

April/May 2014

ISSN 1175/2149

NZSecurity



LOKTRONIC

25 years and still going strong

Public Key Infrastructure

underutilised and a little misunderstood?

Leadership Development

Key to Boost Public Sector Performance

Haumoana brigade

More than wet stuff on the hot stuff

To win an
iPad Air

and many other quality gifts

go to
page 7

www.NewZealandSecurity.co.nz

your electromagnetic locking specialist!

**Underpinned by
25 year's
experience
and service with
integrity.**

Standard features include:

- Field-selectable 12 & 24 VDC options
- 300/550/750 kg holding force options
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless steel nut
- Full protection against transients.

Options include:

- Door Position Switch
- End-to-end Magnetic Bond Sensor
- Header extension angle bracket
- Custom full width housings
- Z/L brackets for inward opening doors
- Frameless glass door brackets
- Powder coated or anodised colours
- Stainless indoor, outdoor and gate locks

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

10
YEAR
GUARANTEE

25yrs
LNZ
Produced and Tested in NZ • Loktronic Products

He's not the only one with
superior night vision.

Introducing Bosch Starlight HD cameras.



Be wise and choose the most light-sensitive HD cameras on the market. The new DINION starlight HD 720P and FLEXIDOME starlight HD 720p RD/VR are the next real breakthrough in HD security. In poor light these amazing HD cameras deliver a clear colour image where others show only black and white. And in extreme low-light they deliver a black and white image where

others show no image at all! Add the Bosch Video Security app and overcome the bandwidth barrier so you can view HD images from anywhere. See video security in a new light at www.boschsecurity.com.au



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

Contact Details

Craig Flint

Telephone: (64) 07 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Crescent

Te Puru 3575

RD5

Thames

New Zealand

All enquiries to

craig@newzealandsecurity.co.nz

Editorial contributions welcome.

June-July

Wholesalers and Manufacturers

Perimeter Protection, Alarms, ID

Management

August/September

Banking, Insurance and Finance

Loss Prevention, Industry Training

Disclaimer: The information contained in this publication is given in good faith and has been derived from sources believed to be reliable and accurate. However, neither the publishers nor any person involved in the preparation of this publication accept any form of liability whatsoever for its contents including advertisements, editorials, opinions, advice or information or for any consequences from its use.

Copyright: No article or part thereof may be reproduced without prior consent of the publisher.

ENJOY a **10 year** guarantee*
on Loktronic Indoor
Electromagnetic Locks!

*Standard terms & conditions of sale apply

Loktronic

0800 367 565

www.loktronic.co.nz

CONTENTS

Security

- 6 Loktronic - 25 years and still going strong
- 10 Public Key Infrastructure
- 12 OPS joins AXIS distributors in NZ
- 14 Hills Electronic Security is on the move in Auckland
- 16 Secured Signing
- 18 The Dropbox problem
- 19 New Briton floor spring range
- 20 Leadership Development
- 22 Stadium Security
- 23 No Excuses
- 24 Commute safely
- 26 Top 10 access control trends for 2014
- 31 Upgraded intercoms and remotes for electric gates
- 32 A leader that likes to push the envelope
- 35 New focus on access management in the rural sector
- 36 Zone Technology
- 38 Thermal imaging allows for accurate and time-saving inspections
- 40 Medical Alarm Monitoring
- 42 Product Showcase

Fire

- 44 Communication breakdown
- 49 Smoke is the killer
- 50 Compliance shortcuts challenged
- 52 Community focus for Haumoana brigade
- 56 FLIR optical gas imaging camera

Associations



www.NewZealandSecurity.co.nz



When you're responsible for the safety and security of an urban public transport system involving hundreds of stations, the amount of incidents to detect, evaluate and act on every day is staggering.

Wouldn't you want a central surveillance system with smart tools to help you quickly and confidently make the right decisions to minimize vandalism and service disruptions and attract more passengers? Tools like automatic alerts and

sharable live video from all parts of the transit system — stations, depots, infrastructure and even wirelessly from rolling stock — with HDTV clarity?

We thought you would. That's why we've made sure our network video solutions can handle it all. So you can make the right decision. For every incident.

Visit www.axis.com/stations or contact Axis at contact-sap@axis.com for more info.



Axis offers dedicated surveillance solutions for all transportation environments • Vibration-resistant onboard cameras and recorders • Vandal-resistant indoor and outdoor cameras • Thermal and low-light cameras for effective night surveillance

AXIS
COMMUNICATIONS

Distributed by:

CHANNELTEN
SURVEILLANCE SOLUTIONS

OPS | Open
Platform
Systems



Loktronic

25 Years And Still Going Strong

Twenty five years ago Loktronic Industries Limited started in business.

As the head of the fledgling enterprise, founder Peter Calvert looked for a source which would provide the information that Loktronic needed, a source for their own training purposes and certainly, for their customers. Back then electric locking in New Zealand was comparatively in its infancy. Having come from a managerial role in the pharmaceutical industry, Peter was used to being able to tap into a vast array of information on most every aspect of modern drug therapy. There were quite literally crate loads of information!

To Peter's amazement but predictably, other than manufacturers' instructions there was almost nothing available in New Zealand which described the application and use of the then available electric locks. He remembers calling on many potential clients. Some were quite pointed in their comments and he recalled two in particular that gave him even more impetus and certainly sharpened his focus.

One comment that comes to mind was, "You're dreaming. This 'press a button and watch a door open at a distance' will never catch on in New Zealand. You've been watching too many Hollywood movies."

Another sceptic said, "How much money do you have behind you? If you don't have much you'll go bust in 3 months. If you have a lot you'll go bust in a year. But you will go bust, there's no place for electric locking here."

"Now astonishingly it's 25 years later and collectively we are here with a few bruises, fantastic successes, some character building failures and a huge amount of experience combined with a whole lot of fun," Peter said.

Peter's aim in April 1989 was to create a company differentiated by both quality



*The premise is simple;
if it is branded
Loktronic it is
designed, tested
and produced in
New Zealand
and for that reason
a large proportion of
the Loktronic
branded products have
a 10 year guarantee.*

of product and service. In particular he wanted to set a standard for service that would become the benchmark by which others would be measured.

To that extent Peter is proud that Loktronic still espouses these old fashioned values as it is the combination of quality, price and service that together equal value, which Loktronic proudly stands for.

Loktronic is a totally New Zealand owned company and concentrates entirely on the New Zealand market.

Whilst Loktronic now stock and sell a range of agency products from third party suppliers, it is the Loktronic branded products which have been the cornerstone of their success. The premise is simple; if it is branded Loktronic it is designed, tested and produced in New Zealand and for that reason a large proportion of Loktronic branded products are guaranteed for 10 years.

Loktronic has resisted the trend to manufacture offshore because control

FREE *Gifts*

250

Quality Gifts

for the first 250 clients
to simply email us on...
gift@loktronic.co.nz and
state 'Happy 25th Birthday'

PLUS, you are
then automatically in to...

WIN a fabulous iPad Air

worth \$949

Be quick, entries close
25 May 2014.



AND, talk to us today about
**NEVER TO BE
REPEATED in
25 year deals*.**

Whatever your project,
large or small,
we'll lock in the greatest
of deals for you. Simply place
your order prior to
25 June 2014.

*Offer valid until 25 June 2014.



Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
mail@loktronic.co.nz www.loktronic.co.nz





Loktronic's founder Peter Calvert

of quality is paramount to them. Local contractors are always used which helps to maintain continuity. Control of quality was a key factor in enabling Loktronic to achieve ISO 9001:2008 registration almost 2 years ago.

More recently Loktronic acquired ViTech New Zealand and absorbed ViTech's already successful product



Sandi Hewlett

group into their mix. Ongoing design and enhancement has further developed ViTech products into the robust range that they now market. They listen to what their clients want and develop solutions based on their needs.

Loktronic owes much of its success to the support that it has had from its staff during the last 25 years particularly during the formative stages. One person stands out; Sandi Hewlett, daughter of the late Sid Pemberton, who spent his working life as a locksmith. Sandi has been with Loktronic since the beginning and brought a wealth of skills and fortuitously understood the jargon of the locking world. Sandi manages the office, though can handle nearly every query to do with electric locking.

Peter Sheehan, who founded ViTech New Zealand some 10 years ago, joined Loktronic with the ViTech acquisition. As a registered electrician he has worked in



Peter Sheehan



Eilish O'Brien

and designed products for the security and fire industries over a 25 year span. Peter manages Loktronic's ViTech Division.

Eilish O'Brien joined Loktronic nearly 3 years ago following a successful career in Ireland as a Project Manager for a construction and civil engineering company. She holds both a marketing degree and an honours degree in business management. Eilish is the Technical and Sales Support person.

How has Loktronic performed against its aim of 25 years ago in terms of service and product? Many of their early clients are still in business and regularly purchasing from them so that is indeed confirmation they have things going right.

Peter concludes, "on the product front, there is more to come, so watch this space and share our pride by using the New Zealand made products that we proudly produce."

● CELEBRATING 25 YEARS ● CELEBRATING 25 YEARS ● CELEBRATING 25 YEARS ●

CELEBRATING 25 YEARS

CELEBRATING 25 YEARS

● CELEBRATING 25 YEARS ● CELEBRATING 25 YEARS ● CELEBRATING 25 YEARS ●



**Your security,
our storage.
The power of choice.**

Marc Cisneros

Protector,
Advocate,
Guardian.

362,512 hours recorded,
15,643 cameras strong,
7,453 sequences stored,
2,423 businesses secured,
1,512 clients protected,
1 surveillance solution.



WD Purple™
Surveillance Storage



See more of Marc's solutions at:
wd.com/choice



absolutely™

Public Key Infrastructure (PKI) underutilised and a little misunderstood?

Public Key Infrastructure has been around for some time, but it is still relatively underutilised in New Zealand. Hampering its uptake has been a lack of awareness of how it can be used, and traditionally high implementation costs.

Since IBM launched New Zealand's first hosted PKI service in early 2011, the cost effectiveness of PKI implementation for smaller businesses has improved significantly, with a range of local and offshore hosting services now offering off-the-shelf and tailored PKI solutions to New Zealand businesses.

So what is PKI again? *A quick refresher*
Public key cryptography is a technique that enables users to securely communicate with - and verify the identity of - a user on an insecure public network, such as the internet. It does this through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI is the underlying systems, policies and processes required for the creation, storage and distribution of digital certificates, which are used to verify that a particular public key belongs to a particular entity and to ensure that messages between entities have not been tampered with.

A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange confidential data, such as credit card details, by way of digital certificates. It is also used as a method of ensuring that an executable program available for download from a website has come from a valid software publisher and has not been altered by anyone in between.

Public key cryptography has become the preferred approach for encryption over the Internet due to its advantages over traditional private key forms of cryptography. But it is not without its problems. According to Peter Gutmann,

a professor in computer science and PKI expert at the University of Auckland, most people vastly underestimate the effort and complexity involved in implementing PKI. "It makes things much more complicated," says Professor Gutman, "it's never going to make things simpler, and it can make things less secure."

Indeed, this year alone we have already been confronted with two major PKI-related security flaws. In late February, Apple released updates for iOS 6, iOS 7, and Apple TV to squash a security bug that affected SSL/TLS connections. The "goto fail" bug was the result of a singular stray line of code in a block of code



The Scientific Software and Systems Limited (SSS) team

COMPACT WITHOUT COMPROMISE

When you need Full-HD performance but require a discrete, compact size, the Panasonic SW-158 and SF-138 mini-dome cameras are the perfect solution. Offering a versatile design without compromising Panasonic's renowned picture quality, these cameras will deliver in the most testing environments.



WV-SW158



WV-SF138

COMPACT MINI-DOME CAMERAS

- Full-HD 1080p images up to 30 fps
- 3.1 Megapixels high sensitivity MOS sensor
- SDXC/SDHC/SD Memory card slot
- Built-in Microphone
- VIQS Technology

VIQS TECHNOLOGY: VARIABLE IMAGE QUALITY ON SPECIFIED AREA

VIQS Technology

VIQS technology delivers Full-HD performance, requiring less bandwidth and smaller data storage capacities than conventional cameras. VIQS cameras allow you to vary the compression rate and image quality, so you can record important areas in Full-HD and all other areas at a lower resolution.



Panasonic New Zealand Limited
18 Sir Woolf Fisher Drive, Highbrook
East Tamaki, Auckland 2013, New Zealand
Telephone: 09 272 0100, Facsimile: 09 272 0134

panasonic.co.nz

Panasonic[®]

responsible for validating the identity of a server. This left users vulnerable to a man-in-the-middle attack where a user on the same network could fake a certificate keychain to a secure site, such as a user's bank.

Then there was the uncovering of the GnuTLS bug, which had left the users of Linux and hundreds of applications similarly vulnerable.

A lack of understanding of PKI among NZ businesses

If you didn't know about the goto fail or GnuTLS bugs - or much about PKI at all for that matter - it seems that you're in good company. According to Ashton Jones of Wellington-based IT security developers and resellers Scientific Software and Systems Limited (SSS), "there is an overall lack of PKI understanding, skill

base, and experience in most New Zealand businesses - even in those that are using elements of PKI now."

"The biggest problem we see," comments Ashton, "is people implementing a PKI solution without fully understanding what they are getting themselves into and without first consulting the business and understanding the business requirements. Developing a 'big-picture' overview of your PKI and its intricacies, and understanding the business requirements, are crucial to reducing the technical, implementation and support problems that can occur."

Professor Gutmann observes that PKI is sold as the solution to everything, but it is not the panacea. PKI tries to solve legal problems, for example, such as adding to weight of evidence in court, but the legal aspects of it tend to be oversold. "Look

at the business case and legal case," states Gutmann, "talk to lawyers and question 'do we actually need to do this?'"

SSS, "once you have a PKI infrastructure in place, you can then fairly easily extend it out to other uses such as email signing and/or encryption, application/device/user access or web TLS certificates." Gutmann points out that while PKI is very flexible, what it provides in terms of flexibility it gives up in utility. In a lot of deployments, PKI has either not been worth it or it has not provided what was wanted. For this reason, he states, most PKI deployments don't end up working out. The question is 'what do you need PKI for'? A case-by-case basis is required. One needs to apply a cautious approach and conduct a feasibility study.

A complex and expensive solution?

Typically, notes SSS' Ashton Jones, the more simple PKI deployments are for internal use and things can start to get complex when organisations need to cater for external customers/website users and the like. "The increased needs around trust/integrity of the Certificate Authority," states Ashton, "can very quickly increase the overall cost and complexity of your PKI environment." This is particularly the case in relation to certificate issuing and revocation.

Ironically, the complexity of PKI also means potential exposure to unanticipated security risk. Many NZ organisations have set up an internal CA and or PKI infrastructure, observes Jaco van der Westhuizen, a consultant with Auckland-based IT distribution specialist MPA, and for most, these key infrastructures are critical to specific projects. However, they are often unplanned, unsecured and unmanaged, which means the business should view them as a security risk. When deploying Certificate Authority, for example he notes "a key consideration is protection of the CA root keys and maintaining the integrity of the resultant PKI, certificates, and PKI dependent applications." According to Jaco, this area is of particular concern in New Zealand as a number organisations have not gone to this level of protection compared to other global PKI implementations.

So, is PKI the way to go for businesses, or is there a better option? According to SSS, it really depends on the problem a customer is trying to solve. If a business just has one or two fairly narrowly defined needs that could be solved by

Axis extends OPS distributor agreement into NZ

OPS will join Axis' existing distributors in NZ and will deal with the full suite of Axis products in the country

Axis Communications and Open Platform Systems (OPS), an Australian value-added distributor of IT network access equipment, have extended their distribution agreement into the New Zealand market, effective immediately.

The announcement follows a successful partnership between the two companies in the Australian market since 2011.

By the terms of the agreement, OPS will join Axis' existing NZ distributors, and will be distributing the full suite of Axis products in the country.

"Axis Communications' products are a welcome addition to our growing New Zealand portfolio. The extension of our relationship with Axis Communications reflects the increasing demand for IP network cameras from our partners servicing a range of industries and sectors in New Zealand," said Kobi Ben-Shabat, MD of OPS.

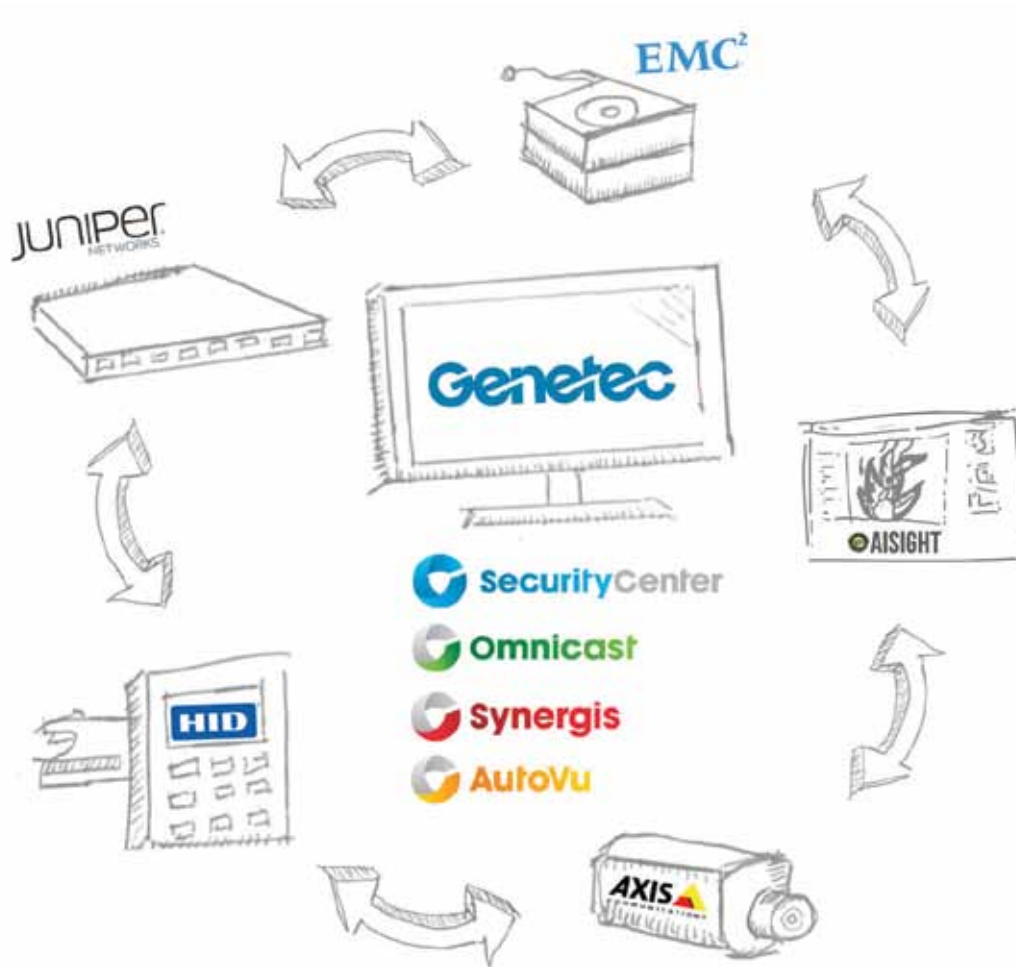
Wai King Wong, country manager for the Oceania region at Axis Communications commented, "The CCTV and video surveillance market is headed in a direction where revenue for network video is expected to overtake analogue for the first time ever. This growing demand is reflected in the extension of our distribution agreement with OPS into the New Zealand market.

OPS enables its partners to tailor solutions to match their customers' exact needs - providing end-to-end solutions across multiple technologies to suit all applications. OPS also provides support services that are second to none. This commitment to exceptional customer service is one of the main reasons we have hand-picked OPS to distribute Axis products across the region." Wong concluded.



Open
Platform
Systems

YOUR TURN-KEY SOLUTIONS PARTNER



Today's security world is challenging. Your customers no longer want discrete products. They expect complete end-to-end solutions.

We believe that our unique approach to unified security is the key.

