is an example of a secure element that is an ideal way to securely store the user's credentials.

Our new generation of readers are smarter and they have got downloadable firmware, so they are NFC capable. We just need to get the appropriate standard implemented in the phones and then implement the appropriate firmware for that on the readers.

I think it's going to be popular the way smart phones are going now because those people who like their smart phones want to use them as much as they possibly can."

For all that, the concept has a way to go, since NFC has not yet been implemented in iPhones and only works on the more recent Android and Blackberry phones (most of the non-Apple mobile phones) even though it was back in 2004 that Nokia, Philips and Sony founded the NFC Forum, the 160 member group behind the system.

Nevertheless, you can probably be pretty sure it's not going to take NFC mobile phones anything like the best part of 40 years that it took Roland Moreno's smart card dream to reach a critical mass.

HID Global deploys a centralized, web-based IP access control solution at Fuxi Power Plant in China

Occupying a total area of 57 hectares, Fuxi power plant is located in Yibin City in the Sichuan Province. China Power has invested over US $732 million in setting up the four-unit, 600 megawatts power plant. When completed, the plant will generate over five billion kilowatts of electricity per annum and achieve an annual output value of US $211 million. Not only does the plant supply power to support the rapid development of the region, but will also contribute to the region's electricity transmission via China's western power grid.

The Challenge
As a key power supply in the region, any unauthorized entries into the Fuxi power plant could pose potential threats to its equipment, personnel and the environment. Therefore, strict staff and visitor access control management needed to be implemented.

Additionally, the plant's traditional patrol system cannot meet the need for real-time monitoring due to the plant's numerous entry points and large coverage area, and the plant environment is combustible with high electromagnetic interference. As a result, the access

Products and Technologies

- VertX® V1000 Network Controller
- VertX® V100 Door/Reader Interface
- VertX® V2000 Reader Interface/Network Controller
- iCLASS® R10 Contactless Smart Card Reader
- iCLASS® 2000 Contactless Smart Card

control system must withstand harsh environments, while providing reliable performance and resistance to fire and electromagnetic interference. The plant's requirements for its access control system included the need for:

Fuxi Power Plant

- Central monitoring through a central network platform to connect the central station and affiliated subsystems to enable real-time monitoring and remote area control.
- Access level settings that restrict access based on job functions.
- Visitor management to verify and record visitors' details to effectively prevent potential threats caused by unauthorized, external visitors.
- Data management to store the entry records and card access information and generate reports for analysis.

Solutions

HID Global leveraged the plant's existing network investment to deploy a centralized, web-based IP access control solution by connecting HID's VertX® V2000 controllers to the host computer via a TCP/IP network for remote monitoring, area control and report generation.

To ensure the safety and proper staff management within the Fuxi power plant, HID iCLASS® R10 readers and credentials were deployed, where all staff must now present their iCLASS card to verify their identity at plant entry points. With the iCLASS readers' data encryption and mutual authentication capabilities, the plant's overall security has been significantly increased and strengthened.

HID Global's access control system also enables access level settings at critical entry zones, such as main production plant, engine room, central station and chemical waste areas. The system restricts entry to specific areas at specific times, grants access to critical zones to authorized personnel only and sets staff access levels and entry times based on job titles. For example, access to the chemical waste area is restricted to certain trained staff, and the administrator can now establish access rights to prevent unauthorized entry and ensure occupational safety. Furthermore, the new access control system enables the

V2000

HID iCLASS® R10 reader

staff's entry records to be used for time and attendance management.

For increased security, the plant enforces effective visitor management measures by utilizing the access control system for temporary visitor badge issuance in order to monitor and record visitors' access. When a visitor enters the facility, he or she is assigned a visitor badge that limits access areas and access times. The security administrator can also track visitor entry and exit activity real-time via the control center.

For system management, the VertX V2000 controller ports into nodes wherever a network exists, reducing the need for wiring in remote areas such as the power-controlled relay facility and the plant's coal transportation building. HID iCLASS R10 readers were also installed at each entry point and connected to VertX V2000 controllers to transfer the entry records to the host.

By integrating with partner software and the plant's electronic floor map, HID Global's access control solution allows authorized staff to monitor the door status at the control center and remotely open and close doors. In case of a door left open or a tamper alarm, the system can determine the incident type and indicate the door location on the electronic floor map. The security administrator can remotely close and release doors depending on the incident type.

Finally, VertX controller and iCLASS readers are UL94-certified with fire-resistant capability, which is ideal for the Fuxi power plant's combustible and extreme operating environment.

Results

The HID Global solution fulfills Fuxi power plant's need for multi-layered and centralized access control management. "HID Global's access control system was installed at the first phase of the project, which significantly enhanced the overall security and improved efficiency," said Mr. Fu Bo, Sectional Chief with Fuxi power plant. "By leveraging the advantages of the web-based, centralized access control system, the administrator can now remotely control various entry points, which has substantially reduced patrol deployment time. The system also provides multi-layered security to eliminate unauthorized access to the plant."

In addition, HID Global's open architecture VertX networked access controllers are designed to meet the plant's evolving requirements through simple firmware upgrades for future system expansion and are scalable to enable additional applications, such as fire alarm, biometrics and logical access.

For more infomration on HID's products and services within New Zealand, please contact Stephen Blakey.