OPS is your preferred Physical and Logical security systems distributor, whether your client is a small business or a large enterprise.

To get in contact with Open Platform Systems today call your nearest branch or visit www.opsystems.com.au



Physical Security
Cyber Security



Stratocast



PKI, a non-PKI point solution might in fact be a better approach for them. "For example, if you just want a tidy authentication solution, the use of PKI and digital certificates may be more complicated than what you need for that." Another example, states SSS, "is encryption of data at rest - while PKI could resolve this problem for you, there are probably more cost effective point solutions available for that."

Several PKI model options

The range of PKI hosting models now available to businesses has helped to counter the awareness and expense problems associated with PKI, with outsourced models bringing PKI within the financial reach of small businesses.

SSS: There are now online managed services that can offer a relatively straightforward medium for companies to establish a trusted PKI without the overhead building the trust internally. Australian IT security and PKI consulting firm Castelain identifies the three major models as follows:

- **Certificate Vendor Model** – The outsourcer can simply act as a certificate vendor, providing certificates from their PKI to perform all registration and identity checks. In this model, the outsourcer tends to charge for certificate issue and takes some liability in instances where it is shown to have been negligent in verifying a subject's identity prior to issuing a certificate.
- **Client Branded Outsourced PKI Model** – The outsourcer uses their own product to build and host parts

or all of a client's PKI system. The PKI is operated by the outsourcer but branded as being the client's own. Given that the outsourcer is typically making use of their existing hosting environment, this model results in a comparatively low establishment cost. Apart from a setup fee to establish the system, clients pay a clickcharge per certificate issue.

- **Unbranded Outsourced PKI Model** – The outsourcer builds a PKI system and offers certificates for sale to corporations willing to undertake their own registration checks. The certificates are generally not client branded and the client accepts liability for their use. The client is subject to a similar fee structure to the Client branded outsourced model.

While outsourcing has no doubt reduced the complexity and costs of PKI to businesses, this doesn't necessarily mean that things won't go wrong with a hosted PKI service. According to Castelain, each model presents its own pros and cons.

For instance, private sector companies can go broke or be acquired; they can potentially sell the business unit responsible for providing the PKI hosting service, adopt alternative products, or decide for commercial reasons to exit the hosting business. There is the potential here for serious disruption and reintegration costs. Similarly, observes Castelain, if the software provided by the outsourcer is no longer supported, the client is forced to switch products and there is

the expense of reintegration and testing. There is also a lack of control over management of any software bugs and associated outages.

Lessons learnt

The market's experience with PKI provides for a number of lessons learnt, and the underlying lack of PKI knowledge out there among businesses suggests that businesses need to be more proactive in approaching the issue.

Professor Gutmann points out that businesses need to understand the problems they need solving and whether PKI provides for the simplest and most cost-effective solution. "PKI for PKI's sake is not generally a good idea," he points out, "you need a specific problem to solve." Similarly, Ashton Jones suggests that a business should find out more about the technology 'before you leap into it', and talk to a specialised vendor about the types of problems that PKI can address.

"If you develop clear goals of what you would like it to achieve in the short term, identify potential future uses down the road, and get expert advice/assistance at the outset," states Ashton, "you should be able to achieve a strategically useful, well-fitting PKI solution for your organisation."

While the perspectives on PKI may differ, the experts appear to agree on the point that blindly assuming PKI will provide the silver bullet solution is a recipe for failure. Do your research in advance. You don't need to know all there is to know about PKI - there are consultancy and hosting services out there who can help, but understand your problem and investigate the range of solutions that are available.

Hills Electronic Security has moved in Auckland



A Hills NZ business

Hills Electronic Security have recently joined SVL, A&TV and Hills Home Living in the new Hills premises in Mt Wellington.

Situated at 15C Vestey Drive, it gives us a greater space to warehouse our entire product offering and with a new innovation space due for completion in the next couple of months, we will soon

have a space in which to showcase the latest technology from all divisions.

Part of our new facility includes a spacious new training room with the capacity to host up to 24 guests and as with the showroom, the training room will feature the latest sound, video and lighting equipment from our Hills SVL division.

This move also signals the unification of Hills. The individual businesses you've known and trusted for years are a part of Hills, the leader in integrated technology solutions. The largest range, best service and most trusted solutions now have one name.

For more info on Hills Electronic Security go to www.hillsec.co.nz.



NEW FC-Series S



Don't call security.
Call FLIR for the complete picture.



Compact D-Series

If your security system is all bells and whistles but can't show you whether it's a possum or a person climbing your perimeter fence then FLIR's new range of thermal imaging security cameras will give you a much clearer picture.

Available in a wide range of performance models including the new FC-Series S and the new Compact D-Series outdoor domes, the FLIR network-ready camera range is now more affordable than ever for your surveillance and security applications.

Whatever mother nature dishes out - blinding sun, fog, smoke, pouring rain or complete darkness - FLIR fixed-mount cameras deliver the sharpest thermal images known to man, day or night.

Here's how:



High contrast scene with standard AGC algorithm applied.



DDE applied – all targets can be observed simultaneously.



Crisp Thermal Images - More pixels allow the user to see more detail in even smaller objects at a greater distance. Choose which resolution of crisp image quality you need: 640 x 480, 320 x 240 or 160 x 120 pixels.



Excellent Range - FLIR thermal imaging cameras can detect targets several kilometres away.



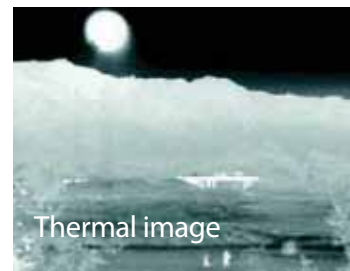
Digital Detail Enhancement - Providing high contrast imagery in almost all weathers optimised for video analytics software.



Wide Dynamic Range - Delivering high quality images even when full sun is in the field of view. Ideal for working with video analytics.

Your vision

Thermal image without Wide Dynamic Range (WDR).



Thermal image with Wide Dynamic Range (WDR).

www.flir.com

For more information about the about the new FC-Series S and Compact D-Series or any other FLIR thermal imaging camera please contact:

FLIR Systems Pty Ltd. Free Call NZ: 0800 785 492

Email: info@flir.com.au

Secure Signing a step closer to the paperless office?

Internet-based secure digital signature services provide a platform for the signing of documents online using secure PKI digital signature technology. Apart from maximizing document security in terms of authentication, tampering and non-repudiation, it would appear that secure signing provides the potential to eliminate paper, printers and couriers from B2B document-based transactions altogether. Yet, as things stand, uptake among New Zealand businesses is negligible.

Documents often sent using secure signing include contracts, non-disclosure agreements, proposal acceptances, change orders, advertisement proofs, expense reports, purchase orders, rental/lease agreements, independent contractor agreements, time sheets, and so on. Using the service, a registered user receives a unique private key for signing, they then add a document to the system, sign it digitally, invite a third party if required and then send the document to relevant parties for their signature. Parties in the signing process are able to verify signatures on their desktop.

Mike Eyal, Managing Director of Secured Signing, a web-based digital signatures service based in Auckland, comments that while traditional approaches to PKI digital signatures have been too complex and expensive, costs have dropped and are now within reach of consumers due to the sharing of provider infrastructure. "Secured Signing's clients share our infrastructure and use tools developed by us to sign documents via a

workflow interface that is customised for or configurable by the client", stated Mike during a recent interview with the NZSM.

A secure, legally-binding solution?

As a rule, the law tends to lag behind technological innovation, and within the current New Zealand legal context, documents such as wills, documents transferring an interest in land, powers of attorney, and deeds must be signed on paper rather than online.

That being said, there is a wide range of documents for which secure digital signing meets the requirements of New Zealand's Electronic Transaction Act 2002, but care must be taken in selecting the right approach. PKI-based document signing has tended to follow one of either two approaches:

- (i) Systems based: document is signed with an electronic signature. Only once a document is exported is it sealed, and up until that point it is vulnerable to tampering.
- (ii) User-based: signatory signs with PKI keys (digital signature) and the document is sealed from that point on (in, for example, PDF format).

Cautioning against use of the first approach, Mike comments that only user-based (digital) PKI provides for the security necessary to comply with legislative requirements, but that businesses tend to lack knowledge of which solution to go with.

A digital signature is in effect a "fingerprint" that is unique to both the document and the signer and binds both of them together, ensuring the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. Digital signatures sustain signer authenticity, accountability, data integrity and non-repudiation.

To this end, proponents of secure signing services argue that their platforms provide for even greater security - and therefore legal enforceability - than physically signed paper documents. Ink signatures can be replicated from one document to another by copying

the image, but digital signatures cannot be copied between documents. Digital signatures can also be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered.

Workflow and efficiency considerations

Mike notes growing interest in PKI digital signatures as more people start to understand how it all works. "The driver for uptake is efficiency and productivity and how one can do more with less and speed up the process," states Mike. But there remains both a lack of knowledge and a lack of awareness that this can be done online. "The issue we're struggling with," Mike continues, "is that businesses don't know; they find the traditional ways difficult to move away from."

As a workflow solution, the potential advantages of online document signing are self-evident, but the efficiencies derived are dependent on what type of secured signing platform a business selects. Common off-the-shelf options include either:

- (i) Look-alike forms, which involve email invitations to signatories and the positioning of 'sign here' tabs on forms that mimic their paper equivalents; or
- (ii) Business rules-based forms that allow validation to occur prior to signing.

In cases where documents are hundreds of pages long and require signing of multiple copies, the use of business rules-based forms in particular has the potential to dramatically speed up the signing process. Document delivery via email notification obviates the need for couriers, and no paper means no printing and - potentially - no physical paper file storage. Associated supporting documents can be uploaded to a secure signing system by taking a picture with a smart phone.

The potential for the secure digital signing is massive, states Mike, "but businesses need to know that the solution exists and to change their mindsets from paper trail to online."



Mike Eyal is the Managing Director of Secured Signing



Open Platform VMS by AxxonSoft



SolidStore



Micro-Module architecture



MomentQuest2



Interactive 3D Map



Time Compressor



Video Analytics



Information boards



User comments



Map with embedded
live video thumbnails



Saving and quick access to queries
for MomentQuest2 forensic search



OpenStreetMap
integration



www.axxonnext.com

CRK
Professional Precision

axxon
Experience The Next®

ph: 09 276 3271 | fax: 09 276 9645 | email: cctv@crknz.co.nz | web: www.crknz.co.nz

The Dropbox Problem

By Laureen Smith, VP Asia Pacific, Workshare

In response to the highly publicised data breach problems Dropbox has caused organisations around the world, Laureen Smith, Vice President of Asia Pacific at Workshare, would like to share the secure enterprise collaboration vendor's views.

Consumers use Dropbox for sharing and storing all kinds of files on all their different computers, tablets and smartphones, between friends, with colleagues or clients, whether they are at home or work. This is because these services are freely available, don't cost anything and are very easy to use. Dropbox was originally designed and developed for individuals to quickly and easily share their personal photos, videos and other documents by dropping them into their Dropbox folder, but it has been adopted in many workplaces as the way to share corporate files with other people or devices.

The problem with Dropbox being used in the workplace is that it is a consumer-grade application, which is self-provisioned and owned by the user. Essentially, there are two major problems with that; the primary concern is security and the issue with that is twofold:

1. Employees access their corporate data via Dropbox and other consumer applications that do not have sufficient security built in.
2. Personal devices that do not have the right level of security in place to prevent unauthorised access, in case of loss or theft, are being used to access company data.

Secondly, if an employee leaves an organisation, they walk out of the door with valuable corporate data in their personal Dropbox account and nobody can do anything about it.

Aware of these issues, Dropbox has built in security measures to try and prevent unauthorised access. However, it is the simple, day-to-day mistakes you can

make while using Dropbox that makes your sensitive corporate data vulnerable. Dropbox is specifically designed to make it easy to share and unfortunately, this is at the expense of data security.

Worryingly, vast numbers of people are now using personal Dropbox accounts in the workplace, with many using it without authorisation from their employer. For organisations, being able to set clear policy for how corporate documents and information is shared and used is paramount, especially for those in semi and highly regulated sectors.

It's a well-known fact that many personal information security breaches are caused by user error. Without policy enforcement to set access rights for users and metadata stripping capabilities to remove hidden data before a document is shared, users are at risk of inadvertently sharing confidential or sensitive documents via Dropbox. For example, users can share files with open links using the drag and drop action. Anyone can then access the content even when the link is forwarded. Further still, there is no audit trail and the 'owner' of the document has no way of knowing who has been given access to a document and who has actually opened it. Dropbox's integrations with third party consumer apps including Facebook and Twitter could also allow content to go viral.

Over 200 million people have a personal Dropbox account and many of these people now have work and personal folders sitting side by side in their Dropbox applications on their desktop, laptop, tablet and mobile phone. Dropbox recently moved to allow these consumers to sort these into groups, but this does not address the core security issues.

Another major problem with using Dropbox in the corporate environment is the lack of collaboration functionality, and often individuals will have documents in their individual Dropbox folders that

are not shared with others and may not be the latest versions. Even if the documents are shared amongst a team, if two of those people both open and edit a file in a shared folder at the same time, Dropbox will save both of their changes in separate documents.

The additional enterprise level attributes that Dropbox does not provide, but companies expect from a supplier include Service Level Agreements with minimum levels of security and availability guaranteed in writing, a strong global network of resellers, professional account management, and 24/7/365 support.

In addition, to be compliant with the Australian Privacy Legislation coming into effect on March 12th, organisations with revenues over \$3 million should be using enterprise-grade applications that can prevent inadvertently leaking sensitive data, personal identifiable information, and intellectual property contained in sensitive documents. Using these enterprise services to automate the management of what goes out of organisations and controlling who sees and accesses it once it is sent externally is the way to avoid being penalised for a data breach.

Finally, if the location of data storage is a concern for an organisation, particularly in light of the new privacy legislation, being able to choose exactly where data is stored and what jurisdiction it falls under will be crucial. With many of the major providers having data centres in the West-Coast of the USA, finding providers with local data centres in Australia is one of the challenges local businesses find. However, this should not be something organisations compromise on.

Workshare has data location services in Australia and Asia. In Asia Pacific, data can be isolated to data locations in Sydney, Singapore, or Tokyo. For organisations and IT, this addresses data sovereignty, privacy legislation, and latency concerns.

New Briton Floor Spring Range

Allegion is proud to introduce two new series of floor springs to its range – the Briton 5000 and 7500 series

The 5000 series replaces the current Briton M5000 series. Designed for heavy traffic, single or double pivoting application doors, the Briton 5000 series floor spring offers compact design and low profile cement case where floor depth is limited. The Briton 5000 series floor spring consists of a high-grade cast iron body, available in two strength sizes 3 and 4. The securely designed speed-adjustment valves protect the spring mechanism from abuse and adverse weather conditions and the internal mechanism components utilise heat-treated high-alloy steels and ball bearings for optimum efficiency. The 5000 series floor spring is suitable for use with timber, metal and tempered glass doors up to 100kg.

The 7500 series replaces the Briton M8000 series. Designed for heavy traffic, single or double pivoting application doors, the Briton 7500 series floor spring from Allegion offers improved adjustability and versatility. The Briton 7500 series floor spring consists of a high-grade cast iron body, which is power adjustable sizes 3 to 6, allowing



onsite adjustment to suit the prevailing conditions. The securely designed speed-adjustment valves protect the spring mechanism from abuse and adverse weather conditions and the internal mechanism components utilise heat-treated high-alloy steels and ball bearings for optimum efficiency.

The 7500 series floor spring is suitable for use with timber, metal and tempered glass doors up to 300kg.

**For more information, contact
Allegion (New Zealand) Limited
on 0800 477 869 or
www.allegion.co.nz**



- Keypad, proximity cards and magnetic stripe card options available
- Convenient and secure
- User friendly
- Open platform
- Up to 2000 users
- Stand alone, full access control

www.allegion.co.nz



Leadership Development

Key to Boost Public Sector Performance

The New Zealand public sector is highly regarded internationally. It consistently leads the world in terms of strong trusted institutions. We are a world leader in terms of perception of the absence of corruption in government. The World Bank rates New Zealand as fifth highest in terms of government effectiveness – ahead of many of the countries against which we are traditionally benchmarked (Australia is 10th and the UK at 15th). The satisfaction expressed by New Zealand in its public services also is very high against international benchmarks.

However, in a world that is growing more and more uncertain, with rapid

social change, technological innovation, big data and rising citizens' expectations, the case for change and continuous improvement even for a world class public sector is needed.

To meet these complex challenges successfully, there are key shifts we need to make and one of these is leadership development.

A recent report released by the State Services Commission (SSC) entitled "Getting to Great: Your map to navigating the straits of internal leadership," found that leadership development now needs to be a focus to boost public sector performance and to build enduring great public institutions.

Knowing the key role of internal leadership in the transformation of the State sector, I wanted to identify successful approaches that could be shared with current leaders and aspiring leaders across the public sector. I wanted to see specific examples of what can be achieved with strong leadership focussed on building high performing public institutions. Thus, this Getting to Great report. This report aims to give State sector leaders tools and strategies to improve their leadership and engage and empower their staff.

The second in the Getting to Great series, the report analysed findings in the area of Internal Leadership in the Performance Improvement Framework* (PIF) reviews of 29 government agencies. The goal was to identify best practices and share them across the State sector.

Included in the report are 32 filmed interviews, case studies, a toolkit and recommended readings. Chief executives

and senior leaders whose agencies' are regarded as strong performers share their success stories, and how and why they are successful. It also includes advice on how to build a high performance culture from 2013 New Zealand Entrepreneur of the Year and Xero Chief Executive Rod Drury. It also draws insight from Public Service Association National Secretary Richard Wagstaff on how to work with union representatives.

The report was designed for everyone interested in how to navigate the leadership pipeline - from graduates through to chief executives. Over the next six to twelve months, workshops and seminars will be delivered to over 1,000 State servants. The workshops have been designed for graduates, emerging leaders, first-time team leaders and first-time general managers. A seminar series has also been designed for HR and OD professionals working in the New Zealand State services.

KEY FINDINGS

There are five key findings at the core of the report: the importance of authentic leadership; using organisational culture as a key enabler; demanding high quality HR analytics; meaningful feedback to staff; and understanding the link between staff and customer engagement. Each of these ideas is central to creating more effective, affordable and legitimate public institutions.

Value authentic leadership:

The strongest performing agencies value authentic leadership. High performing senior leadership teams and Boards



State Services Commissioner Iain Rennie

create an organisational spirit that in turn encourages staff to produce discretionary effort, take risks and innovate. These agencies have authentic leaders who are confident to show their 'whole-self' at work, including admitting mistakes and leading with head and heart.

Create alignment between role, purpose and organisational culture:

The best performing agencies create alignment so that individuals don't default to their personal sense of mission, which may or may not align to agency strategy and required results. This in turn enables a culture where employees can influence what they need to influence to get their job done, thus infusing the agency with a culture and sense that anything is possible.

Embed workforce analytics:

The best performing agencies use workforce analytics, and ensure they are regularly reported and debated at the top table. In practice this means reliable, clean data is being used to create real value, both financial and nonfinancial.

Provide meaningful and timely feedback:

Great leaders develop other leaders. The best performing agencies approach performance management as a way to develop their people – both for their agency and for the system. These agencies approach people management as an ongoing dialogue, characterised by regular high quality feedback.

Reach for higher staff engagement:

The best performing agencies understand that their people want to be trusted and given the discretion and tools to perform. The best agencies then use a combination of clarity in purpose and strategy to create high levels of engagement, which in turn, is used to liberate people to lift productivity and, ultimately, client satisfaction and citizens' trust and confidence.

The report concludes that "the integrity and performance of New Zealand's public institutions - and of the individuals attracted to public service - is the cornerstone of good government. While New Zealand public institutions hold

themselves to high standards of integrity and performance, the way we lead people needs to be improved. In order to make superior performance both common and enduring, much greater attention needs to be placed on building strong public institutions by leading people better."

Clearly, effective and skilled leadership is essential to boost State sector performance and deliver better public services now and into the future.