Stephen is the HID Regional Sales Manager for New Zealand.

Stephen can be contacted on 09 537 0279 or 0210 824 6096 email:sblakey@hidglobal.com.

FlexiDome HD 1080p Day/Night IP cameras

FlexiDome HD 1080p Day/Night IP cameras are progressive scan CMOS cameras that use the Bosch designed Dinion digital imaging technology. The camera uses the latest CMOS-based HD sensor for a sharper, more detailed picture with a 16:9 image format. Features such as multicasting, internet streaming and iSCSI recording are fully supported. The FlexiDome HD 1080p camera delivers the highest standards of performance and reliability in any security and surveillance scenario, day or night.

Outstanding image quality
With a 1/2.7-inch CMOS HD sensor, the FlexiDomeHD Day/Night IP camera delivers outstanding image quality. The Bosch designed digital video processing system optimally handles the HD image format without compromise. Image performance and colour reproduction are superb even under challenging lighting conditions.

Flexible lens choice
The camera comes with a choice of tele, mid-range and ultra wide angle lenses. Each lens is specifically matched to the sensor to ensure full resolution even in the corners. The 1.8 to 3 mm optically corrected ultra wide angle lens provides outstanding performance without the need for de-warping software.

Day/Night switching
In night mode, the camera enhances low light viewing by switching the IR (infrared) filter out of the optical path and providing a monochrome image. The camera can switch from colour to monochrome mode automatically by sensing the illumination level, manually via the alarm input, or remotely via a web browser.

Privacy masking
Four different privacy zones allow specific parts of a scene to be blocked. A mask for any part of the scene can be pre-programmed.

Tough design
The cast-aluminum housing, polycarbonate window, and hardened inner liner can withstand the equivalent of 55kg of force. The enclosure contains the full-featured camera and integral varifocal lens. Ideal for outdoor use, the cameras are protected against water and dust to IP 66 (NEMA -4X) standards. The camera enclosure provides the extra protection necessary for applications such as schools, banks, prisons, retail outlets and industrial buildings. Installation is quick and easy, as the camera comes completely assembled and ready to use. The camera uses Bosch designed lens and optics to deliver true HD resolution with different light levels.

Using the proprietary pan/tilt/rotation mechanism, installers can select the exact field of view. Mounting options are numerous, including surface, wall, corner, and suspended ceiling mounting. The compact, sleek design and virtually flush-mount appearance complements any decor.

Efficient bandwidth and storage management
The cameras use H.264 (Main Profile) compression, bandwidth throttling, and multicasting capabilities to manage bandwidth and storage requirements efficiently, while delivering high image quality and resolution. Bosch's innovative Quad-streaming feature enables the FlexiDomeHD to deliver three H.264 streams (a 1080p30 HD stream, a downscaled resolution stream, and a HD I-frame only stream) together with an M-JPEG stream. These four streams facilitate bandwidth-efficient viewing and recording options as well as integration with third-party video management systems.

FlexiDomeHD cameras offer unparalleled recording options. Attached to the network, they can use iSCSI targets directly without needing any recording software. The recording management capabilities of the system can be further enhanced by using the Bosch Video Recording Manager (VRM).

- **1/2.7-inch Day/Night CMOS with progressive scan**
- **Choice of high performance lenses**
- **Local Storage for flexible recording options**
- **Motorized automatic back focus**
- **High-impact, vandal-resistant enclosure**

Bosch Dome 1080 HD

FlexiDomeHD supports local storage on a microSD card. This can be used for local alarm recording or for Automatic Network Replenishment (ANR) to improve the overall reliability of video recording.

Standard intelligence

With built-in video content analysis, the camera reinforces the Intelligence-at-the-Edge concept where edge devices become increasingly intelligent. The MOTION+ video motion analysis system that is built into all camera versions, is the perfect solution for applications where standard video content analysis features are required. This motion analysis algorithm is based on pixel change and includes object size filtering capabilities and sophisticated tamper detection capabilities.

Advanced IVA version

The hardware-enhanced version of the camera upgrades the video content analysis features of the camera with the more advanced Intelligent Video Analysis (IVA). This version contains such features as idle object, line crossing, flow detection, crowd detection etc.

ONVIF conformance

The camera conforms to the ONVIF (Open Network Video Interface Forum) specification which guarantees interoperability between network video products regardless of manufacturer. ONVIF conformant devices are able to exchange live video, audio, metadata and control information. They are automatically discovered and connected to network applications such as video management systems.

Unsurpassed flexibility

There are many ways to access the camera's video: on a PC using a web browser, with the Bosch Video Management System (VMS), or with the Bosch Video Client. The bundled Bosch Video Client PC surveillance software offers a user-friendly interface to support easy installation and configuration. It also provides easy live viewing of multiple cameras, playback, forensic search and export.

Cost effective, simple installation

Three power options, PoE (Power-over-Ethernet), 24 VAC and 12 VDC are available. Using PoE makes installation easier and more cost-effective, as cameras do not require a local power source. To increase system reliability, the camera can be simultaneously connected to both PoE and 12 VDC/24 VAC supplies. Additionally, uninterruptible power supplies (UPS) can be used, which will allow continuous operation, even during a power failure. For trouble-free network cabling, the cameras support Auto-MDIX which allows the installer to use straight or cross-over cables.