In varying degrees, these five ideas are already making a difference in some agencies. But, as all the international surveys tell us, there are no easy yards. They require support from the political leadership, willingness to reform and a readiness to try things that haven't been tried before, and to quickly jettison ineffective ways of working. The payoff—effective and affordable government that can address long-standing, complex issues and deliver better public services, will be more than worth the effort.

For a full copy of the report, visit <http://www.ssc.govt.nz/getting-to-great-internal-leadership>.

** Performance Improvement Framework (PIF) is a review of an agency's fitness-for-purpose today and for the future. Using the PIF Agency Model, a PIF Review looks at the current state of an agency and how well placed it is to deal with the issues that confront it in the medium-term future. It then proposes areas where the agency needs to do the most work to make itself fit-for-purpose and fit-for-the-future.*



ITPLUS

YOUR TECHNOLOGY PARTNER

Surveillance specialists with a complete range of CCTV products for distribution

www.itplus.co.nz

Telephone: 09 950 4940 • Unit 9A, 9-11, Laidlaw Way, East Tamaki, Auckland • Email: info@itplus.co.nz

Stadium Security

balance visitor safety with visitor enjoyment

Protecting sporting events where large groups of people gather has been at the forefront of the security industry of late, especially with the recent completion of Super Bowl XLVIII at MetLife Stadium in New Jersey and the 2014 Winter Olympics in Sochi, Russia.

Thousands of miles and continents apart, both events attract thousands of spectators from around the world to cheer on their favorite teams or support their home country. Despite their differences, with the Super Bowl celebrating the big game of one of America's favorite sports and the Winter Olympics celebrating multi-national competition, they both have many commonalities from a security standpoint.

Stadium Security and event security are two of the most challenging security scenarios because they both require calculated combinations of manpower and technology to continuously monitor large groups of people. And even with a series of security checkpoints along the way to scan tickets and to manually check bags and backpacks to guard against banned items, these events still require a continuously watchful eye to quickly

identify problems and ensure crowds do not get out of control.

That's where surveillance technology comes into play. In the last five years, upgrading surveillance in stadiums has been one of the most sought after projects because it provides the ability to remotely monitor an event from a single command center and to proactively respond to an issue before it unfolds.

As part of Panama's preparations to host the 39th Baseball World Cup in 2011, country officials outfitted four baseball stadiums in four different cities with new IP-based surveillance technology, which enabled security personnel to quickly identify problems and maintain control of potential security incidents. With the American Dynamics VideoEdge Network Video Recorder (NVR) and the victor Unified Client as the video management solution, these stadiums were able to monitor live surveillance footage for faster response as well be able to quickly search through recorded video after an incident occurred.

Fenway Park, home to the 2013 World Series Champion Boston Red Sox and



Major League Baseball's oldest stadium, provides yet another example where major upgrades to the surveillance systems at this stadium served as the foundation for a recent, large-scale security improvement project. With 35,000 fans coming in and out of the stadium on game day, it was time for the stadium to install an IP-based surveillance system to improve security's view throughout the entire facility and to protect spectators. Integrating American Dynamics video solutions with Kantech access control, Fenway Park was able to update their security system and poise themselves for future innovation. Watch this great video covering Fenway's latest security upgrade.

Sporting events are not the only large-scale surveillance challenges; take for instance the Hollywood Bowl in California, with an audience over 18,000 and so much talent on display, it represents a daunting security challenge. Every corner of the stage, parking lots, and neighboring freeways are carefully monitored to ensure that people and traffic are moving freely. The stage manager relies heavily upon the live video to ensure the show starts on time, allows him to call for more ushers to move people along, or delay the opening act if necessary.

Next time you attend an event, whether it's a baseball game, football game, or a music concert, you can most certainly expect that surveillance is playing an important role to keep both the facility and spectators safe.



No excuses

Security companies know the who, the what and the where.
What they don't have is an excuse to avoid training their staff to meet the Private Security Personnel training requirements.

Lance Riesterer, Head of commercial industries for The Skills Organisation, says the time is now. "If you want to continue to operate in the security industry after 1 October, all your staff who hold a CoA need to be trained."

The who

The training requirements apply to License and Certificate of Approval holders including crowd controllers, property guards, personal guards and their employers.

The what

Three NZQA unit standards:

- **27364** Demonstrate knowledge of the security industry in the pre-employment context.
- **27360** Demonstrate knowledge of managing conflict situations in a security context.
- **27361** Manage conflict situations in a security context.

The where

There are a range of organisations who are able to provide training to meet the requirements.

The NZSA has a nationwide network of delivery – you can contact them on 09 486 0441, by email info@security.org.nz, or visit www.security.org.nz.

For the full list of training providers go to skills.org.nz. Individual organisations will advise you of costs, delivery method and course dates.

The when

- 30 September 2014 - if you have an existing and current Certificate of Approval (COA).
- 3 months from joining the industry – if you're new to the industry.



**This
affects
you**

**Security
industry training
requirements.
Are you ready?**

**Contact us -
we can help get
you started.**

skills.

The Skills Organisation
info@skills.org.nz
skills.org.nz

The inconspicuous companion

Comprehensive mobile video surveillance system introduced to further improve passenger safety

Mission

MVG provides one of the most modern transport systems in the world. More than 500 million passengers travel every year via bus, tram and six subway lines over a network of 95 kilometers with 100 stations and nearly 580 subway cars in Munich alone. Early in 2008, a call for bids was made to equip the subway trains and streetcars with a video surveillance system. "In this case we had a special requirement that the solution had to run entirely via ethernet and therefore be integrated into the existing ethernet of the train units," explains Kurt Stern, Head of Traffic Telematics for Stadtwerke München GmbH/MVG.

Solution

The Munich-based company Indanet won the bid and was commissioned to equip 358 subway cars and 88 streetcars with a digital video surveillance system. Jurgen Fuchs, Indanet's General Manager responsible for business development, describes the selection criteria for the cameras as follows: "We wanted a compact, rugged IP camera with railway approval for our customers that was easy to install and configure. Of course, it also had to support high-quality video which can be entered as evidence in court to identify offenders." Axis has a special camera in its portfolio for this purpose: AXIS M3113-R. The palm-sized network camera is noted for its robustness and delivers high quality digital video images in spite of the rocking and shaking and the high humidity in mass transportation vehicles.

Result

MVG is pleased with the result. "An example of a successful manhunt was the investigation into property damage caused by graffiti on December 5, 2010 in streetcar 17. The perpetrator and the act were recorded on camera. The images were published in the internal investigation records of the Munich police, which finally led to a policeman's recognizing the perpetrator just days later," says Harald Pickert, head of the Crime Division. The opening of the first section of the Munich subway in 1971 and its subsequent expansion to include the Olympic Stadium for the 1972 Olympic Games, marked the advent of so-called industrial television.



"The Munich police welcome SWM/MVG's gradual expansion of video surveillance in the Munich subway trains, buses and trams. In addition to the preventative aspect, i.e. the curbing of crime, video surveillance also makes an indispensable contribution to the criminal investigation and identification of perpetrators. The better the images, the more chances we have for successful search and identification operations."

Harald Pickert, head of the Crime Division, Police Headquarters, Munich.

At that time, only stationary cameras were installed in the underground stations, primarily to serve operational needs.

By 1980, however, the subway network had grown so much that a central control center for scheduling purposes and station monitoring was put into operation at Marienplatz. To document incidents, each of the five monitoring sites in the subway control center was equipped with a video recorder, which could be started by pressing a button. In February 2004, the subway control center moved from Marienplatz to a new location and was also expanded to become the MVG operations center. The move was also a challenge for the video system. The traffic telematics infrastructure process network had been erected throughout the entire subway system with over 100 network nodes (switches) and more than 5,000 connections (ports).

Mobile video systems introduced

The deployment of video surveillance systems on buses and trains is now a standard measure for increasing security and reducing vandalism. In Munich, 162 buses are currently equipped with cameras. At the beginning of 2008 a call for bids was made to equip the subway trains and streetcars with a video surveillance system. The Munich-based company Indanet won the bid and was commissioned to equip 358 subway cars and 88 streetcars with a digital video surveillance system. Jurgen Fuchs, Indanet's general manager, says: "The camera needed to deliver 2 independent data streams: an MPEG-4-compressed stream recorded by our network recorder and stored, as well as an MJPEG stream for live transmission from the vehicle to the control center via a data transmission system."

For all occasions

Axis has a special camera in its portfolio for this major contract: AXIS M3113-R. With this camera, a system can be set up which in extraordinary cases allows the employees of an alarm center to monitor the events in the vehicle. For example, if a vandal sprays the camera with graffiti, shaving foam or something similar, thus covering the camera's lens so that the camera can't take any more pictures, the AXIS M3113-R triggers an alarm. "It is the first network camera on the market which incorporates the specific environmental and monitoring requirements for modes of transport," says Edwin Roobol, Regional Director Middle Europe for Axis.

Commute safely

Case studies by
Axis Communications

Swiss Railways under the watchful gaze of Axis network cameras

Mission

Switzerland is well known for its high security awareness. In keeping with this, Swiss Railways (SBB) decided to increase security in the Zurich S-Bahn by 2010 with the aid of network cameras. A particular requirement of the project was that the solution should run completely on IP networks and thus be able to be integrated into the existing IP/Ethernet network of the trains.

Solution

The Swiss-based Ruf Group won the contract to implement this project and was assigned the task of equipping 115 double-decker shuttle trains (DSTs) with a digital information and video surveillance system. While Ruf provided the displays in the trains, the computer platform and the complete video surveillance system with emergency telephones, Axis supplied the network cameras as a Ruf partner.

Result

The project evoked consistently positive reactions from the Swiss: this is certainly based not only on the relatively high safety requirement, but also on the additional reassurance provided by the video surveillance system. In addition, the successful project also created the basis for extending the security network, for example to the entire rail network

including stations. The collaboration with the customer was also very enriching for Axis. This new order is a gratifying further development of the partnership with Ruf Telematik for the installation in the SBB traffic network. For the transportation sector, in particular public, local mass transit, network cameras are extremely suitable:

They deliver high image quality, are cost-effective to install and the security personnel can access the image material very easily.

For every situation

Axis Communications developed a specially designed camera for this major order to meet the customer requirements: The required Pan/Tilt/Zoom-function (PTZ) of the AXIS 209MFD-R was made possible due to the usage of megapixel technology which not only permits every corner of the carriages to be monitored, but is also capable of delivering pin-sharp close-ups. In addition, this camera was equipped with an M12-connector in order to meet the EN 50155 standard for vehicles on tracks.

The palm-sized network camera is characterized by its robust design and, despite the shaking and high humidity inside mass transit vehicles, supplies digital video images of the highest quality. It is the first network camera on the market to

take into account the environmental and surveillance requirements onboard transit vehicles.

The camera thus allows the installation of a system with which, when extraordinary events occur, the police and the employees of an alarm center can follow up on the incidents from outside the vehicle. For example, if a vandal sprays the camera with graffiti, shaving foam or the like, and covers the lens so that it can no longer record any images, the AXIS 209MFD-R triggers an alarm. At the next station, police will already be waiting to meet the offender. Provision has even been made for icy temperatures: below freezing point, the AXIS 209MFD-R counteracts the formation of condensation and the associated impaired view by heating itself using Power over Ethernet. It was also necessary to make allowances for the opposite case of excessive heat. While SBB was testing the cameras exhaustively, it came to light that, in the event of high temperatures, the housing did not catch fire, but began to melt. SBB notified this problem to the manufacturer and Axis began developing a solution immediately.

A changed mixture of materials proved resistant even to extreme conditions.

For more information about Axis Communications and its products visit www.axis.com or email sap@axis.com



Top 10 access control trends for 2014

Source HID Global

Trend 1

The industry is quickly moving beyond static, proprietary access control architectures to more secure, open and adaptable solutions that support customers' desire for new products and technologies that enable their business.

As the security landscape continues to evolve in new and complex ways, progressive organizations and thought leaders are adopting a new attitude about change, and viewing it as an opportunity for improvement and value rather than an interruption or distraction.

Proactively making changes today will ensure that an organization's access control solution can adapt to future threats and take advantage of opportunities and applications beyond access control. Future high-value applications might range from cashless vending, time and attendance, and secure print management to secure network logon as part of a fully interoperable, multi-layered security solution across company systems and facilities. By using solutions that are based on industry standards such as OSDP bidirectional communications, and incorporating dynamic rather than static technologies, security becomes independent of hardware and media, and the infrastructure can more easily evolve beyond current abilities with the adaptability to combat continuously changing threats.

The industry is still evolving, however, as not everyone shares this attitude.

In a survey of integrators and users, HID Global found that less than 50 percent have upgraded their systems in the last year, and more than half have not upgraded in the past three years. Respondents were given a list of top technology best practices and while 75% felt they were important or very important, half felt they were not implementing them well or at all. Similarly, 93% agreed that a list of top policy best practices were important or very important, but nearly 40 percent said they were not implementing them well or very well. We expect these numbers to shift as strategies for change become better understood and the industry embraces the opportunities that change can bring.

Trend 2

Integrating physical access control with IT security will bring new benefits while changing how organizations operate.

Historically, physical and logical access control functions were mutually exclusive within an organization, and each was managed by different groups. Now, however, the lines between these groups are beginning to blur. Organizations want to provision physical access control system (PACS) and IT identities on a single card (or smartphone) that can be used to open doors and log on to computers, and for other applications. This will create a seamless user experience when securing doors, data and the cloud, and improve how organizations create,

use and manage identities across many different applications on both smart cards and smartphones. Users will soon be able to carry many types of access control credentials as well as one time password (OTP) tokens on a single microprocessor based smart card or smartphone. This has led many companies to seriously consider the benefits of incorporating secure physical and logical access on cards and phones into their facilities and IT access strategies, including the ability to improve efficiency through centralization of credential management for multiple logical and physical access control identities across IT resources and facilities. Organizations will be able to achieve true convergence through a single solution that can be used to access IT resources while also enabling many other physical security applications. There will be a single process for provisioning and enrolling both IT and PACS identities, and it will be possible to apply a unified set of workflows to a single set of managed identities for organizational convergence.

Trend 3

Strong authentication will continue to grow in importance in the face of a rapidly changing IT security threat environment – and will also move to the door.

Security professionals understand the importance of multi-factor authentication, also known as strong authentication, especially for IT security. The industry is quickly moving beyond simple passwords (something the users

iCLASS SE[®]

The smartest access control platform



Next generation access control. An evolution in security, adaptability and performance.



HID Global's technology and media-independent iCLASS SE[®] Platform is a secure identity solution for physical access and the widest range of converged applications and environments. For maximum interoperability, iCLASS SE[®] supports legacy and nearly all card technologies for cost effective, seamless upgrades to higher security and enhanced performance.

To find out more download the iCLASS SE[®] whitepaper hidglobal.com/iclass-se-platform-nzsec or contact us at +61 3 9809 2892 or email at asiasales@hidglobal.com

© 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, and the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

knows) to additional authentication factors including something the user has (such as a mobile or web token) and something the user is (ascertained through a biometric or behavior-metric solution). Unfortunately, users have grown weary of the inconvenience of hardware OTPs, display cards and other physical devices for two-factor authentication. While the industry is replacing hardware OTPs with software tokens that can be held on such user devices as mobile phones, tablets and browser-based tokens, there are security vulnerabilities with this approach.

A far more secure strong authentication alternative is multi-application credentials that use a data model which can represent any type of identity information and can be carried on smart cards or smartphones. Users will simply take the same card (or phone) they use for building access and tap it to a personal tablet or laptop for authenticating to a VPN, wireless network, corporate intranet, cloud and web-based applications, single-sign-on (SSO) clients and other IT resources. There will be no need for a separate card reader or additional devices to issue and manage, nor will they need to enter a password on touch-screen devices

We will also see increasing adoption of other authentication factors including biometrics as well as gesture technology. With a pre-defined wave of the hand or other gesture, users will be able to control a variety of RFID devices, dramatically changing how we interact with access control systems.

In the federal space, widely adopted Public Key Infrastructure (PKI) strong authentication methods will also be moving to the door, using both cards and mobile phones. To support mobile platforms, a new set of specifications called FIPS-201-2 is expected to include extensions such as the concept of derived credentials that can be carried in the phone's secure element using the same cryptographic services as the card. Another expected feature of FIPS 201-2 is that it will allow the use of the Open Protocol for Access Control Identification and Ticketing with privacy (OPACITY) suite of authentication and key agreement protocols. OPACITY will add roughly four times the performance for critical tasks. It will also deliver secure wireless communications, which will enable the use of PIN and biometrics on the contactless interface. This will further strengthen authentication for both physical and logical access control.

Trend 4 **Strong authentication will increasingly be implemented using a multi-layered strategy.**

Today's strong authentication solutions increasingly will be used to secure everything from the door, to data, to the cloud. They will deliver multifactor authentication capabilities for the most effective threat protection, as part of a multi-layered security strategy. In addition to multi-factor user authentication as the first layer of security, both inside the firewall and in the cloud, there are four other layers to implement, including authenticating the device, the channel, the transaction and the application.

Effectively implementing these five security layers requires an integrated and versatile authentication platform with real-time threat detection capabilities. Used in online banking and ecommerce for some time, threat detection technology is expected to cross over into the corporate sector as a way to provide an additional layer of security for remote access use cases such as VPNs or Virtual Desktops, and in the healthcare space, for on-line records access. Health care providers today increasingly rely on digital and mobile technologies to deliver patient care – sometimes willingly and sometimes under regulatory pressure. With the proliferation of these technologies will come new security and privacy challenges that require strong authentication using a multi-layered approach.

Trend 5 **Mobile access control will continue to roll out in stages.**

During 2014, we expect to see the first phases of mobile access deployments in which smartphones will function similar to that of a card transaction today, with limitations due to technology and business ecosystems. In subsequent phases the phone's on-board computing power and multimedia capabilities will be leveraged overcome limitations and provide a more functional and rich user transaction and experience. Looking forward further, the connectivity of smartphones will be used to perform most tasks that today are jointly executed by card readers and servers or panels in traditional access control systems. This includes verifying identity with rules such as whether the access request is within a permitted time and, using the phone's GPS capability, whether the person is actually in the vicinity of the door. The user can then

be validated using a cloud application and granted access via a trusted message over secure communication to the door.

In this new paradigm, mobile devices (rather than an access control system) make the access decisions and doors (rather than cards) present their identity. This role reversal, sometimes called duality, changes how access control solutions are offered. Organizations will be less dependent on the expensive infrastructure required for connecting servers, panels and readers – just electronic locks that respond to a mobile device's encrypted "open" command.

This simplified and more economical model will enable the industry to secure more assets; interior doors, filing cabinets, storage units and other areas that have been prohibitively expensive or complex to secure in the past.

Trend 6 **We will enter a new era of NFC authentication services.**

There is an emerging paradigm in which Near Field Communications (NFC) RFID tags will be attached to many items in many public places, to establish their unique identity so that authenticity can later be conveniently verified using contactless readers or any NFC-enabled smartphone or tablet. This authentication model will enable a variety of new transactions and services, ranging from authenticating items and documents and securely managing chain-of-custody, warranty and other transaction data, to accessing web links provided by smart digital posters (Digital Out of Home Marketing – DOOH), proof of presence (Electronic Visitor Verification – EVV) and authorizing a phone to operate in an organization's virtual telecom system.

These and other applications will rely on the ability to confer trust both on the NFC tags and their interactions with many different devices and applications. Without this trust, tags could be reconfigured or duplicated, leading to counterfeit authentication, fraudulent transactions, and increased user vulnerability to mobile and on-line security and privacy threats. This will require the ability to confer trust to, and provide security for, the readily available NFC tags used for these applications, to eliminate the inherent risks associated with using NFC tags by ensuring they are valid before they can be used. Ensuring this level of trust will require a combination of NFC tags containing cryptographically signed data elements that cannot be copied or modified without detection,

Locked in... no compromise no comparison!

LOKTRONIC proudly continues to be a leading supplier of New Zealand and international electronic locking hardware brands, including....

Abloy Electric Locks • Abloy, Effeft & IR Power Transfers • Effeft Electric Strikes • Egress Buttons • Flair Reed Switches • Haze Batteries • Imported Electromagnetic Locks • Legge Electric Mortice Locks, accessories and furniture • Lockwood Electric Mortice Locks, accessories and furniture • Loktronic, Cisa, Effeft and Asian Gate Locks • Loktronic and Trencab Key Switches • Loktronic Power Distribution Modules • Loktronic Power Supply Cabinets • Powerbox Power Supplies • Prastel Door Controllers • Roller Door Locks • Rosslare Keypads • Trimec Drop Bolts • Trimec Electric Strikes • Trimec V-Locks • Trojan Em Rex & Prox Rex Devices • Trojan Relays • STI Secure Housings for Keypads, Fire Alarms and Exit Devices • ViTech Anti-Interference Device • ViTech Battery Tester • ViTech Fire Brigade Alarms, Type X and Type Y • And many others.
Plus, a wide range of spares and accessories.

Designed and made in New Zealand, our famous **LOKTRONIC** electromagnetic locks and Fire Door Holding electromagnets carry a solid

10 year* guarantee

And, our **LOKTRONIC** outdoor electromagnetic locks continue to stand the test of time!

25 years service and experience.
A future of secure growth and development.



* **Sales** * **Spares and accessories** * **Repairs** * **Advice**

Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
mail@loktronic.co.nz www.loktronic.co.nz



plus secure cloud-based authentication services that are backed by a proven server infrastructure. With this ecosystem in place, it will be possible to develop applications that enable an NFC-enabled smartphone or reader to communicate tag information to a secure, cloud-based server, which validates whether the tag is authentic and a proof of presence and transmits this information back to the smartphone or reader.

Trend 7

The migration of intelligence to the door will continue with the further adoption of IP architectures and future capabilities of smartphones for access control.

Physical security and access control solutions continue moving to IP-based architectures that are easier to deploy and maintain. In addition, a standards-based IP architecture facilitates the integration of a physical access control system (PACS) with other systems that can share the same network. A major benefit of this approach is the ability to move intelligence to the door, which streamlines system monitoring, management and reporting via standard web browsers. By migrating to true open architecture IP-based intelligent controllers, users also can simplify future infrastructure enhancements and modifications since they can invest in hardware platforms that are not tied to proprietary protocols and software.

IP-based access control is moving beyond host-controller communications to include controller-module and controller-reader communications as well. Additionally, we will see a move to untethered connectivity in this networked access control environment. Wireless intelligent locksets are the first step, and will become more prevalent as new, lower-cost, energy-efficient models are introduced to the market. Mobile access control using smartphones is also on its way, which will leverage these devices' wireless connection to act as both the key and processor and become the rules engine for making access control decisions. It will be possible to build and deploy readers (and locks) without any significant intelligence or connectivity capabilities and, because of the interoperability benefits of open-architecture IP-based intelligent controllers, users will have a broad range of controller and reader platforms to choose from, including basic readers and wireless intelligent readers that provide access to multiple credential technologies.

Trend 8

Printing and encoding advancements will simplify card personalization while speeding throughput for more durable cards that can be securely issued from anywhere, at any time.

Today's printers, card materials and software work together to solve today's card issuance challenges, delivering fast and efficient instant issuance capabilities while also optimizing card security by incorporating visual and logical technologies for multi-layered validation.

Ongoing advancements in encoding technology include in-line personalization solutions that streamline card issuance while also making it easier to support multi-technology migration environments.

Users will continue to gravitate to field-upgradable units that enable organizations that already own a card printer to add an encoder in the field so they can leverage smart card benefits well into the future.

We will also see faster printing and encoding solutions and more durable card materials, as well as printers that support the wireless communication of ID and other information in an "anywhere/anytime" distributed issuance scenario.

Card materials also continue to improve, and the industry will see products such as Euro MasterCard Visa (EMV)-based payment cards that will last three times as long as in the past.

Trend 9

Visitor management systems will continue to move beyond the businesses to schools, hospitals and other institutions where high-profile incidents have proven that safety and security shouldn't be left to paper logs.

Visitor management systems are now widely adopted in the corporate environment, and they are increasingly spreading to other institutions, agencies and campuses. For instance, in the hospital environment, paper systems are being replaced with registration systems that are capable of screening, badging and tracking all visitors or, at a minimum, critical areas such as pediatric wards, as well as "after hours" periods when staff is reduced.

These visitor management systems include key features such as support for the HL7 interface control so visitors can be matched to a variety of key real-time information about patient status and room numbers, ensuring no visitor is ever sent to the wrong patient room.

Another example is federal agencies, which are migrating to systems that can

quickly process visitor access while ensuring that all security procedures and policies are followed in accordance with Homeland Security Protection Directive-12 (HSPD-12). These systems read and process PIV cards in support of HSPD-12 and also can scan and process Transportation Worker Identification Credential (TWIC) cards using OCR scanning, as well as Common Access Cards (CACs) using 2D bar code scanning.

The most effective systems feature simple-to-deploy middleware software that seamlessly integrates with the PACS and validates PIV credentials, which enables agencies to use PIV card data to better manage cross-over visits from other agency employees.

Trend 10

There will be accelerating worldwide adoption of multi-purpose electronic ID (eID) credentials.

In 2014 we will continue to see governments adopting eIDs to streamline government-to-citizen services. Powerful multi-purpose eID credentials can maintain the highest levels of security while addressing objectives such as entry to secure facilities, faster border crossing, and access to health and social services.

For instance eID cards are combining optical security media for visual and digital security with RFID tags for accelerated border crossing. Secure issuance is also a big part of the eID revolution. In 2014, we will see the market continue to shift from a centralized issuance mindset as governments focus on achieving increased efficiencies, convenience and enhanced productivity through distributed identity personalization. We will also see continued developments in technologies that prevent counterfeiting and obstruct tampering, while facilitating quick and accurate authentication of cards, e-passports and other eID documents. Innovative breakthroughs, such as crack prevention technology, will enable governments to reap the economic and programmatic rewards of highly secure eIDs that are far more durable.



For more information on HID's products and services within New Zealand, please contact Stephen Blakey on 09 537 0279 or 0210 824 6096 email: sblakey@hidglobal.com

Upgraded intercoms and remotes for electric gates

Issues around access control are being constantly evaluated and resolved in New Zealand through the application of cost effective and common sense solutions.

The wireless UHF intercom for electric gates introduced last year by Withington Electrical has undergone further development to the speaker and microphone volumes. Director Simon Withington says he is very happy with the results, having personally tested it at 1.6K in a suburban area with a small hill in the way. "It now works as I had initially wanted it to." He adds, "I would like to get a couple out in challenging areas to test, then look at the compliance testing. From what I have been told in brief discussions with a testing lab there should not be a problem."

Withington Electrical is also the New Zealand distributor for a Spanish company that has devised a rolling code remote which will work on a wide range of European gate automation brand names such as BFT, Nice, Novotechnica, Came Faac, Liftmaster, Prastel, Proteco, Chamberlain, Merlin and B&D outdoors... just to name a few!

Simon says, "This one remote will do all of them. I have some cloning



Upgraded wireless UHF intercom for electric gates

remotes coming which work on a greater MHZ scale up to 866MHZ for the new FAAC frequency. I have wireless single code but two channel keypads and receivers which are also multi branded. So if a customer had, for example, a Nice gate automation installed and wanted to use a spare button on an existing remote for say the garage door,

one of these receivers can be coded to that remote."

Simon plans to launch a website for these products later in the year for the retail sector but says he is certainly encouraging trade customers to make contact now. He says that he has an exceptionally good price for these multi remotes of \$25+GST for a four button remote.

High Speed Gate Automation

From commercial gates to heavy prison gates, barrier arms to high speed swing gates with a variety of high speed gate motors.



We installed a high speed automatic gate motor to a 15m gate in Palmerston North



A barrier arm for Peter Jackson's Wellington Headquarters

We also manufacture, install and service

- Stainless gate drop bolt locks
- Remote controls and receivers
- Cantilever slide gate hardware
- Vehicle loop detectors
- PIR safety beams for automatic gates and doors
- Keypads wireless and stand alone fixed wired
- Light commercial 24v linear swing gate motors



Swing gate motor for gates up to 15m



These swing gates are part of the Government House refurbishment

We design and manufacture all our automation products in Wellington, but pride ourselves on our installation and service anywhere in New Zealand. For more information and trade enquires contact:

Simon on 0274 488 506 or visit www.highspeedgateautomation.com

A leader that likes to push the envelope

If two of the key platforms for getting to the top are hard work and forward thinking, then our profile this month stands as a great example. He also embodies the best of those qualities that make for a high value individual, both for the company's principals and for the team he leads; experience, knowledge and decision making ability.

In our modern commercial environment, certified industry training or a tertiary qualification count for an awful lot in gaining employment, establishing a career and moving up the rungs of the vocational ladder. It is something Mike Rutherford, Chief Operating Officer at First Security Guard Services Ltd knows full well.

While he did it the hard way by leaving school at 15, he has gone on to lead what is arguably the largest security business in New Zealand. It is something he hopes every one of the 1,800 employees at First Security could emulate while at the same time he understands the intrinsic changes and growth of the modern business world and the importance of training and qualifications.

Mike began his vocational pathway by working and training as a chef initially followed by a brief hiatus in television rentals and restaurants. He fell into his current market sector some 40 years ago when he joined the Armoured Freightways Group (now Armourguard) as an armoured crewman, moving on to become a senior crewman and then operations manager. By 22 years of age he was based in Wellington as the company's youngest branch manager.

Putting his money where his mouth was, Mike purchased his own business, Star Security in Whangarei in 1984. He

continued building the business and in 1991 sold to Securitas. He continued as manager of the business for the new owners before transferring to Christchurch to become southern regional manager, with an oversight of New Zealand from Hawkes Bay south, including Wellington.

The Securitas business at the time included alarm monitoring which was later sold to Signature Security.

When Securitas was purchased by Chubb, Mike transferred to Auckland with the illustrious title of national manager of patrol services and branch development. In 2005 he was head hunted by Ross Johnson, owner of First Security. The business was at that time a medium sized operation and someone with the ability to manage it at the corporate level was required.

With some 300 employees, First Security was then mainly an Auckland-based service with offices in Wellington.

This all changed a year after Mike joined when the business was sold to Danish giant ISS, a facility service company, described as the fourth largest employer in the world with some 536,000 staff. As a wholly owned subsidiary of ISS Denmark, First Security shares a strategic direction that has been unchanged for over a decade. This changed just recently with the company sold to Australian-based Wilson Security. Wilson Security is a division of the Wilson Group, which as well as security has wide spread interests in parking, storage, technology and health services across Australia.

This acquisition continues Mike's involvement in the strong growth of First



Forward thinking and embracing change have paid dividends for First Alert's Mike Rutherford

VideoNetBox II

SMAVIA Appliance for up to 8 IP Channels, 2× 2.5" HDD



SMAVIA Appliance

Compact Design

Open Platform

Up to 8 IP Channels

The **VideoNetBox II** is a compact appliance with a processing capacity for up to **8 IP video channels**. The basic version with 2 IP video channels can be expanded with up to 6 additional video channels using a license code.

The **VideoNetBox II** is perfectly suited for wall mountings. Its compact and robust design allows for a flexible use. Together with the dedicated software **SMAVIA Recording Server**, it is the ideal IP security solution e.g. for retail stores, gas stations and private residences.

SMAVIA Viewing Client

The corresponding software **SMAVIA Viewing Client** allows for the independent and convenient evaluation of the recordings over Ethernet (LAN/WAN). It can be run on devices with a Windows XP / 7 operating system and is included in the **VNB II**'s scope of delivery together with an access license.

iPhone Server

The integrated **iPhone Server Software**²⁾ allows for a mobile access with the smartphone application **Dallmeier Mobile Video Center** over the iPhone. The display of live images and playback of recordings follow a special procedure which is independent of the recording settings of the VNB II.

Open Platform

The pre-installed software **SMAVIA Recording Server** is designed as an open platform. Together with the according licenses, **3rd-party IP cameras** with **motion detection** can be recorded and configured over the **ONVIF protocol**³⁾.

Easy Mounting

The compact, robust and well-proven **VideoNetBox** enclosure was further optimised for the current **version II**. After opening the cover on the rear, **hard disk drives** can be easily installed or exchanged in a few simple steps.

Features Hardware

- Compact server hardware with multi-core CPU
- Flash memory for operating system
- Suitable for up to 8 SD, HD or megapixel video channels
- **Analog Upgrade Kit** for the **hybrid operation** with up to 8 channels (analog/SD-IP/HD-IP) optional
- **One local playback** of one camera (analog, SD IP or HD IP) optional
- Multi-split **local live display** of several cameras (analog, SD IP and HD IP) optional
- High-speed storage due to fully compatible components
- Optimised for the easy installation of hard disk drives
- Numerous mounting options on walls or ceilings

Features SMAVIA Recording Server

- Licenses for **2 channels** included, expandable to up to 8 channels
- **Basic license** for the access of a **SMAVIA Viewing Client** included
- **Free conversion** of the **basic license** to a **floating license** on acquisition of additional access licenses
- License for **updating the SMAVIA software** for 12 months included
- License for **SEDOR® camera sabotage protection** optional
- License for **PRemote-HD** in real-time optional
- License for **LocalViewing** optional
- License for **ViProxy** optional
- License for the **recording of multicast video streams** included
- License for **real-time recording** included
- **Recording of 3rd-party IP cameras with motion detection** optional³⁾
- **Configuration of 3rd-party IP cameras via ONVIF protocol** optional³⁾
- **BANK Package** in compliance with **DGVV Test (UVV-Kassen)** optional
- Connection to **Active Directory** over LDAP
- Evaluation with **SMAVIA Viewing Client** or **SeMSy®** over Ethernet

Security which really accelerated with the purchase of Chubb Protective Services in 2008. The later purchase of Prisoner Escort Court Custodial Services virtually quadrupled the size of the business overnight.

Today Mike manages a strong, dedicated security service involved in concierge and personal security services, alarm systems and response services, guard services and security patrols. At the peak of the summer season when cruise ships are thick on the harbours, the team can run to over 1,800 dropping to 1,200 over the winter.

First Security now encompasses 13 offices in all major metropolitan centres. This means some 95 patrols throughout New Zealand on an average night, 35 in Auckland alone. As well as the mobile services, there are a large number of static guard services and a high end call centre dealing with a wide range of problems from property issues to noise, environmental and 'animal.'

First Security contracts to a number of large clients such as Auckland Council, the major transport services, universities and other 'blue chip' businesses. They stay away from events and crowd control which is seen a specialty sector.

Mike's team is large and diverse, members drawn from all walks of life. Some see employment in the business as a step as opposed to a full career but Mike believes that recruiting great people is fundamental to the success of the business. "We have systems to recruit, train, equip and retain high calibre personnel. So as one of the fastest growing security companies in New

Zealand we are always looking to recruit suitable people to join our team."

While a significant portion of recruitment comes through the careers pages of the First Security website and through referrals, a robust selection process which can also include psychometric testing is undertaken. Mike says a candidate's abilities are closely judged including all the basics such as numeracy and literacy. Adaptability, or decision making ability, is also very important says Mike. A full time national training manager who has a police background sets the training programme. As we have discussed in previous profiles, new legislation requires centre level 'mandatory training' prior to an individual getting a security licence. Mike describes this as a basic entry level requirement.

"After this each employee is set a PDP or professional development programme tailored to their role within the company.

The aim is to develop that person over a six to 12 month period according to their responsibilities. In our hierarchical system virtually all our managers come through the ranks, hence a demonstration-based assessment system looking at key attributes is vital. Gaining an NZQA level two security qualification is a key goal."

Mike says the identification of potential senior and supervisor personnel early on and giving them the necessary leadership skills has been essential. "Hopefully we have pushed some envelopes within the industry which can only be a good thing.

We aim for our remuneration levels to be higher than the market rate and individuals can advance quickly if they have the desire to do so and prove themselves."

Leadership for Mike often also means being a pioneer, an innovator, and learning from others. For example, First Security has been a leader in the widespread use of call verifiers and mobile data terminals.

Mike says, "The security sector is in a state of change in a variety of areas from ownership to electronics. As an industry we need to position ourselves to support the electronics sector. Manpower development needs to be undertaken in conjunction with electronics and absorbed into it.

"We also need to continue getting smarter with our service offerings and with our standards. The changes to industry legislation in the lead-up to the Rugby World Cup have made a big difference across the sector from doormen and bouncers to technology, surveillance and investigation."

Whatever the future holds, Mike Rutherford is very happy that the company he leads and holds the New Zealand based directorship for has been acquired by a well respected, supportive and innovative industry leader.

He might be an industry veteran in a new era but that experience and knowledge is still leavened by another key attribute; forward thinking.

First Security sells to Wilson

ISS has signed a sale agreement with Wilson Security to acquire both the commercial security contracts of ISS Security in Australia and the First Security Business in New Zealand. Following a review of all its activities, ISS in New Zealand and Australia determined that the commercial security business was not core to the strategy and did not give as much ability to leverage the strength of ISS.

The sale will make Wilson Security the largest provider of guarding services across Australia and New Zealand. Security is their core business and they have developed a market leading position, so it is felt it was a good match.

The transaction is subject to approval from relevant local authorities and is expected to close before the end of March. Following the transaction Wilson Security will become the preferred security partner for ISS in New Zealand and Australia.

The ISS Security brand will continue in Australia, with a focus purely on security at major airports, which are part of the Aviation & Transport Division of ISS. ISS will remain the largest provider of aviation security services in Australia, with 900 trained and licensed officers providing services to 13 airports.



At the peak of the summer season when cruise ships are thick on the harbours, the team can run to over 1,800 dropping to 1,200 over the winter

New focus on access management in the rural sector

Farmers are finding new ways of fighting stock theft as well as catching out cannabis growers. A security company has built the country's first underground surveillance system which does not need mains power or cellular networks and is totally covert.

Auckland-based Specialist Surveillance Services Limited Director, Roger Winslade says it has already caught poachers in a forest near Auckland last month.

"It's basically a very sophisticated device for picking up metal. If metal comes within 17 metres of it, it is triggered and sends the alert through, so there are no false activations with animals, wind or anything like that."

Armed poachers on a quad bike entered a private forest at Woodhill north-west of Auckland.

Almost as soon as they had entered the private forest they woke up a Scorpion 1000, a new hidden covert intruder detection device, the brainchild of Specialist Surveillance Services Limited.

Just like the sting from a real scorpion it was 'game over' for the poachers.

Within 90 seconds the Scorpion 1000 sent an alert to a private security patrol giving the exact time of the alert and location of the poachers.

The poachers had no idea the private security patrol was closing in on them

until they were bailed up and the local Police had them in custody.

Police seized two rifles; knives and hunting equipment. Charges have been laid relating to the poaching activities with the offenders due to appear in court.

Trespass action has also been taken against the trio by the landowners.

The Scorpion 1000 is a game changer in the way remote or isolated location security can be managed says Winslade.

The Scorpion 1000 can help farmers, forest owners, contractors, councils, orchards, vineyard owners or anyone having theft problems or illegal access issues.

Federated Farmers estimates \$120 million is stolen from rural properties each year in the form of stock, general farm equipment and petrol or diesel.

It has created the Stop Stock Theft website with police, where victims can report stock theft anonymously to build a database on when and where theft happens most.

Rural security spokesperson Katie Milne says at this time of year especially, cannabis growers are rife in secluded areas and they'll often steal equipment and fuel as well.

Winslade says the detector is the first of its kind in New Zealand.



Specialist Surveillance Services has a Scorpion with a real sting in the tail

SUBSCRIBE NOW

Readers of NZ Security include those working directly and indirectly in the domestic and commercial security industry. From business owners and managers right through to suppliers, installers and front line staff.

Among our readers are IT security experts, surveillance professionals and loss prevention staff.

Our readers take their job seriously and make an active choice to be kept informed and up to date with the industry.