Automatic back focus

An automatic motorized back focus adjustment ensures the camera is focused accurately for both day and night operation.

Intuitive user interface

The FlexiDomeHD camera has a very intuitive user interface that allows fast and easy configuration over IP. An auto-focus lens wizard can be activated either from the PC or through the camera buttons. This makes it easy for the installer to choose the workflow that suits best for setting field-of-view and focus with 1:1 pixel mapping.

Easy Upgrade

Remotely upgrade the camera whenever new firmware becomes available. This ensures up-to-date products, thus protecting investment with little effort.

Access Security

Various security levels are available for accessing the network, the camera and the data channels. As well as password protection with three levels, 802.1x authentication using a RADIUS (Remote Authentication Dial In User Service) server is supported. To secure Web browser access, use HTTPS with a SSL certificate stored in the camera. For total data protection, the video and audio communication channels can be independently AES encrypted with 128-bit keys by installing the optional encryption site license.

Bosch Video Client surveillance software

The bundled Bosch Video Client PC surveillance software offers a user-friendly interface to support easy installation and configuration. A wizard allows the configuration of multiple cameras simultaneously using an auto detection device. Multiple cameras can be monitored in one screen and video clips on the SD card can be archived and searched in a single application.

NZ Fire smokin` ahead with technology

By Keith Newman

The New Zealand Fire Service sees itself as a world leader in the use of innovative response technology with two significant upgrades this year taking it even deeper into the world of digital despatch and communications systems.

Upgrades across a range of digital technologies are opening the way for rich digital interaction between fire alarm panels and computers in vehicles and the ability to deliver real-time information on what's happening at the scene of the fire.

An important part of the digital chain will be computers on trucks. A couple of years back when this was first scoped out ruggedised units would have cost up to $8000 each, now the same capability is possible for around $600 per unit.

The longer term mix is touch screen technology and even 3D, which could give a more realistic view of what fire fighters will face when they arrive on scene. Experimentation in the US is being closely monitored to see where it might match local fire fighting needs.

Meanwhile NZ Fire Service IT and communications teams are scoping out smarter ways to use digital networking, IP telephony, the Intergraph CAD (computer aided despatch) system , satellite tracking and the digital radio capability they'll begin upgrading to later this year.

Bill Butzbach, director of strategic development and assistant to the National Fire Commissioner, says there's an in-house debate going on currently that will "without a doubt affect the way fire protection systems evolve in the future."

The NZ Fire Service emergency communications centre

fire door holding
electromagnets

Standard, floor mounted, wall to door distance 114mm

A)

B)

C)

FDH40S
unbreakable universal mounting

• Low power consumption - low operating temperature
• One product suits floor and wall mounting
• Universal armature - offsets to 55º to suit doors opening past 90º • Wall mount extensions available
• 12 VDC models and 24 VDC models • Push off button with no residual magnetism • Oversize armature for easy alignment • Emergency release button
• Electroless nickel plated armature and electromagnet
• Stainless fastenings • Full local support and back up
10 YEAR GUARANTEE*

Designed, tested and produced in New Zealand to AS4178

A) Wall mounted, 126mm extn. tube (overall 202mm)
B) Wall mounted, 156mm extn. tube (overall 232mm)
C) Wall mounted, 355mm extn. tube (overall 431mm)

Flush mounted, wall to door distance from 50mm

Surface mounted, wall to door distance 70mm

BOTH options are packaged in the same box

FDH40SS
stainless steel surface and flush mounting

This device enhances an outstanding range of unbreakable products which conveniently hold open fire doors. When a smoke/fire alarm is activated the magnet instantly releases the door to the closed position to prevent the spread of smoke and fire. These units feature satin finished stainless steel covers for optimum aesthetic appeal and durability. To allow maximum flexibility the electromagnet is pre-assembled onto a plated steel mounting plate. The installer can utilise one device for surface mounting or for flush mounting.
10 YEAR GUARANTEE*

For expert advice and assistance with your security locking needs, trust in Loktronic, call us on 0800 367 565

19711

*Standard terms & conditions of sale apply.

Investigation is already underway into how the service can work with the rich data provided by modern fire alarm systems and panels. "We've got smart CAD at the receiving end and we own the alarm transport system pipe but it would be up to the building owners to invest in so-called smart panels so we could make better use of that," he says.

When NZ Fire Service has "fully conceptualised the vision" of this technology shift, it will engage with building owners, the fire protection industry and technology providers to see what's possible.

Security shows the way

Butzbach says much of this technology already exists and you only need to draw parallels with the security industry to see where it's all heading. "Imagine if we had heat detectors telling us the rate of rise in a fire, where it started and where it's moved to, before you even got there? What would that do for our tactics?"

And he says the use of remote cameras to check the fire floor before an engine was even despatched could have a profound effect on whether one truck or a fleet was sent. "It could really add to our efficiency and reduce false alarms which are a huge cost to building owners and disruptive to staff and productivity when employees have to leave the building."

Butzbach says new technology could improve the reliability of fire alarms and drive maintenance costs down. "We're trying to take this holistic view and while we've not done much more that conceptualise and dream we're absolutely committed to pursuing it."