For only \$50.00 plus GST you can ensure that you receive a 1 year subscription (6 issues) by filling out the form below and posting to:

New Zealand Security Magazine
27 West Crescent, Te Puru, 3575
RD5, Thames, New Zealand

or email your contact and postal details to:
craig@newzealandsecurity.co.nz

Mr Mrs Ms _____

Surname _____

Title _____

Company _____

Postal Address _____

Telephone _____

Email _____

Date _____

Signed _____

nzSecurity Magazine
A trusted source of information for industry professionals

Looks do matter

The new DINION IP 4000 and IP 5000 HD cameras

Video surveillance as a security measure often requires balancing optimum performance with aesthetics. Especially in such applications as offices, hospitality or retail stores, design and appearance can be just as important as technical performance. The new DINION IP 4000 and 5000 cameras from Bosch Security Systems meet these multiple and

demanding requirements by combining the latest technology with outstanding aesthetic design.

Both cameras offer an attractive range of features with regard to the highest image quality, management of bit rate, and lowest storage requirements, as well as important audio capabilities, cloud-based services plus easy and

cost-effective installation. Taking image quality first, the cameras are available in two resolution versions: the DINION IP 4000 HD with 720p and the DINION IP 5000 HD with 1080p. The desired amount of detail can be selected according to the intended application, while intelligent Dynamic Image Noise Reduction (iDNR) automatically





adjusts the level of noise reduction based on movement in the scene. This ensures crisp images and saves up to 50 percent on bit rate and thus memory requirements, considerably lowering storage and overall system costs.

As regards audio capabilities, the built-in microphone and two-way audio functionality turn these DINION IP cameras into even more effective security tools, as the operator or security guard can not only listen to but also question intruders or communicate with visitors who appear to be in need of assistance. Easy installation and configuration are guaranteed by the cameras' Power-over-Ethernet (PoE) functionality, as well as due to the preconfigured user modes. For retail applications in particular, the cameras come with a direct monitor output, enabling a confrontation monitor to be directly connected to the camera. It is therefore ideal for entrances and other situations where people need to be made aware of the presence of video surveillance.

Nowadays, customers demand smooth and instant access to high definition video from any location and at any time. Bosch has responded to this need by offering its Dynamic Transcoding technology. By constantly measuring the available bandwidth and automatically adjusting the bit rate of the camera, this patented technology enables smooth live video streaming, regardless of the available bandwidth, as well as full-HD details when playback is paused anywhere and anytime. Thus, image quality and detail are maintained while suspicious events are easily and quickly detected. This Dynamic Transcoding technology can be fully exploited in combination with the new DINION IP 4000 and 5000 cameras by simply adding one of the Bosch DIVAR IP recording solutions or a Bosch VIDEOJET to the total Bosch video surveillance solution.

"The two new DINION IP HD cameras are the logical solution for small and medium-sized enterprises where both professional security and appearance



BOSCH

Invented for life

matter," explains Derek Lin, Product Manager Video Systems at Bosch. "Their aesthetic design makes them ideal for seamless and discrete indoor installation, offering maximum security for people and property while simultaneously respecting the building's architecture. They demonstrate that high performance and aesthetic design can be made affordable for everyday video surveillance applications."

The entire Bosch IP portfolio seamlessly integrates with software and recording solutions from Bosch and other vendors. Third party integration is ensured by the ONVIF conformity of all Bosch IP cameras, as well as the Bosch Integrated Partner Program (IPP), which simplifies the interoperability of video surveillance products. The IPP portal provides access to a comprehensive library of integration tools, video solutions, services, and information about compatible products. More information is available from: ipp.boschsecurity.com.

ZoneTechnology
Your Security Supply Partner

Auckland: (09) 415 1500

Wellington (04) 803 3110

Christchurch (03) 365 1050

Email: sales@zonetechnology.co.nz

Website: www.zonetechnology.co.nz

Thermal imaging allows for accurate and time-saving inspections of electrical cabinets inside aircraft cockpits

Aircraft cockpit inspections, both pre-flight and post-flight, consist of a wide range of control routines that need to ensure the safety of its passengers during a flight. Next to that, it is essential that inspections are carried out as efficiently as possible, because every idle hour that is keeping an aircraft waiting on the ground is time and money lost. In that respect, Dutch technical inspection specialist Thermografisch & Adviesbureau Uden BV found a way to significantly speed up electrical inspections inside the cockpit, while at the same time guaranteeing accuracy and reliability. The secret: thermal imaging technology from FLIR Systems.

Thermografisch & Adviesbureau Uden BV is an experienced agency which is specialized in independent inspections and supplies recommendations to the industrial and construction markets. The company's expertise ranges from building inspections, over climate and mechanical installation inspections, to process control and inspection of electronic components. For all of these applications, Thermografisch & Adviesbureau Uden BV heavily relies on thermography.

"We had a long history of performing inspections of electrical cabinets for industrial applications by means of thermal imaging cameras, but we had never applied this technology for the inspection of cockpit electronics," comments Mr Ralf Grispen, owner of Thermografisch & Adviesbureau Uden BV. In fact, that particular question came directly from Thermografisch & Adviesbureau Uden BV's long-term customer Star Air, a Danish cargo airline, part of the A.P.Moller-Maersk Group, specialized in providing highly reliable cargo lift capacity.

Thermal imaging for cockpit inspections

"Star Air knew that we could successfully perform inspections of water ingress in composite materials of airplanes by means of thermal imaging cameras," comments Mr Grispen. "But technicians of the airline company wanted to know if we could use the same technology for the inspections

of wiring and cabling inside the cockpit as well. We decided to give that a try."

Mr Grispen and Mr Rob Huting, co-owner of the company, travelled to Cologne Airport, where Star Air's aircraft fleet is located. Technicians of the airline company made the cockpit of a Boeing 767-200 ready for electrical inspections, and the Thermografisch & Adviesbureau



The high-res P640 thermal and visual camera is a smart choice for thermal imaging surveys.



The FLIR P640 allows us to view the smallest electrical parts and the smallest temperature differences.

Uden BV team started its routines. The inspection job was a success: the thermal imaging cameras showed the temperature differences of the cockpit's electrical cabinets in the greatest detail and the team was indeed able to detect an initial defect in a resistor.

In addition, the test resulted in a contract award to Thermografisch & Adviesbureau Uden BV by Star Air for the maintenance inspection of 11 Boeing 767-200 freight aircraft.

Time-saving inspections

"Faulty resistors heat up, and that's exactly the reason why thermal imaging technology can easily detect such defects, even very small problems in an early phase," comments Mr Grispen. "In the case of Star Air, this technology proved to be a perfect fit for preventive maintenance and electrical inspections inside the cockpit in general. Especially with older aircraft, which are subject to wear, it is critical to inspect connections and fittings on a regular basis. With thermal imaging cameras from FLIR, we can get this job done in a fast, accurate and cost-effective way."

Cockpit inspections with thermal imaging technology are very accurate and time-saving. The main advantage of thermal imaging is that you can locate electrical problems very quickly and accurately. With thermal imaging you are able to immediately see which component is causing the problem.

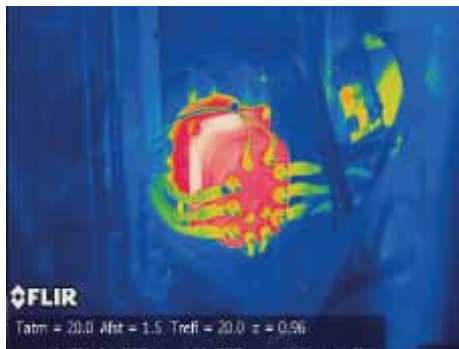
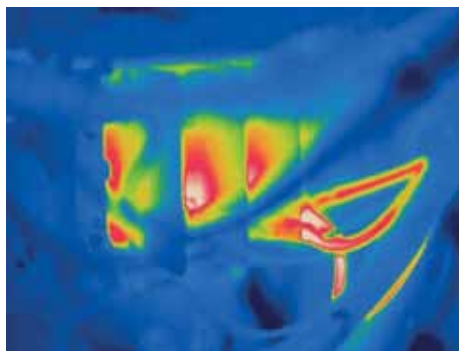
“We encourage the use of thermal imaging for cockpit inspections, because it gives us an accurate view of the condition our aircraft is in,” comments Mr Carsten Holm, Vice president technical at Star Air. “As a dedicated provider of quality air cargo services, Star Air does everything in its power to guarantee that all equipment is in perfect state and that cargo and crew can enjoy a safe flight. We are glad that thermal imaging technology from FLIR Systems helps us achieve that.”

Seeing the smallest details

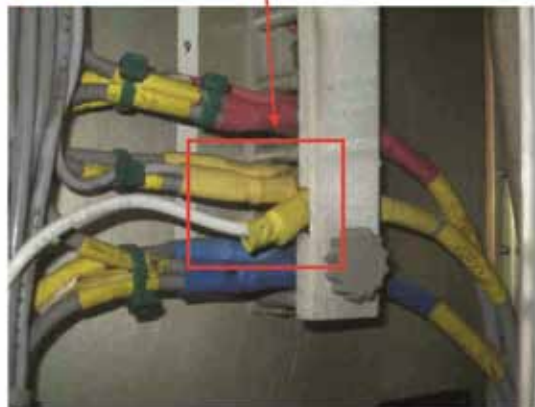
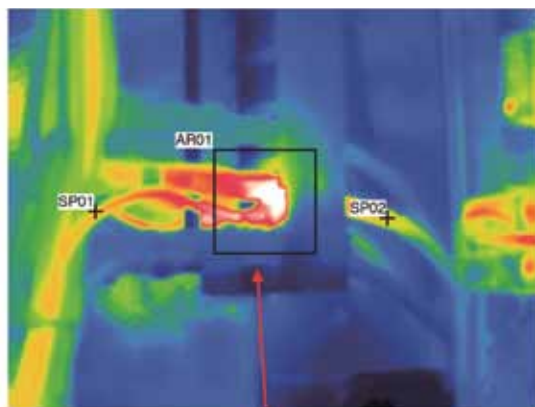
Thermografisch & Adviesbureau Uden BV is using the FLIR P640 thermal imaging camera, a high-resolution thermal and visual camera that has a host of advanced features, which makes it a smart choice for thermal imaging surveys.

“The camera provides us with a very high resolution, which enables us to view the smallest electrical parts as well as the smallest temperature differences,” comments Mr. Grispen. “An additional benefit of the FLIR P640’s large color LCD is that you can simultaneously share your images with your customer or your colleagues. For us, this is a feature that cannot be underestimated, because it allows us to reassure our customers and show them that we do a good job.”

“Also the possibility to make short movies with the FLIR P640 makes this camera a very handy tool to have. And



The FLIR thermal imaging camera was able to detect a temperature increase in the electrical wiring and components.



Disclaimer:
Images for illustrative purposes only and may not be representative of the actual resolution of the camera shown. Technical specifications subject to change without notice.

Temperatures	
Label	Value
SP01	39,2°C
SP02	39,2°C
AR01 : max	52,7°C
AR01 : min	28,1°C

The FLIR reporting software delivers a perfectly documented and detailed report of our findings to the technical staff that will do the actual repairs.

finally, I think the camera finds a very good balance between robustness and ergonomics,” Mr Grispen continues.

FLIR P640 thermal imaging camera

The FLIR P640 camera is easy to operate and delivers accurate temperature measurements at safe distances. The FLIR P640 provides professional users, including infrared consultants and professional thermographers, with a unique competitive advantage.

The P640 presents more pixels, which means greater temperature measurement accuracy, particularly for small objects. To the professional thermographer, this means clear, practical benefits – and a strong competitive advantage. With the P640, you can now resolve smaller objects from further away and still get accurate temperature measurements.

Extensive reporting capabilities

“The reporting software that comes with the FLIR P640 is very easy to use and allows us to deliver a perfectly documented and detailed report of our findings to the technical staff that will do the actual repairs. We regularly receive the latest updates from the FLIR software so we can enjoy extra features.”

FLIR certified

Thermografisch & Adviesbureau Uden BV also makes use of the services of the FLIR Infrared Training Center (ITC). “We have a team of three people that

are fully FLIR ITC certified,” comments Mr Grispen. “We regularly attend trainings organized by FLIR Systems, so we are always up to date with the latest developments of the company’s product portfolio. As with all FLIR after-sales services, we are very pleased with these trainings, because they help us apply thermal imaging technology in real life applications.”

About thermal imaging

Thermal imaging is the use of cameras constructed with specialty sensors that “see” thermal energy emitted from an object. Thermal, or infrared energy, is light that is not visible to the human eye because its wavelength is too long to be detected. It’s the part of the electromagnetic spectrum that we perceive as heat. Infrared allows us to see what our eyes cannot. Thermal imaging cameras produce images of invisible infrared or “heat” radiation. Based on temperature differences between objects, thermal imaging produces a clear image. It is an excellent tool for predictive maintenance, building inspections, research & development and automation applications. It can see in total darkness, in the darkest of nights, through fog, in the far distance, through smoke. It is also used for security and surveillance, maritime, automotive, firefighting and many other applications.

Medical Alarm Monitoring

By Julia West

As more New Zealanders are living for longer, many of our elderly as well as people with disabilities are choosing to remain living independently. As a result there is a growing need to provide a sense of safety in the home.

Burglar alarms provide security from intruders, while medical alarm monitoring offers safety and support for those who may need emergency help at home.

There are over 40 medical alarm providers in New Zealand with many being relatively small players. The five major providers are St John Medical Alarms, Bupa Care Services, ADT Security, Safe Link, and Kiwi Concern.

A monitored medical alarm consists of a base unit and a pendant or wristband with a trigger button. The base unit is installed in a telephone jack point and usually sits next to the primary landline. Most models have a battery backup in case of power failure.

The pendants are waterproof and usually worn around a person's neck while the wristband is worn like a watch-strap. The pendant and wristband contain batteries that need replacement from time to time.

If a user needs help, they press the trigger button on their alarm and a message is immediately sent to the monitoring service identifying the person's name and location. (The trigger button is designed to prevent people from pushing it accidentally). The operator then calls the user to make voice contact by phone or through the loudspeaker on the base unit.

If the customer answers, the operator will ask what has happened to determine what level of care is needed. They will also keep talking to the person until help arrives.

The alarm bases are very sensitive and it's possible for the operator to talk through the loudspeaker to a person in

another room. If the user doesn't answer, the operator will call 111 for an ambulance to be dispatched. Most companies will also let a family contact know if a person is being taken to hospital.

Organisations such as St John Ambulance and Freedom Medical Alarms send an ambulance immediately while ADT Security, Bupa and Safe Link provide the option of calling the user's neighbour, family member or friend first, rather than immediately sending for an ambulance. According to Bupa, only 50% of users who activate their medical alarms actually want or need an ambulance. Bupa provides three-way voice communication so the operator can talk to the user and have their support person on the line as well, so that everyone knows what is happening. For some people, knowing they can get help from someone they know encourages them to use their alarm rather than worrying about calling out an ambulance unnecessarily.

The geographical range of a medical alarm "trigger" is similar to that of a cordless phone. They work throughout most homes and provide some coverage in the garden, depending on its size. Longer distance pendants are available for those living on larger sections or lifestyle blocks. All alarm services operate 24-hours a day, seven days a week.

Some base units can have movement sensors added for people living alone with significant health risks. The alarm checks if the customer is up and about when they should be. If the person is not active, the monitoring service will call to try and make voice contact and if that is not possible, emergency help will be dispatched.





Obviously it's vital that users wear the alarm pendant or wristband all day, every day. People sometimes leave them on the bedside table or kitchen bench because they either don't like wearing them or don't believe anything will happen to them that day. Leaving the alarm on the bench is not going to help them in an emergency.

As Internet connections and other telecommunications devices such as fax machines can block emergency signals, most medical alarm companies install a local disconnect device (a telephone adapter) into additional phone sockets in the house. These in-line devices automatically clear the line allowing the alarm to successfully send an emergency signal even if the user has left the phone off the hook.

It's useful for anyone living alone to have a lockbox with spare key secured discretely outside of the house. If there is an emergency and no-one inside can open the door, then the monitoring service will notify ambulance staff of the location and code of the lockbox so they can gain access without having to break in.

ADT Security, owned by ADT Armourguard, is one of the largest global electronic security companies. ADT Security also offers a complete in-home 'back to base' security system which provides 24/7 coverage for all alarm situations including movement sensors, smoke alarms, medical alerts and panic buttons. This system provides



medical and personal assistance as well as protection from burglary or fire emergencies whether the customer is at home or away.

Safe Link is a New Zealand owned and operated business based in Tauranga which offers personal medical alarms nationwide. The company is an accredited supplier of monitored medical alarm systems to the Ministry of Social Development and a member of the Telecare Services Association of NZ. Kiwi Concern Medical Alarms (also now owned by ADT Security) uses 'Erica', a personal medical alarm system designed and built by Chiptech in Christchurch. Their 'Pearl' pendant, complete with red illumination, is one of the more attractive alarms and can be worn on a neck chain, as a wrist band, belt buckle, or even mounted on the wall. They also offer 'easy-press and blow' pendants for those with disabilities and have a range of wireless smoke detectors, fall detectors, inactivity sensors and door open sensors available.

Kiwi Concern has recently developed a new medical alarm system for those who don't have a home phone. The Ness GSM Medik-Link provides a GSM cellular pathway for communication in the absence of a landline. It's ideal for 'Naked phone line' households and for those in remote locations where reliable GSM dialer monitoring is needed.

Pricing for monitored alarms is consistently around \$20 per week or about \$1000 per year. However, there is wide variation in consumer contracts and cancellation policies amongst the various companies. Some, such as Signature Security and Homeguard Medical Alarms have a minimum 36-month term. Bupa Care Services offer a 24-month minimum term with an early termination fee, while St John has a 3-month minimum term and Freedom Medical Alarms have a 30-day minimum unless you are switching supplier. Kiwi Concern, however, has no compulsory term of agreement.

Consumer Magazine encourages prospective buyers to check the terms and conditions before they sign a contract.

Some companies such as St John Medical Alarms and Safe Link also offer an in-house demonstration and a free trial period of up to a month.

The Ministry of Social Development (MSD), through Work and Income, is the main funder of medical alarms because it provides subsidised alarm monitoring for people with a disability or health condition. People receiving a Disability Allowance need to visit their doctor and get a medical

alarm certificate to confirm that the alarm is needed for their health and safety.

ACC also sometimes covers the cost of medical alarm services for patients recovering from accidents, and Veterans' Affairs provide financial assistance for medical alarm costs for war veterans.

In 2012 the MSD conducted a major review of alarm-monitoring companies and developed a 'Code of Professional Conduct for Approved Suppliers of Monitored Medical Alarms'. The department also leveraged its position to negotiate cheaper prices with suppliers and now requires fair cancellation policies. As a result of these changes, the industry has set up its own Code of Practice and Code of Ethics as well as a complaints process under Telecare Services Association of New Zealand.

There are of course alternatives to medical alarms such as setting up a landline or mobile phone to provide a cost-effective safety net. A mobile phone can provide a relatively inexpensive alarm system. It also has the advantage that it can be used further afield – not just at home. The phone can be set up with a speed-dial key to call a neighbour or family member or to dial 111.

Telecom offers a service for touchtone phones called 'Hotline' which automatically calls a pre-programmed number if the phone receiver is removed from the hook or if you press the "call" button on a cordless phone. TelstraClear offers a similar service called 'Auto dialing' where if the receiver is left off the hook for more than 8 seconds your phone will automatically ring a preset number.

These services are available in most areas with the usual local, national, mobile or international call charges applying.

According to Consumer Magazine, falls are the single largest cause of injury for New Zealanders and the second most common reason for using ambulance services. Every year 1 in 3 people over the age of 65 have a fall. For those over the age of 80 the rate increases to 1 in 2 (Source: Accident Compensation Commission). Often the amount of time it takes to get help determines how quickly a person recovers from a fall or any other medical emergency.

Medical alarm monitoring systems support people's freedom and independence by providing a sense of safety and peace of mind in the home. With quick access to emergency help at the press of a button, older people and those with disabilities feel more capable of living independently without compromising their well-being.



Power supply cabinets

- Mounts for our 5 most popular models of power supplies; 6 key-hole anchor points for easier mounting
- Lift off hinged doors for added convenience
- Louvre ventilation on doors
- Roller ball reed switch provides anti-tamper to front and rear of cabinet
- 6 x 25mm knockouts, 2 each sides and bottom
- Medium cabinet holds 5 x 7 A/h batteries
- Large cabinet holds 14 x 7 A/h batteries
- Cam lock for security
- Front lip to retain batteries and for additional strength
- Removable shelf and removable back plate to facilitate easy bench mounting of equipment
- Lip return on door for greater rigidity
- Durable powder coated white finish
- Heavy gauge 1.2mm steel

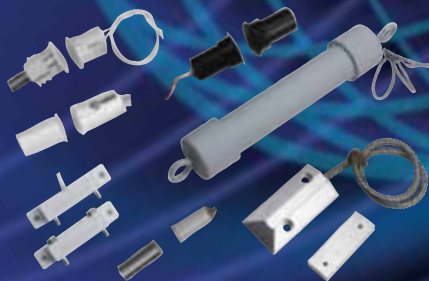
Designed, tested and produced in New Zealand.



Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden
Auckland P O Box 8329 Symonds Street Auckland
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881
0800 FOR LOK www.loktronic.co.nz

20238_PSC



total reed switch solutions from Flair

From closed loop, open loop to SPDT, we've got the lot.

Talk to Loktronic now about our comprehensive range of Flair Reed Switches. Not only for "standard" use, but also for specialty applications, from taught-wire types to waterguards, from collared to stubbies, from overhead door with offset to floor contacts, from latchguard to sub-miniature, from push-fit to surface mount.

Flair reeds from Loktronic: an unbeatable combination.

Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden
Auckland P O Box 8329 Symonds Street Auckland
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881
0800 FOR LOK www.loktronic.co.nz

20237_FL



Loktronic for power supplies

Source all your power supply requirements at Loktronic and choose from a range of over 20 ex stock options, with 100's more to select from.

Complete range of monitored security PSUs in 12 and 24 VDC from 2.5 A - 20 A. DIN rail units in 12 and 24 VDC from 10 - 100 watts. Plus, inline and Plug packs and DC/DC converters.

Power supplies from Loktronic - a great deal.

Loktronic

Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
www.loktronic.co.nz

20757_BP



ASSA ABLOY



FUJINON



NETGEAR®

Auckland: (09) 415 1500 • Fax: (09) 415 1501 | Wellington: (04) 803 3110 | Christchurch: (03) 365 1050 | E

CRK

Professional Precision

Ph: 09 276 3271

www.crknz.co.nz

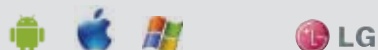


LG LNV7210R

2 Megapixel full HD 60 fps SMART Network IR Vandal Dome Camera

- 3~9 mm F1.2 (x3 Compact Zoom max 60 fps @ 1920 x 1080)
- Remote Motorized Pan/Tilt
- Mobile Monitoring iPhone, Android & Windows
- 108dB of Wide Dynamic Range
- H.264 (High Profile Supported) / MJPEG
- Built-in Video Analytics:- Defog, Audio/Face/Tampering Detection
- Micro SD Card Recording available
- Vandal-Proof, IP66

iPhone, Android and Windows compatible.



CRK

Professional Precision

Ph: 09 276 3271

www.crknz.co.nz



LRH7160D

24CH Megapixel Hybrid Digital Video Recorder

- Analog 16CH+IP 8CH,
- Analog 8CH+IP 16CH
- HDMI output 1920 x 1080 Display
- Max. Resolution : Up-to 3Megapixel
- Mobile Monitoring iPhone, Android & Windows
- Time and Date Sync from NTP Server
- Automatic Backup by Schedule, Health Check (HDD)
- e-SATA for Quick and Easy Archiving
- Dynamic IP Support for DDNS / DHCP

iPhone, Android and Windows compatible.



CRK

Professional Precision

Ph: 09 276 3271

www.crknz.co.nz



Real Time IP Kit Plug & Play!

Ganz Real - Time High Definition recorder has everything on board (Built inDHCP, POE)

- enabling a quick plug and play system. Eliminating the need for external switches and complicated Networks.

- 1 x Ganz 4CH NVR
- 2 x Ganz HD Dome Cameras
- 1 x 22" LG HD Monitor
- 1 x 4GB Usb flash-disk
- *Optional Cable available

iPhone, Android and Windows compatible.





IP Video Intercom

- Wide range of single villa to multi-apartment stations options
- Wide range of control panels with / without phone handsets
- 1.3MP camera on station units
- Control panels also capable of communicating with Dahua IP CCTV cameras
- 2 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz
www.itplus.co.nz



HD-SDI CCTV

- Wide range of true-WDR full-HD (1080P) HD-SDI cameras
- Wide range of low to medium to high-end HD-SDI DVRs
- HD-SDI accessories
- Built-in DDNS client and user-friendly GUI on DVRs
- 3 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz
www.itplus.co.nz



Smart IP Access Control

- Wide range of standalone to fully scalable IP based access-control devices
- Reader/controller units also available on Weigand & RS485
- Fingerprint, Facial & IRIS based access control
- RFID & Keypad based access control
- 2 years b2b warranty

RESELLER ENQUIRIES WELCOME



Ph: 09-950 4940 | E: info@itplus.co.nz
www.itplus.co.nz

AIPHONE®



BOSCH

ZoneTechnology
Your Security Supply Partner

mail: sales@zonetechnology.co.nz | www.zonetechnology.co.nz



Loktronic for gate locks

Choose from a comprehensive range of 23 models of electric gate and outdoor locks for a wide range of applications.

6 models from the famous Loktronic stable, and 7 imported models with holding forces from 300kg, 550kg, up to 740kg; all locks complemented by accessories to facilitate fitting.

7 models of strikes by Trimec and eff-eff, Rim mounted locks from CISA, and a versatile range from Securiton and Interlock.

Gate locks from Loktronic – a wise choice.

Loktronic



Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
www.loktronic.co.nz 20756_BP



Key switches

This versatile product range is produced with two functions

Momentary contact (90°)

Turns 90° clockwise from vertical to turn on

Maintained contact (180°) locked on or locked off

Turns 90° clockwise from vertical to turn on

Turns 90° anticlockwise from vertical to turn off
SPDT switch 5amp rating

Accessories are: Key switch mounting bracket
escutcheon for mounting bracket

Suitable for: Access control, air-conditioning,
lifts, lighting.

Supplied random keyed. Can be master keyed.

Client's own key cylinder can be converted.

Front or rear fixing.

Designed, tested and produced
in New Zealand by Loktronic.



Loktronic



Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
www.loktronic.co.nz 20681_KS

Loktronic Power distribution module



The Power Distribution Module allows the removal of power to a group of doors on a fire alarm activation whilst conforming to regulations. Provision for individual fused power supply to each door lock.

Red and black uncommitted terminals to facilitate distribution from power supply or battery, to load.

Comprises

- Fire Drop Relay DPDT 12 VDC • 6 x 2 Amp FU 500
- Terminals with LED Indication • 2 x Red Terminals
- 2 x Black Terminals • 1 x DIN Rail
- All terminals are labelled.

Designed, tested and
produced in New Zealand.



Loktronic



Loktronic Limited Unit 7 19 Edwin Street Mt Eden
Auckland P O Box 8329 Symonds Street Auckland
1150 New Zealand Ph 64 9 623 3919 Fax 64 9 623 3881
0800 FOR LOK www.loktronic.co.nz 20239_PDM

Silo mentality leads to passivity in looming fire protection crisis

Keith Newman discovers a communication breakdown between the trades and the fire protection industry, a lack of clear standards for compliance sign offs and the Government downplaying revelations that the nation's commercial buildings are riddled with non-compliant passive fire protection (PFP) systems.

A looming crisis impacting many of the country's commercial and public buildings is being blamed on slack workmanship, building owners, developers and subbies trying to save a buck and general ignorance about how passive fire protection systems should be installed and maintained.

Concerns about sub-standard passive fire protection (PFP) systems, which are designed to slow the spread of fire and smoke, have been raised by the building, engineering and fire industry for years.

A series of reports from the Building Research Association (BRANZ), the Institute of Professional Engineers (IPENZ), the Fire Protection Association (FPANZ) and the Fire Services Commission have highlighted the issues in recent years.

However, more rigid testing, the leaky building crisis and increased seismic checks after the Christchurch earthquakes have confirmed the problem is endemic, and the Government is being urged to tighten up gaps in legislation.

The pressure is also on for the trades to lift their game when it comes to working with PFP systems; for professional fire engineers to be more widely used and for building consent authorities (BCAs) and others who sign off on PFP work to be better educated and have standardised certification.



Ron Green, Chairperson of the Association of Building Compliance (ABC)

Ron Green, Chairperson of the Association of Building Compliance (ABC) and a Director of Building Compliance and Fire Consulting and Fire Group Consulting, has warned for many years that inadequate PFP systems are placing building occupants at risk, jeopardising business continuity and potential insurance cover.

He claims 99 percent of the buildings he inspects don't comply with the Building Code, and less than 10% will be only 60% compliant.

Green, with 33-years' experience in the fire protection industry, claims most buildings in the country could be shown as deficient and describes the situation as systemic.

He says there is a general lack of understanding, knowledge and planning across the industry and the blame must be shared because the Building Act makes various entities accountable.

The prime responsibility is with the building owner and after construction those responsibilities continue as the owner requires an annual WOF to confirm everything on the consent and compliance schedule has been inspected.

BCAs must check everything is compliant before construction and sign off again at the end to say everything is done correctly.

Fire stopping failures

While some sign offs have missed non-compliant fire separations or inadequate workmanship, the bulk of issues arise when careless or uninformed tradespeople punch holes for cabling or pipes then fail to 'fire stop' them to the required standard, or at all.

Green is calling for wider use of passive fire specialists and wants fire stopping to be subject to a third party inspection like other fire protection systems. "Even a simple penetration has special requirements and should be

“99 percent of the buildings I inspect don’t comply with the Building Code and less than 10% will be only 60% compliant.” Ron Green Chairman of the Association of Building Compliance.

inspected when it’s done; it’s too late when construction’s complete.”

Essentially, he says, poorly built, inadequately installed and badly maintained systems, impact everything from high rise apartment buildings to commercial buildings, hospitals, rest homes, office blocks and local and central government structures.

“I inspected a new building recently and 90 percent of the fire stopping was incorrect, rating from bad to poor with contractors having to do reworks to get it right,” says Green.

Another recent example is an accommodation building which had no fire rated walls within the ceiling void above fire rated doors. “Obviously the door had been moved in an alteration but the builder did not obtain a building consent for altering a specified system.”

Green speculates the overall problem could be worse than the leaky buildings debacle. “You can test fire alarms but you don’t have fires all the time to expose the problems with passive protection...a single event could bring catastrophe.”

Amendments to the Building Act in 2012, forced the listing of fire and smoke separations as “specified systems”, highlighted these issues, although it’s alleged this also added complexity and wasn’t followed up with trades and compliance education.

Currently Green claims fire stopping is signed off on ‘producer statements’ and many of these are “falsely signed”. He says many tradespeople “try to get away with it and hope the BCA doesn’t pick up their mistakes.”

He claims there’s a culture among the trades of cost cutting and seeing if they can get away with shortcuts in passive fire protection and fire stopping. “Some just don’t know it’s wrong while others know better. Rather than blaming the inspector they should get it right first time,” says Green.

Legal minefield ahead

Adina Thorn, Principal of Adina Thorn Lawyers in Auckland, believes we’re about to see a lot more court cases against councils, builders and others who’s decisions have resulted in non-compliant fire protection structures.

Thorn, a leaky home specialist concerned with the assembly of buildings, fire rating, classification and protection, suggests it’s still early days for determining how many cases will end up in court.

“If the council has given a CCC (Code of Compliance Certificate) then it’s their responsibility and they might be liable. It all depends on what is considered reasonable.”

Like Ron Green, she believes a lot of CBD buildings constructed over the past 20-years have “some fire issues”. The challenge is who is going to take responsibility; the builder-developer who decided to use non-compliant materials, councils who signed it off or fire engineers if they were involved?

Thorn says she’s surprised at the magnitude of the problem and judging by the inquiries she’s receiving, building owners are nervous about fire safety. “There’s a real concern. People in big buildings in particular are anxious and have a lot of questions about fire safety.”

There’s a growing discussion around fire classification and the different rules for who’s responsible if the Gib is not fire rated and if it is, why it’s only gone half way up the wall instead of all the way?

While the information varies on a case by case basis, council processes are being challenged. “There’s a lot of unanswered questions... What process was council adopting during this period and how confident are they in that. I suspect we only know one percent of the information at the moment.”



*Adina Thorn, Principal of
Adina Thorn Lawyers, Auckland*

“There’s a real concern. People in big buildings in particular are anxious and have a lot of questions about fire safety.” Adina Thorn, Principal of Adina Thorn Lawyers

Thorn says there appears to be a big gap in knowledge about what councils check for when signing off building consents and COCs. “In my view some of these issues should be determined by a fire engineer or a mechanical engineer who does fire but that’s not what’s been happening.”

Unprofessional protection

Passive fire protection is a special class of building products and materials including flooring, ceilings, walls, doors roller shutters, glazing and dampers in ductwork that are technically specified as fire resistant and rated to prevent flame and smoke from spreading between units, fire cells, floors or into stairwells and lifts.

Even if those systems are built to specification they can be compromised when plumbers, electricians, security, fire, air conditioning and communications specialists, for example, cut holes for cabling or pipes.

While there are very specific ratings for fire wall thickness and how to secure and seal holes, including the use of collars, pillows and sealants which expand in the heat, this is often overlooked through laziness or lack of information.

There’s also some confusion around the lack of accurate documentation that should be available to those who renovate buildings, often resulting in new services damaging fire protection systems.

While the Ministry of Business, Innovation and Employment (MBIE) which took over from the Department of Building and Housing last year, continues to update aspects of the Building Code, documentation covering PFP is only a guideline with no standing in law.

Green and others want a more robust regime, and fear that with so many sub-standard installations signed off by councils, a false sense of security has been created.



Andrew Cleland, CEO of the Institute of Professional Engineers (IPENZ)

Peter Thorby, MBIE's Manager of Building Standards who looks after the Building Code, says he's seen no evidence a high percentage of buildings are non-compliant. "We're aware of some issues but nothing suggests a widespread or endemic issue that needs to be dealt to in particular."

If there are examples of fire resistant Gib not going all the way to the ceiling, he says the owner should be informed. If nothing happens it should be reported to the local authority. "It's human nature to miss things; if there was a mistake with the code of compliance we certainly encourage IQPs to point this out."

Thorby says theoretically all the investigations and sign offs should make the system self-correcting from design to maintaining annual compliance checks through the building warrant of fitness (WOF).

"Inspections by building owners and their agents should pick these things up and require the tradespeople go back and fix them."

He's not seen any evidence of materials being used inappropriately although surveys, including the BRANZ 2008 report, do give examples of "some things not being done properly". As a result MBIE went through its own process highlighting the importance of "doing PFP work correctly".

Thorby says it determined the "deficiencies...were best addressed through education and awareness raising. New constructions since 2008 should be fine."

As part of its technical review of territorial local authorities, MBIE encouraged them to go onsite and have a high-level check of specified systems.

"We're not advocating that they go crawling through roof spaces or under floors just double check on the work of IQPs."

Push for professionalism

The Institute of Professional Engineers (IPENZ) continues to argue that safety critical structural and technical work, including passive fire protection, should only be done by chartered professional engineers.

Chief Executive Andrew Cleland says the weakest link in the system is that building consent authorities aren't consistent in who they accept work from including those with no fire engineering knowledge.

What's needed is to get the right people doing the work, the right regime for checking proper implementation and good systems in place. He says that's been a problem and there's still some way to go to remedy this.

IPENZ reviewed these issues several years ago; "I don't think the world has shifted on much since then," says Cleland. He continues to raise the issues with MBIE. "Our argument is that their attempts to improve accreditation with the building consent authorities should have happened a lot faster."

Cleland suggests ideally MBIE should require all passive fire protection to be considered as restricted building work or persuade every building consent authority in the country to only accept design work from chartered professional engineers.

Currently an acceptable or "cook book" approach is usually a highly prescribed and "conservative" way of doing things and does not need a professional engineer while "alternative" or custom one-off, individual designs, do.

Cleland says the cook book approach is often quite expensive so building owners prefer the alternative method which has to be peer reviewed.



Left. A crude attempt at sealing around cabling in a fire wall (courtesy Mike Green)

Right. The way it's supposed to be done. Courtesy Hilti NZ

"The processes of building consent authorities lack rigour and their behaviour is highly variable."

IPENZ Chief Executive, Andrew Cleland

Both involve complex interactions. Mistakes will inevitably occur if the consenting authorities fail to engage the right people or don't have the in-house skills to pick up "inadvertent behaviours".

Cleland says good fire engineers and chartered engineers are frustrated with what they see. "The processes of building consent authorities lack rigour and their behaviour is highly variable."

All IPENZ can do under the current statutes is make available a list of chartered professionals who can do this work.

MBIE's Dave Thorby agrees there's no limitation on who can do commercial building design work and it doesn't have to involve a professional fire engineer. "There's nothing in the legislation that says the designer or builder must be licensed for that work."

With passive fire protection, he says, it's always important that there are clear directions to designers, particularly around smoke and fire control and fire walls. "There's nothing new in that space."

To ensure designs comply, the "backstop check" is the building consent authority. "I would expect that most builders would be aware of what passive fire protection looks like and at the end of the job the sign-off process should be reasonably robust. Things shouldn't slip through but they can."



Education lacking

What all parties do agree on, is that effective education on acceptable PFP systems and their maintenance, particularly among the trades who come along after initial installation, has left a gap so big you could drive a fire truck through it.

While tighter inspections will continue to unravel legacy problems, MBIE and various fire and building industry and training groups are determined to ensure these aren't replicated, particularly through the Christchurch rebuild and the major construction boom in Auckland.

The challenge often has more to do with ignorance about fire stopping requirements than builders or owners being devious, says Ron Green. "The knowledge is not there, the planning is not there; if people don't know what they're doing, how can they get it right?"

Brian Davey, former NZ Fire Service Operations Manager and Past President of the Institute of Fire Engineers, says changes to the Building Act include a lot more technical detail about materials and installation.

He says the MBIE should have ensured those changes were reflected in the education of the trades and spelled out in the simplest possible terms, not hidden away in technical documents.

While MBIE publishes a lot of best practice documents they simply leave it up to professionals to comply, says NZ Fire Service Engineering Manager Simon Davis. "We need a more standardised approach and a way to educate everyone about their responsibilities."

He says it can be a very expensive process to rectify problems post-construction so it's essential to get things right first time. Rather than dealing with a 50-page report, he suggests everyone in the construction process, including the IQPs who come in after the fact, should be dealing with clear documents and drawings so they know exactly what's required and how to comply.

"What we're talking about here is nuts and bolts, trade practices, things that happen on site. You can put all your belts and braces in but at the end of the day you can't inspect quality into a building or do it afterwards."

MBIE comfortable for now

MBIE believes its documentation is clear but is happy to look at anything that might not be.

"We have conversations with all sorts of people who would like to see things done differently but at the moment we're relatively comfortable that the system as

a whole is well designed," says Building Standards Manager Peter Thorby.

Most tradespeople including electricians, those who install air conditioning units, sprinklers and fire alarms must have their work signed off as part of the Code of Compliance (CoC) but that wasn't the case for PFP systems until recently.

Under the Building Act 1992 fire separations came under 'the means of escape from fire', and IQPs "who didn't know enough" routinely approved sub-standard installations, says ABC Chairman Ron Green.

When the Building Act was updated in 2004 'Fire and Smoke Separations' were designated as separate specified fire systems and only through amendments in April 2012 were they forced to replace 'Means of Escape from Fire' on the compliance schedule.