He says NZ Fire Service is investing heavily across the board in technological improvements including its despatch,

Bill Butzbach, NZ Fire Service, Assistant National Commander and head of the emergency communications centres

"Imagine if we had heat detectors telling us the rate of rise in a fire, where it started and where it's moved to, before you even got there? What would that do for our tactics?" Bill Butzbach, NZ Fire Service Assistant Fire Commisisoner.

telephony and radio systems. "It's about future proofing because we can see the benefits that can be realised in the medium to long term."

The most recent improvement was an upgrade of the Intergraph CAD software across the three major emergency communications centres in Auckland, Wellington and Christchurch. "For 12 hours we were back to doing everything manually but now the new graphical user experience for the operators is a lot less clunky and much simpler," says Butzbach.

The system interrogates maps, pulls data from the core NZ Fire Service database and has resulted in a faster, more resilient despatch system. Ahead of the new system going live some serious retraining was required.

"The look and feel is fundamentally different to what it was before — there's no room for error."

Call centre operators get 11-12 weeks of training and mentoring then go online with a buddy before they become qualified. "We don't just let anyone loose in there," says Butzbach, who's also head of the NZ Fire Services emergency communications centres.

Shared service enhanced

In the mid-90s the NZ Fire Service set up an agreement with NZ Police to move to the new Intergraph CAD emergency communications centre environment, now a virtual platform, enabling multiple parties to share the same content.

"That's made a huge difference in terms of fall back contingency and business continuity. If something is out of commission for any reason we can seamlessly switch over to any of the other two systems, which was certainly the case during the Christchurch earthquake," says Butzbach.

Previously if there was a crash it could take 12 hours or more for the back-up server at the Royal Police College in Porirua to come back on-line. "A couple of years ago we put in this thing called Oracle Dataguard which, on a good day, will see our crash over in 3-10 seconds or no more than a minute on the worst occasion."

That capability gives both NZ Police and the NZ Fire Service a great deal of confidence and also enables them to interact directly with St John and other ambulance services which have their own independent communications centres.

"In the past it was all manual with a special 'allied emergency services direct line'; now, if we need to call for assistance or share a job, our CAD system talks directly to their CAD system."

Butzbach says this breakthrough occurred when Police and Fire developed their own bespoke application called InterCAD so events can be directly copied across systems.

"There's no wrong door approach when people dial 111. The job is accepted and banged through electronically and it just appears on our screens — this has revolutionised how we interact together."

Behaving as one

Another key ingredient to the joint systems is the Solidus IP telephony platform which enables the geographically dispersed services to behave as one organisation, handling different incoming media in real-time with pop-up screens for specific information.

Once a call is received from the Telecom i-CAD answering system it is directed to the first available operator, regardless of where they are in the country, resulting in faster call times. "Our target is to answer calls within eight seconds which we're now doing 97 percent of the time," says Butzbach.

Everything is geospatially linked through map-based systems and the use of GPS (global positioning systems) satellite tracking. "We've got into that in a big way and about 400 of our key fire engines and specialised appliances are fitted with this kit."

Butzbach says the enhanced despatch centre can see on screen where the various engines are at any time and inform them directly if they miss a turn or get lost.

"This is especially good in rural areas where it's easy to miss address points and we can see where they need to be going. They might say 'we're on this ridge and can see the fire' and we can advise which rural track will give them the best position to stage their operation."

He says there's a real safety aspect to the GPS system as well. "We have lost trucks in the past through motor accidents and it can take time for them to be discovered; now we can be alerted really quickly."

NZ Fire Service has a fleet of 800 trucks and is rolling out the GPS capability incrementally. "We have prioritised and will keep re-evaluating once we've done the benefit realisation work. All the indications are that this system is returning everything we wanted and more."

Quicker the better

Butzbach says the new approach also opens the way for future proofing and a time when people will be able to interact more directly with the CAD system from the fire appliances.

"We're always looking for more automation because of the time critical nature of our business. The technology already exists to do this kind of thing but we need to make sure it's reliable."

The quicker information gets to the CAD the better. "The faster the bells go, the faster the trucks are on the road and if they get good information while they're on the road the more efficiently they'll be able to do their job."

A lot of time is spent with "the troops" out on the road, visiting commercial and industrial premises, collecting data about building access and layout. This is entered into the Station Management System and sent to appliances on call out as a prompt number showing where the diagrams are in the hard copy risk plans.

That number relates to building plans, on-site water maps, utilities and other important information which over time will be automatically delivered to PCs in the command units.

The CAD will also be able to interrogate local authority databases for storm water and other utilities and automatically show building layouts and how far away the next hydrant is, for example.

"You can't keep banging out hoses if there's not enough places to supply them. We'll draw water from a wide range of sources, including mains infrastructure for bulk water but we need to know about this before we get on site," says Butzbach.

Digital radio roll out

Until recently mobile communication has been through analogue radio systems but as NZ Police are now migrating to a more reliable and secure digital radio system, NZ Fire is gradually following suit.

"The analogue system was serving us well but as technology is advancing so rapidly we see the potential to be tapping

into a range of rich data to give us more mission critical information on the trucks," says Butzbach.

The first roll out will be in Wellington in September and Christchurch early next year. "We'll leave it to bed in for a while before moving beyond that and still maintain the analogue network."