There is, however, no requirement for contractors or sub-contractors to be trained in the installation of PFP systems and no compliance checking for fire stopping. "There needs to be a better quality assurance system that includes a statement from those who install fire stopping systems," says Green.

MBIE's recommendations for engineers, compliance officers and IQPs to validate passive fire protection systems remains open to interpretation and until recently little training has been available.

Dave Gittings, MBIE's Manager of Consent System Capability, says the Building Code only specifies the outcome to be achieved not what has to be done. Other documents recommend acceptable solutions and verification of methods of compliance, although there's nothing mandatory.

"The designer has initial responsibility and if the application for consent meets those requirements a building consent must be issued. The test for the consent authority is compliance with the Building Code." Gittings insists "it's simple stuff"



A badly stopped collar for PVC pipe penetration in a firewall

MBIE remains supportive of organisations that highlight awareness and education in their sectors. "We certainly need better education across the trades to ensure they're aware of when they are penetrating a fire wall and how to fix it." Gittings says it's important those who put in services, including TV cabling, step back and see the fire wall is there for a reason and needs to be sealed properly afterwards. "It's not okay to leave a little hole here and there; 40 holes is not good."

Green, FPANZ and Andrew Cleland from IPENZ agree there needs to be regular checks during the construction process by people who know what they're looking for to ensure irregular practices don't destroy the integrity of fire systems.

"You can do it with a stick or educationally. If you have a combination of those two and incentivise people not to stuff it up, that's far better than beating them with a stick afterwards," says Cleland.

He says inspection is not necessarily the answer, what's needed is "a more holistic approach to quality assurance".

While still engaging with MBIE over passive fire protection issues, Ron Green continues to consult with BCAs and run training sessions for fire engineers, builders, IQPs and BCAs. "Unfortunately it's the trades that don't attend the sessions."

He's had builders and contractors admit their previous work was done incorrectly and others concede they've signed off things that are unsafe. "They're quite shocked when I show them the areas of concern... it's often a wake-up call."

Compliance cost shock

Growing awareness of non-compliant legacy systems is fuelling greater attention to detail during annual building WOF checks, particularly as building owners apply for consents for alterations or seismic upgrading.



A ceiling cabling installation carefully fire stopped the professional way. Courtesy HiltiNZ

As councils and IQPs tighten up their practices some building owners are getting a nasty shock when they discover costly remedial work is required.

NZ Fire Services Engineering Manager, Simon Davis, agrees seismic problems are having a direct impact on fire protection, particularly in old unreinforced brick and mortar buildings in villages and older suburbs around the country.

He says, the extent of remedial measures will in some cases depend on what the country can afford. "Putting steel frames into some of these buildings is presenting a significant challenge and that's before you start addressing the fire safety systems."

Davis has been arguing for years that there should be broader industry knowledge of PFP systems and how everything ties together, suggesting this has often only been given lip service. It's now a major issue, "the devil is in the details...If you don't know what it is that you are enforcing it's very difficult."

Under the Building Act licensed building practitioners (LBP) have to be trained to a certain level. "In an ideal world everything would be fine but we live in a world where people are struggling; it's competitive and subcontractors who are being screwed down have to find a buck somewhere."

Often he says the lowest price gets the job and "you only get what you pay for". What's needed, he reiterates, is for fire engineers and private and council building inspectors to upskill and play a more active role from the design process right through to post-construction checks.



*Simon Davis,
NZ Fire Service Engineering Manager*

Davis says right from the beginning fire engineers should make it clear what their expectations are and then ensure this is carried through. Design drawings should show the resistance ratings and where the doors are, detail the penetration points for various services and how to treat them.

"We need to make sure the drawings provided to the contractors and subcontractors are thorough and depict the routes for services to go through the firewalls and the details of how those penetrations will occur."

Standards-based start

Seasoned fire consultant Brian Davey says lack of consistency across consenting authorities is a worldwide problem, with different councils and officers having different interpretations of the same wording in legislation.

For example the view of some New Zealand councils that stand-alone smoke alarms are part of a security system requiring a code of compliance while others say they're part of an early warning system for empty buildings. He fears over regulation in this case will be a deterrent to use.

Some authorities have views based on how one building inspector thinks and that's how everyone ends up doing it. As for Building Act compliance for passive fire protection, he suggests there's a need for greater clarity and "a process of determination...to get consistency."

Recent amendments to the Building Code "Protection From Fire, Acceptance Solutions and Verification Methods, Practice Note 22 (PM22)", are seen as a step in the right direction, more clearly spelling out who's responsible for what.

The best practice document published by the MBIE with buy-in from IPENZ, the NZ Fire Service and others, helps identify all the information that should be provided to contractors and subcontractors.

PM22 is a timely contribution in helping to bring some cohesion to what NZ Fire Service's Davis says has been a very "disjointed industry" with the building industry often having little to do with the fire protection industry.

FPANZ formed a passive fire group in 2010 with the goal of establishing common practices and awareness around passive fire protection for all trades. NZQA qualifications are currently under review, including a proposal for a registered inspections qualification covering PFP for private and council inspectors.

Getting all the parties together in an interest group that's essentially a who's



*Brian Davey, Independent Fire Consultant and
Past President of the Institute of Fire Engineers*

who from the various sectors has been a great achievement, says Davis. Rather than working in small pockets it brings all the pieces of the jigsaw together in one place and "gives some substance to the process".

Davis commends the approach taken by Ron Green and his company which struck an arrangement with a regional hospital board that only agreed fire protection materials be used on its new three building construction.

A fire engineer will oversee all stages and contractors must undertake basic training on installation procedures. "That's always been the most challenging aspect but it's also the way to do it," he says.

Speedy solutions essential

The reality is that more stringent investigations into the causes of fires will focus on how well fire protection systems have worked. If there's evidence of a failure, the owner, the council, the builder, tradespeople or the IQP who signed it off are likely to cop part of the blame.

While the reputation of the fire protection industry is being challenged through allegations about sub-standard systems in our commercial and high rise accommodation buildings, there's also an opportunity to take the lead in plugging the gaps.

Improved education, proposed standards and a greater role for fire engineers throughout the building and consenting process is clearly a good starting point although ensuring best practice is implemented across the sectors remains a major challenge.

As industry groups like FPANZ, IPENZ and BRANZ determine ways to fix the errors of the past and prevent them being replicated in current building projects, the underlying feeling is that the trades and MBIE must take their recommendations seriously before a real world disaster results in another round of finger pointing.

Smoke is the killer



The fatal fire at Lakanal House apartment buildings in South London in 2009 got out of hand partly through the use of non-compliant building materials which allow smoke more rapidly between floors.

Failure to properly install, check and maintain passive fire protection (PFP) systems that prevent the flow of smoke from the source of a fire into adjoining rooms or floors, not only threatens lives but could place liability on those who signed off the work.

While smoke detectors and sprinklers may quickly alert people to a fire, Ron Green Chairman of the Association of Building Compliance (ABC) says badly constructed fire walls and inadequate fire stopping allows smoke to travel quickly between rooms and floors.

"We did a test with the NZ Fire Service and I was astonished that smoke filled a room within five minutes through holes that had not been properly sealed."

He says New Zealand should take heed of what happened in the MGM Grand Hotel and Casino fire in Los Angeles in 1980, where smoke from the ground floor killed more people in the upper floors than the fire did.

Smoke had migrated through the seismic joints. "It's the smoke in the air that's the killer".

Green says New Zealand building owners, builders, sub-contractors and consenting authorities need to get it right when designing and maintaining PFP systems.

Imagine a fire in a hospital where there are holes in the walls or ceiling, he asks. "If smoke got in where people thought they were safe it would just be a nightmare, particularly if staff were trying to move patients around in the early hours of the morning."

There's no shortage of evidence of what can go badly wrong if PFP systems don't work as they are designed. For example the Dohar Shopping Mall fire where smoke quickly overwhelmed people or the Lucknal House apartment block fire in London.

Brian Davey was an expert witness in last year's inquiry into the 14-storey Lakanal House apartment block fire in South London which got out of hand for a range of reasons including the use of non-compliant building materials. The fire claimed six lives.

"Building inspectors need to closely and regularly monitor how tradesman on site are installing these things," says Davey.

Like Simon Davis of the NZ Fire Service says "a saucepan with a hole in it is not going to hold water and it's the same with fire and smoke, it's going to find that weakest spot."

Mystery shopper shortfalls

As part of his advocacy role, Ron Green Chairman of the Association of Building Compliance (ABC), plays the mystery shopper, turning up at trade outlets to ask for advice.

On three recent occasions, he asked what was the appropriate fire rated system for a job he described clearly and the wrong product was recommended.

"The information these people are giving needs to be right. I needed something that would give a one hour rating for cables passing through a plasterboard wall but they offered a fire rated sealant tested for gaps within concrete. They just didn't know."

Because the label stated 'Up to 4 hour rating' he says the assistant thought this was the answer.

Green says each manufacturer has different tested systems to achieve a designed fire resistance rating for varying gaps and/or penetrations through plasterboard or concrete. Each system has specific installation requirements and limitations to achieve those ratings.

That might include maximum hole size, minimum and maximum gap between cable or pipe and the wall, pipe size, the depth of sealant and what needs to happen if there are two layers of plasterboard.

He says if a contractor doesn't know the requirements and limitations of each system, they'll choose the wrong product. "That can be further complicated if they rely on the shop assistant to advise them because often they don't know either."

Trade knowledge lacking

Green insists that this should be part of the knowledge of tradesmen installing plaster board and making penetrations through a fire wall or floor. "It's a skill that should be part of their trade but there's no requirement that they should have this training and those who're signing this work off have little knowledge either."

Simon Davis from the NZ Fire Service, says the providers of passive fire protection systems need to be given their due.

"They've had them tested and have put out technical literature. It's up to the various parties to take the time to understand what that means and apply it."

Gib product for example is sold as a system. "It has to be installed correctly for it to work including how you screw it together, the sub-strate, how you finish it, any preparations and how you finish those."

He says more building control authorities are now beginning to ask for producer statements to ensure these areas are covered off.

BRANZ to investigate PFP quality claims



The Building Research Association (BRANZ) expects to embark on a detailed investigation into ongoing concerns about the quality and effectiveness of passive fire protection (PFP) in modern commercial premises later this year.

The independent building industry-owned body which consults and provides research and resources is currently working with industry stakeholders on the best methodology to undertake this work.

“What’s being investigated is the quality of delivered or installed passive fire protection; not just a snapshot in time but ongoing issues of maintenance and the effectiveness over the life of the building,” says BRANZ Fire and Structural Engineering Services Manager, Greg Baker.

BRANZ began a four year, million dollar, research project in October 2013 entitled “Effectiveness of Passive Fire Protection” as part of its Building Research Levy investment programme.

Once it’s determined the best way to gain access to and inspect buildings it expects to begin inspecting 20-30 mainly high rise commercial buildings constructed after 1991 when the first performance-based Building Code was introduced.

This is a follow up to a 2008 Fire Protection Association of New Zealand (FPANZ) research report which surveyed a smaller number of buildings.

BRANZ continues to maintain that PFP systems need to be designed, specified, installed, inspected, certified and maintained by professionals who have the necessary skills to achieve an effective and durable life safety outcome for building occupants.

The report will look at materials and installation issues with a focus on ceilings where special care is expected. “In multi-storey buildings there’s usually a concrete reinforced roof with a suspended ceiling below where services such as lighting are placed,” says Baker.

Depending on what it uncovers, it may identify specific problems and make recommendations to the Ministry of Business, Innovation and Employment (MBIE), the building regulator, as part of making its findings public.

Compliance shortcuts challenged

“Some clients have agreed to fix up failures and newly generated penetrations while others simply go to another compliance person to obtain a Form 12A in order to gain their warrant of fitness.” Ron Green, Chairman of the Association of Building Compliance (ABC).

The integrity of some fire engineers and independently qualified persons (IQPs) is being challenged as building owners allegedly shop around for less rigid sign offs on sub-standard fire protection systems.

Often owners become frustrated when they learn of the cost of remedying issues originally signed off by councils when it comes time for annual compliance testing for their building warrant of fitness (BWof) and are looking for someone who will simply rubber stamp that work.

Ron Green, Chairman of Association of Building Compliance (ABC), says a growing number of his members who are IQPs, claim they’ve lost work because they refused to sign off on sub-standard fire separations previously given a certificate of compliance (CCC).

“Some clients have agreed to fix up failures and newly generated penetrations while others simply go to another compliance person to obtain a Form 12A in order to gain their warrant of fitness”.

Green has at times come under fire for his firm stand, for example insisting that the ceiling area be checked to ensure there’s adequate fire stopping above fire rated doors in accommodation buildings.

The reality, he says, is building owners, contractors and IQPs could be liable if inspections don’t cover all the areas relating to fire separations. “If I’m signing something off under the Building Act, I want to make sure it’s OK.” In a hospital, for example, he checks above the ceiling because that’s where the holes are.

Keeping owners honest

In one court case against an IQP who was fined \$50,000, the Judge stated their

role was to keep the building owner honest and the public safe.

The mounting allegations of suspect industry practices come hot on the heels of a series of investigative articles in the Sunday Star Times claiming secret settlements made to building owners by fire engineers and certifiers to fix their stuffups.

In a series of articles in the paper’s business section, journalist Rebecca Stevenson claims out of court settlements relating to a number of Auckland apartment complexes and several other cases, are either before the courts or heading that way.

The paper claims lawyers for leaky building claimants allege one in five claims for defective and shoddily-constructed apartment blocks also involve claims to fix faulty and sub-standard fire and smoke alarm systems.

Stevenson claims the problem of faulty workmanship in fire protection systems is widespread, including cases where non-compliant fire alarm, sprinkler systems and smoke detectors have been discovered.

NZSM has confirmed similar claims through its own research, although sources wished to remain off the record.

And while there’s a tendency to pass the buck, Ron Green says people shouldn’t simply blame council consenting officers who gave the go-ahead. “Under the Building Act the building owner is responsible and some of that responsibility also falls to the designer, the builder and the fire engineer who all have to sign it off.”

Part of the problem is that until recently few people in these roles have had the knowledge about fire stopping, an area Green and his associates specialise in.

fired up protection

ViTECH



LOKTRONIC's expansive product range has just become even wider with these first class **EGRESS** and **FIRE PROTECTION DEVICES** and **PROTECTIVE COVERS**.



STI-1130 Ref. 720-102
Surface mount with horn and spacer
255mm H x 183mm W x 135mm D

STI-13000-NC Ref. 720-090
Flush mount, no horn
200mm H x 135mm W x 65mm D



STI-13510-NN Ref. 720-092
Surface mount, horn and label optional
200mm H x 135mm W x 100mm D

STI-1100 Ref. 720-054
Flush mount with horn
255mm H x 183mm W x 84mm D



STI-6518 Ref. 720-060
Flush mount, no horn
170mm H x 95mm W x 49mm D

STI-13210-NG Ref. 720-094
Surface mount, horn and label optional
200mm H x 135mm W x 100mm D



All **STI 'Stoppers'** are made of tough, UV stabilised polycarbonate. Many can be supplied with or without a 105 dB horn. Other models and sizes available including weather resistant options.

STI-WRP-R-11 Ref. 720-059R

Resettable call point surface mount, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass. **IP 67**



STI-RP-WS-11/CN Ref. 720-052W

Resettable call point surface mount and flush, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

STI-RP-GF-11/CN Ref. 720-051G

Resettable call point surface mount and flush, DPDT. Positive activation mimics the feel of breaking glass. Visible warning flag (pictured) confirms activation. Simple key to reset operating element - no broken glass.



STI-RP-RS-02/CN Ref. 720-058

Resettable call point surface mount and flush, SPDT. Positive activation mimics the feel of breaking glass. Visible warning flag confirms activation. Simple key to reset operating element - no broken glass.

STI-6255 Ref. 720-042

Mini Theft Stopper discourages inappropriate use of equipment. Sounds a powerful 105 dB warning horn when activated. Tough, ABS construction. Reed switch activation for cabinets and display cases or unique clip activation for freestanding equipment. Does not interfere with use of protected fire fighting equipment. Compact design 85mm H x 85mm W x 25mm D.



STI-6720 Ref. 720-047

Break Glass Stopper. Keys under plexiglas. Protects emergency keys from inappropriate use. Keys remain visible. Fast, easy installation. Simple, inexpensive plexiglas. 3 year guarantee against breakage of the ABS housing within normal use.



Battery Tester Ref. 730-100
ViTech rugged steel case 5, 15 and 30 amp battery tester for fire and alarm use.



Fire Brigade Alarm: (Closed/Open) Ref. 730-201
ViTech branded Type X and Type Y models with temperature compensated pressure transducers with digital display showing pressures for defect, fire and pump start.



Anti-Interference Device
Ref. 730-400 series
ViTech AID for sprinkler valve monitoring; fits all ball valve sizes.



ViTech products are designed and produced in New Zealand.

Loktronic

Loktronic Limited Unit 7 19 Edwin Street Mt Eden Auckland
P O Box 8329 Symonds Street Auckland 1150 New Zealand
Ph 64 9 623 3919 Fax 64 9 623 3881 0800 FOR LOK
mail@loktronic.co.nz www.loktronic.co.nz



More than wet stuff on the hot stuff

- Community focus for Haumoana brigade

Keith Newman adds a personal touch to a story about the award winning Haumoana Volunteer Fire Brigade in the small Hawke's Bay community where he lives.

On 31 July 2013, life changed at our coastal home in Haumoana, looking out toward Cape Kidnappers. The extension ladder my wife was using while cleaning the guttering gave way and she dropped three metres onto the cobblestone courtyard, landing on her back with a sickening thud.

I was metres away in my office and after dialling 111, all I and a neighbour could do was insist she remain exactly where she was. First on the scene was an engine from the Haumoana Volunteer Fire Brigade; a team of four calm, collected individuals managed the situation admirably until the ambulance arrived 10 minutes later.

Paula spent a month in hospital and eight months in recovery. Those who were first on the scene continued to ask for an update, making me extremely grateful to be part of a caring community with such a committed volunteer fire brigade.

There are over 8000 volunteer fire fighters in New Zealand and they do



The Haumoana Volunteer Fire Brigade 2013



Haumoana Volunteer Fire Brigade Chief Bill Tims

much more than put the wet stuff on the hot stuff. Typically they're well trained for a range of emergencies and like the Haumoana brigade spend an increasing amount of time dealing with accidents, incidents and medical-related emergencies.

In August 2013, the Haumoana Fire Brigade was presented with the 2012 Emergency Management Qualification (EMQUAL) Training Excellence Award; it was the urban or rural fire force that had achieved the highest level of training excellence in New Zealand.

EMQUAL, responsible for setting national standards and facilitating training assessments, had been approaching brigades around the country encouraging them to transform the knowledge and skills they were acquiring into recognised unit standards.

Haumoana took up the challenge with 16 of its 21 members achieving the NZ Certificate in Urban Fire and Rescue Operations, Level 2. "We topped the country for getting the buy in from our members," says Chief Fire Officer Bill Tims. By the time the EMQUAL award was presented another three members had passed.

That's not the first time the Haumoana brigade has stepped up to a challenge to do things differently. In 1996 it was approached by the regional manager of St John Ambulance, concerned it wasn't able to turn out to emergencies within the expected 15 minute timeframe.

"We were asked whether we would be interested in upskilling in first aid and helping our community. We didn't even hesitate," says Tims.

"They trained us, and we were one of the first brigades in New Zealand to sign a memorandum of understanding with St John. We've never looked back." The brigade won a Chief Executive's award for that.

Long-term loyalty

The Haumoana, Te Awanga and Tuki Tuki Volunteer Fire Brigade was formed in 1946 with about 20 members using bucket pumps, beaters, a home-made petrol driven gear pump to draw water from local creeks and private transport including a member's model T truck.

A quarter of a century later in 1971 five of the original members were presented with their 25-year gold star at a function in their honour. Today there are 14 members who have served at least 25-years.

On 8 March 2014 another batch of five got their gold stars in an event attended by two of the surviving founding members, Hugh Baker and Ian Bambry.

Bill Tims, who's been with the brigade for 38-years, 20 of those as fire chief, agrees one of the great assets of the brigade is the loyalty of members and the community.

So what keeps him going? "The excitement of it all. We go to some terrible calls but at the same time we're helping people...it becomes like an addiction."

Generally, he says, people who join the brigade like to give back to the community. What other motive could there be than the sense of adrenaline and adventure that comes with answering the pager and the howl of the siren which often means downing one set of tools and heading to the station to pick up another.

"I always remember as a young fellow, when I joined the Haumoana brigade,



Fire Brigade Promotions Manager Brian Slader

someone said to me, 'you are going to see some funny things but make sure that it stops at the eye before it gets into your brain'."

Tims says, you get to witness people with severe burns, strokes, cot deaths, heart attacks and people who've been killed or battered about in car accidents.

"The thing is you are there to do the best you can possibly do in the situation. It'll still play on your mind but you can't take it on personally...you can only do what you can do."

Quake and appliance upgrade

In 2010 the NZ Fire Service invested \$450,000 on quake strengthening the Haumoana Fire Station originally built in 1958; after all it is in the heart of



Haumoana's 2010 Iveco Eurocargo appliance

an area that faced tremendous seismic upheaval during the 1931 Hawke's Bay earthquake, and still gets its share of tremors.

"The last thing you want is not being able to get out of your building in the event of an earthquake," says Tims. The appliance bays were also enlarged to house a shiny new \$400,000 2010 Iveco Eurocargo engine

On average the brigade receives three calls a week or 110-150 calls a year. "It could be anything from a house fire to flooding, a cat up a tree or someone falling off a roof," says Tims, knowingly.

He reckons 35-40 percent of call outs are medical related. The weirdest? Having to use a jigsaw to cut up a plastic bath after a two year old got his finger stuck down the plughole.

There are neighbouring brigades in Havelock North, Hastings and Napier which still leaves Haumoana to cover quite a substantial area including Clive, Haumoana, Te Awanga and Tuki Tuki Valley.

"Every time our siren goes a paid brigade pump from either Hastings or Napier responds to the same call," says Tims

In 1977 the then Hawkes Bay County Council supplied a tanker to the Haumoana Brigade to use in the area as well as being on call to respond to calls in the wider Hawke's Bay. The Hastings District Council has maintained this relationship with the brigade.

Currently it has a shiny new \$400,00, 2010 green Nissan tanker on station, the fourth tanker to be stationed at Haumoana courtesy of the council. "Whenever we go to a fire call we know we have truck loads of water behind us. They maintain it and we drive it and turn out wherever it's needed in the district."

Adapting to local needs

Following the appointment of new NZ Fire Service National Commander Paul Baxter in January 2012, Tims says there's been more of a focus on each fire station meeting the needs of their local communities.

"We are a fire and rescue service now and will continue to grow and adapt based on community expectations although balancing that with what can be practically achieved," says Tims.

Being a coastal community with hills on the southern side and rivers and drains

that flow out to the sea, presents its own challenges including inundation and flooding.

Stop banks and a groyne at the Tukituki river mouth now provide greater confidence than in the 1970s when the river overflowed and parts of the town including the fire station, were flooded.

The most recent event was Easter 2011 when torrential rain over a 48 hour period saw the brigade initially responding to help a homeowner pump out his flooded house and ending with 30 homes evacuated and many residents isolated by floodwaters.

Water poured down off the hills, a new drainage system that hadn't been fully commissioned failed, the Te Awanga lagoon overflowed and a number of streets and the local motor camp were inundated.

The Haumoana and Hastings brigades, the Cape Coast Civil Defence unit, the Army, the Red Cross and the Salvation Army were involved in co-ordinating the evacuation and transporting people to higher ground, providing medical support and blankets and feeding evacuees and rescuers.

In the debrief afterwards it was agreed that because of the lack of heating at the Haumoana School which doubles as



Haumoana Fire Brigade 1940



The Haumoana Fire Station in the 1970s flood

the Civil Defence evacuation centre, the Haumoana Brigade needed to get into fundraising mode again.

They've since purchased a generator and diesel heater which are now available when needed in civil defence situations.

Ironically the brigade and the community had been engaging in a tsunami awareness and evacuation exercise when the rains came so the response was fairly orderly.

"If 5-10 metre waves come through here no-one's going to stop that, all we can do is forewarn people through loud speakers on our van and go door to door letting people know there's a surge coming," says Tims.

"All we can do is repeat the Civil Defence warning, if there's a shake big enough to knock the furniture off your wall then head to the Haumoana School and stay there until it's safe to return."

Double calls outs rare

Those who are interested in joining the volunteer brigade are encouraged to hang out with the locals at the station for up to six months before being sent off for an intensive seven days course at the regional NZ Fire Service Training Centre in Rotorua.

The course requires a certain level of fitness, getting up to speed on first aid and becoming familiar with firefighting procedures ahead of being allowed to ride on the fire truck in an emergency. Those skills are transferrable to any brigade in the country.

Volunteers are always on 24/7 alert and if you are in the area at the time you

are expected to turn up. It's not often a second call has to go out. The last occasion that happened was the prolonged blaze at Hawk Packaging, makers of egg cartons and apple packing trays, in Tomoana Rd, Hastings on 17 January 2012.

It was one of the largest fires in Hawke's Bay's history requiring engines from across the region including Dannevirke and as far away as Palmerston North.

Neighbouring homes were evacuated and the inferno was so intense it melted oxygen masks and tyres, shattered windscreens and blistered paint on the fire engines.

The last big house fire the Haumoana brigade attended was in 2008 when two people ended up in hospital with serious injuries and an elderly woman died. Tims notes there's been a dramatic drop off of house fires of any size, largely through education. "A lot of it is awareness; many in the community have smoke alarms now."

The NZ Fire Service has an annual awareness drive during daylight saving time, reminding people to change their batteries. People still ask for basic smoke alarms which are made available free. "It's not always the burning bit but what comes before that gets you, the smoke or carbon monoxide fumes overcome people very easily."

False alarms are also on the decline; last year there were only 15. Tims reckons a lot more care is taken in maintaining alarm systems and a deterrent is perhaps the fact that there's a charge if there are multiple false alarm call outs to the same premises.

Incentive to improve

Tims says the community holds the brigade in high regard and while it's a bonus being recognised for being successful, he says the more successful you are the more you want to improve. "We're disciplined but not over the top... we know how to have a laugh."

And while there was a time when the Haumoana brigade had a competition team to test its skills against other brigades they pulled back about a decade ago, aware that much was already being asked of brigade members who valued their down time.

The team does get together five nights a month, one for a general catch up and paperwork as part of the requirements of being an Incorporated Society and the rest are training nights to put the members and equipment through their paces.

"We get into teams, get the stop watch out and ramp it up with a bit of urgency," says Promotions Manager Brian Slader. "It depends on what skills are up for renewal and it's to ensure everyone knows how to use everything that's on a truck."

In 2002 the Haumoana brigade won the NZ Fire Service, "Chief Executive Leadership and Innovation Award" for partnership development work with St John and The Hastings District Council.

That award recognised the long-term relationship as first responder in medical emergencies, the strategic relationships with Hastings City Council which provides the water tanker housed at Haumoana and its fundraising efforts for new cardiac equipment.

"We went around like the old Telethon days raising money for a defibrillator. We raised about \$5000 toward the \$8000 cost – the community gave heaps," says Tims.

Like most brigades there's an overall operational allowance from the Fire Service Commission and the occasional donation from people who appreciate the service that's been provided. The local Lion's Club is a great advocate and there's a steady stream of change from a tin at the local Four Square.

Generally though everything is done on a break even basis. "If we need something we all get in and do it. We've done fire wood cutting over the years but there's not a lot of those opportunities today," says Tims.

"Mostly if we don't have it we don't spend it, although we were really appreciative of the emergency lights and torches for our helmets provided by the Hastings Host Lions Club which we would not have been able to afford."

FLIR optical gas imaging camera helps improve environment and safety at Borealis Stenungsund

Many petrochemical plants handle invisible gaseous hydrocarbons. Most of these gases pose some sort of safety aspects. They may be toxic, or can cause health issues in case of long term exposure. Others are highly flammable, explosive even, and most of them will have a negative impact on the environment if they enter the atmosphere in large quantities. That is why leak detection is of vital importance in these petrochemical plants.

One of such plants is the Borealis high-pressure, low-density polyethylene (LDPE) plant in Stenungsund, Sweden, which produces LDPE products for the cable and wire sector and has an annual production capacity of 350,000 tonnes. The Borealis cracker facility delivers the main ingredient: ethylene, which is converted into polyethylene in a high-pressure polymerization process.

Ethylene is a highly flammable hydrocarbon. To further increase the safety within the plant and reduce the environmental impact, Borealis has purchased an optical gas imaging camera from FLIR Systems. With this gas leak

detection tool Borealis ensures that no gas leak escapes the attention of the process operators.

An optical gas imaging camera is a quick, non-contact measuring instrument that can visualize gas leaks in real time. Where many other measuring instruments only present the inspector with a number, optical gas imaging cameras present visual information, making the leak detection process more intuitive. Optical gas imaging cameras can also be used in hard-to-access locations, since they can detect small leaks from a distance. "When we started testing this relatively new technology I was at first very skeptical," says shift supervisor LDPE Jan Åke Schiller. "But seeing these optical gas imaging cameras in action I quickly realized that they had an immense potential for leak detection here at the polyethylene plant and in petrochemical plants in general."

Advantages of optical gas imaging

Before the purchase of a FLIR GF306 optical gas imaging camera, Schiller and his colleagues used so-called 'sniffers', devices which measure the concentration of a certain gas in one single location and generate a concentration reading in parts per million (ppm). "The main advantage of the optical gas imaging camera is that it provides you with the possibility to detect gases visually," says Schiller. "Where sniffers just give you a number, an optical gas imaging camera allows you to detect gas leakage anywhere within the field of view of the camera. This speeds up the inspections considerably. Now that we have the optical gas imaging camera we do a quick scan at every startup. With a

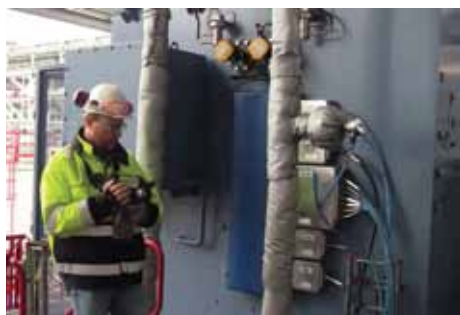
quick scan we cover approximately 80% of the entire plant in about thirty minutes. You would need a team of ten people with sniffers to work for two full days to reach the same result."

This doesn't mean that they stopped using sniffers altogether, stresses Schiller. "We use the sniffers alongside the optical gas imaging camera. We use the optical gas imaging camera to detect the leak and then use the sniffer to quantify the leak." Schiller was surprised to see how sensitive the FLIR GF306 optical gas imaging camera turned out to be. "I detected leaks where the sniffer gave a reading of below 100 ppm, especially when operating in the High Sensitivity Mode, this camera is surprisingly sensitive, it can be used to detect even smaller gas leaks from about seventy meters. This enables the operator to perform these inspections from a safe distance."

High Sensitivity Mode

The High Sensitivity Mode (HSM) is a special feature included in all GF-Series optical gas imaging cameras. It is an image subtraction video processing technique that effectively enhances the thermal sensitivity of the camera. The HSM feature subtracts a percentage of individual pixel signals from frames in the video stream from the subsequent frames, thus enhancing the differences between frames, which make leaks stand out more clearly in the resulting images.

All leaks to be repaired are reported to the maintenance crews. In this part of the process the use of optical gas imaging cameras also has an advantage over sniffers, according to Schiller. "When you are using sniffers you have to describe



Shift supervisor LDPE Jan Åke Schiller was skeptical at first, but is now convinced of the potential of optical gas imaging cameras.



Leaks show up in the optical gas imaging footage as a smoke like vapor.



Polyethylene is used to produce a wide variety of plastics, from wiring insulation to car dashboards.



In the control room all gas flows throughout the plant are closely monitored.

the exact location of the leak using words which can be difficult sometimes. With the optical gas imaging camera we can simply attach a video file to the work order and the maintenance crew will see for themselves where the leak is located. This allows me to spend less time on generating leak reports and more time out in the plant, detecting leaks, or performing other duties.”

Higher inspection frequency

Due to the fact that these inspections are much less time consuming now that he uses the FLIR GF306 optical gas imaging camera, the leak detection



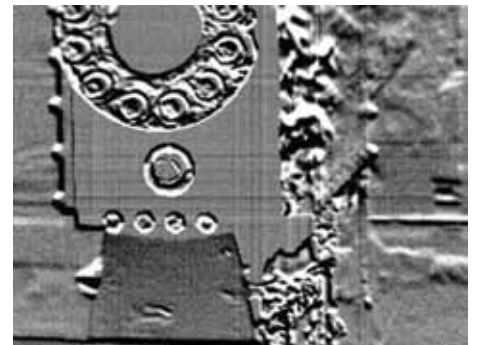
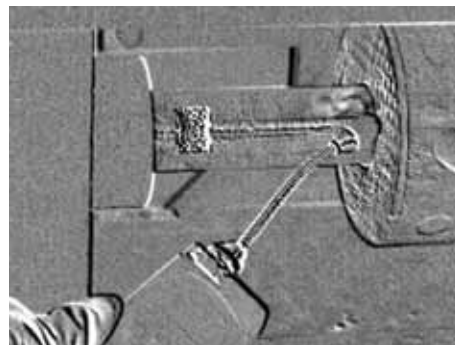
The small gas leak detected with optical gas imaging camera is quantified with a sniffer. As the concentration is below the threshold this leak does not get a high priority.

frequency has increased significantly, according to Schiller. “When we only had sniffers we did other yearly inspections. To cover all of the pipework that this plant contains, which is all in all over 100 kilometers in length it takes a team of people with sniffers a whole week to inspect the whole plant. With the optical gas imaging camera this takes one person one day. Now that we have the optical gas imaging camera we inspect the entire plant twice a year and we also perform a quick inspection at every startup. So the inspection frequency has gone up considerably.”

A tool that is used as often as the FLIR GF306 optical gas imaging camera is being used at Borealis in Stenungsund needs to be lightweight, compact and ergonomically designed to prevent back and arm strain. All FLIR GF-Series optical gas imaging cameras are ergonomically designed. With its rotating handle, direct access buttons and tiltable viewfinder and LCD screen, the FLIR GF306 optical gas imaging camera is designed from the end-user’s perspective, offering advanced ergonomics to improve worker safety. With a weight of 2.4 kg, the FLIR GF306 optical gas imaging camera is also relatively light and compact.

Infrared absorption

The FLIR GF306 optical gas imaging camera contains a cooled Quantum Well Infrared Photodetector (QWIP) that produces thermal images with a resolution of 320 x 240 pixels at a thermal sensitivity 25 mK (0,025 °C).



Light temp deviation along ceiling probably due to deposits inside the piping.

The gas visualization functionality of the FLIR GF-Series optical gas imaging cameras is based on infrared absorption. Gases absorb electromagnetic radiation in certain parts of the spectrum. FLIR GF-Series optical gas imaging cameras contain a spectral filter, a focal plane array and optics that are specifically tuned to such a part of the spectral range. Since the gas absorbs infrared radiation it blocks radiation from objects behind the gas, causing gas leaks to show up as either a black or a white plume in the thermal image, depending on whether the user opted for the ‘white hot’ or the ‘black hot’ settings.

Recording video footage

Apart from real time visualization the FLIR GF306 optical gas imaging camera is also capable of recording both visual light video and thermal video footage.

"This is very important, because the moving smoke like plume shows up much more clearly in a video than in a still picture," explains Schiller. "For leak reports we usually start our video recording in the visual video mode, to show the location to the maintenance crew, then we switch to the gas detection mode to show the leak and then we switch back to visual video mode to verify the leak location. This method has worked really well for us."

"This plant is relatively new, it was opened a few years ago to replace the old polyethylene plant," adds Schiller. "The new polyethylene plant had a few teething problems, but with the help of the optical gas imaging camera we have been able to make it into one of the leak-tightest polyethylene plants in the world. To give an idea this new plant produces twice as much polyethylene as the old plant did, but the amount of VOC's escaping due to leakage is ten times less. In my opinion the FLIR GF306 optical gas imaging camera has helped to make this very low leakage rate possible."

Detecting leaks in unexpected locations

According to Schiller one of the advantages of using optical gas imaging is that you will be more likely to detect the leaks in unexpected locations. "Leaks can really turn up in the strangest of places. There was one case where a support pipe was welded onto a bend in the pipework, but the welder had been overenthusiastic and his welding had caused a leak from the pipework into the support. With the optical gas imaging camera it was very easy to locate the gas escaping from the pipe



Leaks can pop up in unexpected locations, such as in this pipe support.

support, since it stood out very clearly in the thermal image, but with a sniffer it would have taken ages to detect the leak, if we would have ever detected it at all, for who would look for leaks in a pipe support?"

"Another example of an unexpected leak location was when I found gas escaping from insulation material. Due to a leak in a connection at the other end, gas leaked in behind the insulation and at the other end it leaked out again. And this is just one of a list of leaks detected with the optical gas imaging camera that would have been nigh impossible to detect with a sniffer. A sniffer has to be held exactly in the right spot to detect a leak, so the inspector will only hold in locations where leaks may be expected. With an optical gas imaging camera you see all leaks within the camera's field of view. You can use it to spot leaks easily, quickly and it makes your inspections more thorough."

Worth the investment

"Some companies might be reluctant to buy an optical gas imaging camera due to the price tag, which is understandable as a sniffer is much cheaper," continues Schiller. "But the difference in purchase cost is deceptive. For one thing, inspecting with sniffers is much more labor-intensive



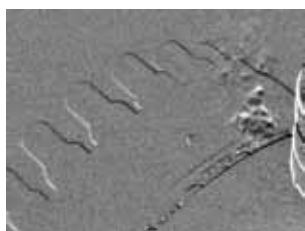
Another unexpected leak location. Due to a leak in a connection the gas escapes from the insulation material.

and man hours do not come cheap, well not here in Europe at least. Secondly leaks in unexpected locations are difficult to find and easy to miss with sniffers, so using optical gas imaging cameras will help ensure the safety of personnel and of the inhabitants of the surrounding area and in my opinion safety is definitely worth investing in. Using optical gas imaging also increases the sense of safety for the plant's workers. They feel safe in the knowledge that no gas leak escapes my attention with the FLIR GF306 optical gas imaging camera."

"Last but not least the use of optical gas imaging will help reduce the amount of gas lost to the atmosphere," continues Schiller. "Given the fact that these gases are our base material it is a waste to lose it due to leakage. I would much rather turn it into plastic. So gas leakage is in fact throwing away money. By reducing the leakage the optical gas imaging camera will earn back its purchase cost. So all in all I would definitely say that an optical gas imaging camera is worth the investment."

Disclaimer:

Images for illustrative purposes only and may not be representative of the actual resolution of the camera shown. Technical specifications subject to change without notice.



The FLIR GF306 optical gas imaging camera can detect even smaller leaks from a distance, such as this leak - spotted using the HSM.



This valve is leaking ethylene, showing up as white smoke in the black hot thermal image.



This HSM footage clearly shows a gas leak.

More about FLIR Systems and its products can be found at www.flir.com

FLIR SYSTEMS Australia Pty Ltd
Toll Free: 1300 729 987
Tel: +61 (0)3 9550 2800
Email: info@flir.com.au
www.flir.com

New Zealand: Tel 0800 785 492



BROOKS Provide Complete Fire Solutions...

Starting from the ground up!



...for Residential, Commercial and Industrial Applications

BROOKS New Zealand
Ph: 0800 220 007
Unit 106 "The Zone"
23 Edwin Street Mt Eden
Auckland 1024
Web: www.brooks.co.nz

BROOKS Australia
Ph: 1300 78 FIRE
4 Pike Street
Rydalmere NSW 2116
Web: www.brooks.com.au



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 55° to suit doors opening past 90° • 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

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**



BOTH
options are
packaged
in the
same box