Apart from issues of reliability, he says, it opens up a whole range of other network opportunities including interfacing with voice over IP for communications. "We're just starting to get into that with the Police."

Ultimately digital radio will be an essential component of the overall digital despatch system, integrated with the CAD and telephony platforms.

Mobilising from anywhere

As part of that transition NZ Fire Service has introduced a Cisco-based system that can link through the internet to access its radio networks across the country.

"We have prioritised and will keep re-evaluating once we've done the benefit realisation work. All the indications are that this system is returning everything we wanted and more," Bill Butzbach on rolling out GPS in the nation's 800 fire appliances.

"In the past we mobilised our trucks using cell call radio signals, and while Wellington could turn out everyone from North Cape to the Bluff, Auckland could only get to as far as Palmerston North and the South Island only within the South Island."

Now he says Auckland can despatch Bluff and Christchurch might switch Wellington or Auckland. "We practice this every week, starting in different centres and then progressing around the country to ensure this works seamlessly."

Butzbach says the fire service is continually discussing how it can improve the use of its IP network and systems, and is involved in senior level forums with NZ Police and government groups on innovation and how to be more proactive.

As far as nationwide roll out of digital radio goes, he says a lot will ride on the savings as indicated through the whole of government digital radio experience. "For us the main point is answering calls faster, getting the right kit there a hundred percent of the time, along with the key information, to get a good result."

He says the NZ Fire Service has won innovation prizes internationally for its technological achievements. "It goes to the heart of what we do as Kiwis. Through the nature of our country we are forced be national in our focus."

Overseas, he says the fire service is run by local authorities in smaller units which often don't have the budget or wherewithal to invest like New Zealand does. "We try stuff out — there's not too many jurisdictions with the kind of technology we have," says Butzbach.

There's strong interest from other forces, including those in the UK, and often the NZ Fire Service and NZ Police are invited to technology forums. "We get asked to tell our story and share our good news with other agencies. Rather than sell it, we freely provide advice for the common good of our industry which is international in nature."

Alarm at fire-related consent rejections

NZ Fire Service urges fire engineers to lift their game

Too many building applications are being fired back to consenting authorities by the New Zealand Fire Service because fire engineers have done a less than professional job demonstrating compliance.

Fire Engineering Manager, Simon Davis, says changes in the Building Act are highlighting a lack of professionalism among fire engineers who aren't paying enough attention to emergency access, venting, water provisioning, new technology and ensuring fire protection systems work together.

He says the design work advising building consent applicants is often so poor it takes many iterations to get it right, resulting in wasted time and money. "The idea is to do it once and do it right; that's why you employ a professional

"We invariably find the fire engineering fraternity have got it wrong, have used poor engineering process or completely overlooked things and not been able to demonstrate compliance," NZ Fire Service head engineer, Simon Davis.

engineer — if you have a dog you shouldn't have to do the barking," he quips.

"We'll work with the applicant and consenting authorities to get the job as close to complying as possible but if the application is not done properly in the first place then its not going to get through."

Over the past five years NZ Fire Service has taken on the role of reviewing the fire safety aspects of building consents on behalf of the New Zealand Fire Service Commission, processing 20-30 consent applications every fortnight.

It has nine engineers in its Auckland offices dealing with applications from the country's 75 building consent authorities (BCAs), mostly relating to commercial and industrial premises, and has to return them within 10-days with comments and memos.

Wrong too often

Davis says three of the 28 clauses in the Building Act relate to fire protection; safety, means of escape and operations and facilities for the use of the fire service. "We invariably find the fire engineering fraternity have got it wrong, have used poor engineering process or completely overlooked things and not been able to demonstrate compliance."

He says fire engineers should be fully aware of the requirements. "Unfortunately we often find the information is rather scant and we have to provide quite a few comments on deficiencies."

Davis says compliance issues have been considerably tightened since the 1991 Building Act was replaced earlier this year. "It's not the responsibility of the consenting authority to point out mistakes or offer advice, it's the applicant's job to review all the requirements and provide all the information."

To ensure the NZ Fire Service is on track and providing the right feedback to the various building consent authorities, the NZ Fire Service Commission audited its work six times over the past five years and all the reports confirm a high failure rate in fire compliance.

Although the NZ Fire Service has published a water code of practice which has become a New Zealand standard even those efforts have provided evidence that the industry needs to lift its game.

Fire engineers are still not "turning their mind" to this, says Davis. While the requirements might not be outlined

Simon Davis, NZ Fire Service head engineer

Turn night into day!

NEW FLIR F-Series

Total Darkness

Thermal Image

Fog or Smoke

Thermal Image

NEW FLIR PT-Series

Network-ready thermal imaging cameras for security applications

Thermal imaging cameras are becoming more and more popular for security and surveillance applications. Many users are asking for thermal imaging cameras that can seamlessly be integrated in new or existing TCP/IP networks. The new FLIR F- and PT thermal imaging cameras are an answer to their demands. The F-Series are fixed mount thermal imaging cameras. Once installed they always look in the same direction. The PT-Series are mounted on a precision Pan/Tilt. This drastically increases situational awareness. They also contain a daylight/low light camera that can be used when conditions permit. All cameras can be installed in a TCP/IP configuration or an analog configuration.

According to your needs, you can choose from a wide variety of lenses. You also have the choice of image quality: 640 x 480, 320 x 240 and 160 x 120 pixel detectors are available.

Available at:

Hills
Electronic Security
New Zealand

www.hillsec.co.nz

◆**FLIR**®

in detail in the Building Act, "without access to sufficient water in the vicinity of the building the fire side of things is practically useless."

Future proofing

And he says fire engineers also need to be aware of the technology path the industry is heading down so the drawings they come up with are truly representative of the completed building. In other words, how useful will those design drawings be if presented graphically to the fire service during a call out?

He says everything in the design and consenting stages needs to be part of one big loop. "If you get it wrong at the beginning then everything can go pear shaped later on. The consent level is major building block and if the paper work is done correctly it makes the job of contractors and builders a lot easier.

To assist with that awareness the NZ Fire Service has produced a Fire Fighting Check List (www.fire.org.nz) which raises the various issues that that need to be considered in building design.

This includes ensuring all the aspects of emergency services fit together, from extinguishers and alarms to access to hydrants; fire facilities rooms where sprinkler valves are housed, pumps to bring water to a building's hydrant system and emergency warning systems. "In an emergency there's no time to fix things — they need to work first time."

Part of the package may be an automatic voice system with a public address system so occupants can be informed not to go down certain stairs which might be blocked or damaged, or a phone so people can call if they're stuck.

"It's currently acceptable for people with disabilities to be kept in a building but we need to know where they are so we can rescue them. There are a range of things that require some detailed thinking that often seem to be missing."

Davis says vital areas that relate to public safety are not being taken as seriously as they ought to be. "We have issues around 3000-4000 memos over the years raising these issues."

Information available

He says the information is available and the audit reports on the service provided by NZ Fire have resulted in the Department of Building and Housing and IPENZ publishing a detailed practice note about what's involved in demonstrating compliance with the Building Act

With compliance issues about to be placed more directly in the hands of the applicant through self-certification, Davis reiterates, awareness about fire protection issues and the level of professionalism in the industry has to improve drastically.

"If it's done properly it'll make our job redundant and place those checks and balances on the engineering fraternity themselves," he says.

Obstacles include the fact there's a shortage of qualified professional fire engineers in New Zealand and a reluctance within the industry to require fire engineers to become qualified.

NZ Fire Service established a lectureship in fire engineering and helped create a position at Canterbury University, resulting in a world-recognised Masters level fire engineering degree, but it's not a compulsory engineering studies subject.

"We regularly see engineers working in the fire area who have no formal qualifications; they've just picked it up as they've gone along," says Davis.

That presents something of a dilemma as the Government recently made it compulsory for all building practitioners to be licensed which includes engineers. The missing link now he says is being able to easily identify those with fire protection industry skills.

Davis wants clarification around which engineers are competent to do that work; something NZ Fire Service and building consent authorities are hoping the Institute of Professonal Engineers (IPENZ) will take on board.

Ventilation vagaries vexing

New research shows that buildings that aren't equipped with adequate venting systems can impede the efforts of fire fighters and are at greater risk of being completely destroyed if a fire takes hold.

The New Zealand Fire Service is concerned that some building developers are lagging behind the world when it comes to installing efficient venting systems for smoke and heat.

"We've noticed a bit of resistance from developers who don't see the benefits of installing proper ventilation in large buildings and consider it an unnecessary cost," says NZ Fire Service head engineer Simon Davis.

He says the problems often occur in warehouses; which are getting larger all the time, where there's a false belief that plastic skylight roofing material is adequate for fire venting.

"Historically plastic roofing was used for lighting but over the past 20 years it's been assumed that these will melt or give way in heat and provide adequate venting."

However research done by fire industry specialists at Canterbury University and internationally has shown that by the time those materials burn or melt fires can escalate to the point where neither the building, the equipment nor the economic activity inside can be saved.

What's needed, says Davis, are roof units designed to vent when triggered by smoke or heat. "A lot of product made overseas and in this country uses thermal links or detection systems that open venting at an earlier stage in the fire."

This provides much greater opportunity for the fire service to get into the building and attack the fire aggressively to prevent loss of the building and contents. "If this venting hasn't occurred we're in a position where we've got to try and throw water in through holes in the building and there usually aren't many holes in a warehouse."

Davis says proper venting allows the fire service visibility and keeps the temperature down.

It can be triggered electronically or simply using thermal links in fire dampers such as bimetallic metal that bends or solder that melts and releases the device.

And it's not only designers that have been resistant to including specialised venting in large premises but fire engineers. He says the industry needs to get up to speed quickly, as its a requirement of the Building Act and part of the conditions that enable the fire service to gain access to a building.

He says two recent determinations gained by the Building and Housing Department relate to the need for effective venting in buildings. "While there was allowance for some compromise after these structure were built they're also served to put the industry on notice that these aspects need to be considered."

Compliance bodies divided on fire competence issues

The New Zealand Fire Service and some of the country's Building Consent Authorities are at odds with the Institute of Professional Engineers (IPENZ) over how to determine engineering competencies, particularly around fire protection.

NZ Fire Service head of engineering, Simon Davis, wants IPENZ to declare the specialisation of its members so its clearer where competencies lie among the 15-20 different engineering disciplines

However, IPENZ insists labelling its members isn't going to make a difference, believing the issue of competency is the responsibility of individual practitioners. It reckons if the NZ Fire Service or BCAs are unhappy with the quality of work being presented by Chartered Professional Engineers they should lodge a complaint.

Ideally, says Davis, engineering registration bobyy IPENZ could administer a programme where individual technical fraternities indicate where structural, civil, geotechnical, fire engineering and other specialisations apply.

"So far they've resisted doing this. All you can tell from their website is that they are Chartered, but not in what area. That's a concern to building consent authorities and the NZ Fire service," he says.

IPENZ Chief Executive Andrew Cleland believes the move to isolate competencies is largely being driven by the regulatory community. "They seem to think that seeking out a label helps reduce their liability in a commercial sense which is not true."

Name and shame

The normal rule with major professions is that registered lawyers, accountants and engineers self declare their skills and competencies. "If they are submitting negligent or sloppy work then the complaints process needs to be enacted," says Cleland.

"We can't have agencies saying we're having bad work submitted and, without submitting a complaint, expect the registration authority to sort it out."

He says some jurisdictions try and provide information about fields, using single word descriptors for example, but this can be badly misinterpreted. "A structural engineer for example could be an expert in reinforced masonry, timber, steel or concrete design or a combination of those."

Even in fire, he says, there are those with skills in the design of egress while others specialise in sprinkler and alarm systems.

In IPENZ view, the system of each practitioner taking responsibility for themselves has worked for decades and this additional information will provide no protection. "The evidence that this adds to surety isn't there."

Cleland says when an engineer produces a statement they've done the work properly, they're essentially verifying that they have the necessary competence to undertake this task and that there are reasonable grounds to believe it complies with the Building Code.

If an engineer undertakes work for which they are not competent they are in ethical breech. "If they're a Chartered Professional Engineer they can be pursued through a disciplinary case."

If the NZ Fire Service is receiving design documents submitted by a Chartered Professional Engineer (CPE) that are not competent they should name that person. "Send us the work and say we have evidence of non-competent work, then we as the registration authority can pursue that person."

Cleland says IPENZ has tried to provide guidelines for good practice and brings its engineers back for reassessment every two years but that doesn't mean they'll always be practicing competently.

IPENZ has recommended to all building compliance authorities that any engineering work be submitted by a CPE. "They should only take work from people over whom there is jurisdiction."

As far as qualifications go, he says IPENZ assesses all engineers on their specialisation. "They need to show the knowledge and skills and we appoint a panel of their peers to do an assessment."

He says there's nothing in the law that stops anyone putting up a sign to say they're a fire engineer but if a BCA accepts their design that's their choice. "If it involves an alternative design we are saying choose a Chartered Professional Engineer. That way if they submit poor quality work then there's method of dealing with this."

While IPENZ does a valuable job, Davis from the NZ Fire Service, says local government officials administering the Building Act need to know where people's competencies lie. "That's why an industry body needs to take up this role."

IPENZ CEO Cleland says his organisation will review the matter again because there's a stronger call for it but "there's a small amount of value for many perverse outcomes that can apply."

Interlogix TS1162
3-LED Arming Station

The new Interlogix **TS1162** 3-LED Arming Station is now available from Hillsec. The TS1162 arming station can be connected directly to the Challenger RS-485 LAN, up to 1.5km from the Challenger panel or Intelligent Access Controller.

It has an input for request to exit (RTE) control and an open collector output that can be used to control a door relay or door strike. The **TS1162's** performance and robust construction make it suitable for a wide range of applications, including dusty or wet environments (rated to IP67). It may be used as a Challenger system remote arming station. The unique design of the housing allows the keypad to be used in the most demanding surroundings. It can be installed directly onto a metal surface without insulation.

For more information, call or visit your local Hillsec branch today.

For all product information visit
www.hillsec.co.nz

Hills VoiceNav Lite
A security system that talks to you!!

The Hills VoiceNav Lite sets a new benchmark as an affordable, speech enabled, 16 zone LED code pad that is compatible with all Hills Reliance control panels. Encased in an elegant and slim profile design with individually illuminated soft touch keys, the VoiceNav Lite is perfectly suited for all residential and commercial applications, requiring up to 16 zones of control.

The VoiceNav Lite comes well equipped with essential features, such as the unique built-in "personal voice guide" (PVG). The built-in personal voice guide enables users to control their security system with ease through the use of smart voice prompts, eliminating the need to decipher confusing flashing lights or referring back to lengthy user manuals. The VoiceNav Lite's speech engine capabilities provide users with an exciting experience, not previously available in any standalone LED code pads.

Keen to find out more? Visit or contact your local Hillsec branch today for a quick run through of the VoiceNav Lite's extensive features.

For all product information visit
www.hillsec.co.nz

UTP IP Extenders

Vigitron's new high speed Ethernet extenders for coax and UTP cable with extended Pass Through PoE

Vigitron's MaxiiCopper™ Vi2300 UTP IP extenders bring new performance standards to the growing need for high speed full bandwidth IP data and power over extended distances. Symmetric Bandwidth (SBW™) assures full bandwidth is available over the entire operating distance for both uploads and downloads with virtually no packet information loss. Signal transmission and power transmission can be extended up to 914m. Multiple remote site devices such as Megapixel cameras or VoIP can be transmitted on a single cable using the Vi2804 fixed managed MaxiiCollector network switch with up to 64 devices transmitted on just 16 cables. Extended Pass Through PoE (EPTP™) eliminates the need for separate device and transceiver power supplies and power sources saving valuable installation time and money. Type tested to NEMA-TS 2 testing standard, operating under extreme temperature conditions of -40C to + 75C results in the perfect solution for warehouse, parking lot, loading dock and other type of perimeter applications.

The Vigitron Coax IP extenders is also available. Vigitron's MaxiiCopper™ Vi2400 media converter and IP extender provides cost saving solutions for converting analogue security systems to IP by eliminating the need to run new cabling.

For more information, contact your Hillsec branch.

For all product information visit
www.hillsec.co.nz

INTERLOCK™
ASSA ABLOY
IRDL Electronic Roller Door Lock

The Interlock Electronic Roller Door Lock is a low voltage, high torque motorised bolt suited for securing large rolling, tilting, hinged or sliding doors.

- Multi-voltage input (12-24VDC)
- Multiple locking attempts with fail alarm
- Selectable automatic locking upon door closure
- Selectable Fail Safe/Fail Secure
- Bolt position sensors
- Concealed wiring through the base or via a 20mm wiring gland (not supplied)
- Key secured cover
- Floor or wall mounting
- Designed and assembled in New Zealand

Distributed by Atlas Gentech (NZ) Ltd
Freephone: 0800 732 637

SONiM
BUILT FOR LIFE™
Maker of the world's toughest mobile phone

Man-down sensor that automatically signals an alarm and provides continuous GPS tracking if security or if personnel needs assistance or is in trouble.

3-YEAR WARRANTY

EXTRA-LONG BATTERY LIFE
Up to 18 hours talk-time or 1 month standby with continuous use of GPS-based applications.

WATER SUBMERSIBLE
Fully submersed in fresh and salt water at a depth of 1m for 30 minutes.

DROP/IMPACT RESISTANT
Designed to withstand 2 meter drops onto concrete or hard surfaces.

Distributed exclusively in NZ through:
Atlas Gentech (NZ) Ltd
Freephone: 0800 732 637

PARADOX®
SECURITY SYSTEMS
MAGELLAN™
WC588P Wireless Carbon Monoxide Detector

- Highly sensitive electrochemical carbon monoxide sensor
- DC battery operated wireless alarm
- Compact, low-profile design
- Built-in siren
- Available in 433MHz or 868MHz
- Protection against the ingress of foreign bodies / Insect Guard
- Anti-tamper sensor
- Test / Hush button
- LED operation indicator
- Low battery indicator
- Easy installation
- CE and EN 50291 certified

Distributed exclusively in NZ through:
Atlas Gentech (NZ) Ltd
Freephone: 0800 732 637

www.atlasgentech.co.nz

Connect with your customers

DESIGN   VIDEOS   WEBSITES   COPYWRITING

MosaicMedia.co.nz

09 426 2050

Having trouble winning
TENDERS?

Log into our website

Compare the specs of these **vivotek** IP cameras against other brands

Then look at the price!!

www.securityimports.co.nz

IP8362
Network Bullet Camera

- 2-Megapixel CMOS Sensor
- Up to 30 fps @ 1080p Full HD
- 3 ~ 9 mm Vari-focal, Auto-iris Lens
- Removable IR-cut Filter for Day & Night Function
- Built-in IR Illuminators, Effective up to 20 Meters
- Real-time H.264, MPEG-4, and MJPEG Compression (Triple Codec)
- WDR Enhancement for Unparalleled Visibility in Extremely Bright or Dark Environments
- Weather-proof IP67-rated Housing
- Built-in 802.3af Compliant PoE
- Built-in Micro SD/SDHC Card Slot for On-board Storage
- Mounting Bracket with Cable Management for Protected Installation

IP8151/51P
Fixed Network Camera

- CS- or C-mount Adjustment Ring for Flexible Lens Installation
- Built-in 802.3af Compliant PoE
- 1.3-megapixel CMOS Sensor
- Supreme Night Visibility
- Up to 30 fps @ 1280x1024 (1.3MP)
- 3.1 ~ 8 mm Vari-focal, Auto-iris Lens (IP8151)
  3.1 ~ 8 mm Vari-focal, P-iris Lens (IP8151P)
- Removable IR-cut Filter for Day and Night Function
- Built-in Focus Assist Button for Precise Focus Adjustment (IP8151P only)
- Supports WDR Enhancement for Unparalleled Visibility in Extremely Bright or Dark Environments
- Real-time H.264, MPEG-4 and MJPEG Compression (Triple Codec)
- Multiple Simultaneous Streams
- Built-in SD/SDHC Card Slot for On-board Storage*

Distributed by:

SECURITY IMPORTS

You will be amazed at the quality and we are happy for you to personally bench test.

CONDITIONS APPLY:

www.securityimports.co.nz   sales@securityimports.co.nz

Dunedin Office
11 Wharf street
Dunedin
+64 (0) 21 776238

Auckland Office
5 Arawa Street
Grafton Auckland
+64 (0) 9 2152300