

NZSecurity



April / May 2016

**Christchurch a
case study in crime
prevention through
environmental design**

**Health and Safety
at Work Act 2015**

**Industry CCTV
generosity to protect
Koru School**

www.DefsecMedia.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



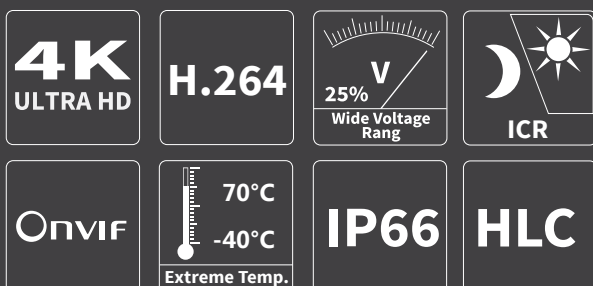
IPC6248SR-X22

4K Ultra-HD Network IR PTZ Dome Camera



Features:

- 1/1.7" progressive scan CMOS
- Up to 4000×3000 resolution
- 22x optical zoom(6.5~143mm)
- Smart IR, up to 150m IR distance
- Alarm I/O, Audio I/O, ONVIF
- All-weather design, IP66, -40°C ~ +70°C
- AC 24V, DC 24V, 14~48W



Contact Details:

Craig Flint

Telephone: +64 (07) 868 2703

Mobile: +64 (0) 274 597 621

Postal and delivery address:

27 West Cresent

Te Puru 3575

Thames RD5

New Zealand

Email & Internet:

craig@defsecmedia.co.nz

www.defsecmedia.co.nz



www.facebook.com/defsecmedia/



twitter.com/DefsecNZ



www.linkedin.com/company/
defsec-media-limited

Upcoming Issues

June / July 16

Wholesalers and Manufacturers Featuring
Perimeter Protection, Alarms.

August / September 16

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.

CONTENTS

- 6 Note from the Editor
- 10 Christchurch a case study in crime prevention through environmental design
- 12 Netgear IP surveillance boot camp hosted by C R Kennedy
- 13 Competent or Confident? You decide
- 14 Dahua Security Solution for SHOP N SAVE in Fiji
- 16 Introducing the Health and Safety at Work Act 2015
- 18 Industry CCTV generosity to protect Koru School
- 20 Australia's New Driver's License & Card Management System
- 22 Gallagher
- 24 KCS TraceME
- 27 Burn Support Group Charitable Trust
- 28 Continuous Development Brings Benefits
- 30 CCTV surveillance in the command & control continuum
- 33 NZSA Chairman sets out 2016 vision
- 34 Gary Morrison the newly appointed NZSA CEO: Q&A
- 36 Removing the 'What ifs': Baggage security on international flights
- 38 Frontline: Guarding in the news
- 40 IP opens doors to a new world of physical access control
- 42 Australia Round-up
- 44 Showcase
- 46 Cybersecurity perspectives from KPMG & PwC get airplay

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

*Standard terms & conditions of sale apply.

Loktronic 0800 367 565
www.loktronic.co.nz

20051

Industry Associations

www.security.org.nz



www.biometricsinstitute.org



www.asis.org.nz



NEW ZEALAND INSTITUTE OF
PROFESSIONAL INVESTIGATORS INC.

www.nzipi.org.nz



www.masterlocksmiths.com.au

Innovating for a **smarter, safer world.**

Axis offers a wide portfolio of
intelligent security solutions:



Video encoders



Network cameras



Physical access
control



Network video
recorders



Video management
software



Audio and
accessories

Visit www.axis.com or send an email to
contact-sap@axis.com for more information.

Note from the Editor: **safe** cities, **unsafe** profession

Welcome to the April 2016 edition of NZ Security.

In this edition we continue our 'safe cities' theme by highlighting the crime prevention through environmental design (CPTED) aspects of the Christchurch rebuild, and by featuring part-two of pioneering CCTV integrator Peter Houlis' lessons learnt in implementing early UK safe city schemes.

We also report on the recent donation of 16 CCTV cameras to Auckland's Koru School, a low decile school in Mangere, by a consortium of leading businesses within the security industry. More than simply a good news story, it's a rare example of altruistic industry-police-community collaboration aimed at countering crime against schools most vulnerable to theft, willful damage and its consequences.

In this edition we also return the spotlight to the work of frontline security professionals. Let's be clear, drunkenness and substance-fuelled aggression among members of the public are posing – as they always have – real problems for security personnel. King hits and so-called 'coward kicks' are putting guards in hospital, while excessive use of force by guards is increasingly feeding the 24-hour news cycle.

Although our reporting will always choose impartiality over side taking, recent news reports reflect disturbing trends in this space that require comment. Drunkenness and aggression – despite their often tragic results – are not going away anytime soon. Frontline security professionals work within a context that can turn ugly in an instant, and recent events indicate that many guards are ill-prepared for this.

So, is training for security guards adequate, is it specific enough... and, if not, should it be required by law to be so?

Recent diverging views within the industry in New Zealand over the role and comprehensiveness of mandatory training are relevant here, as too the early March media coverage of 'license shopping' in Australia, where interstate security qualification disparities are creating loopholes leading to ill-trained and ill-qualified guards flooding the workforce there.

We welcome your feedback in relation to the magazine, in fact we'd prefer to hear from you. Read the magazine, check out the website, follow us on social media, and please tell me what you think at nick@defsecmedia.co.nz

Nick's professional background is in government and the military. He was posted to Shanghai, Beijing and Suva as a diplomat during a 14-year career with Australia's Department of Immigration and Border Protection, and has also served in the Australian Army's Signals (RASIGS) and Transport (RACT) corps. He holds Masters degrees in Asian Studies and International Relations from the Australian National University and the University of Sydney respectively, and he is a graduate of the Royal Military College of Australia.

Nick's research has been published in several peer-reviewed journals and for the Washington-based Jamestown Foundation on international security, cyber conflict and terrorism. His writing has also appeared in international affairs publications including The Diplomat, National Business Review, Global Times and World Policy Institute Blog. His insights are regularly sought via interview by outlets such as CNN and Agence France-Presse (AFP).



www.defsecmedia.co.nz

4K

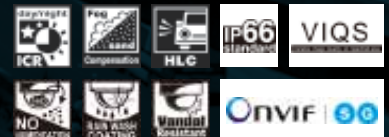
IT'S IN OUR DNA

The new Panasonic WV-SFV781L Camera embodies Panasonic's Security DNA philosophy. We provide True 4K from the Panasonic made optics to the chipset and black box technologies, such as the rain wash coating. The WV-SFV781L is designed from the ground up to provide the best 4K experience.



WV-SFV781L VARI-FOCAL CAMERA

- 4k images up to 30fps
- Ultra wide 6x motorised optical zoom
- 12.4 Mega pixel sensor
- Rain wash coating
- Fog compensation



OUTSTANDING CLARITY

THE PANASONIC VARI-FOCAL OPTICS AND 12MP SENSOR

4K OFFERS IMPROVED CLARITY

With 4x the resolution of FHD more details can be seen.

FALL OFF REDUCED

The Panasonic 4-25mm optics insure the image stays sharp right to the edges.

12M PIXEL MODE

The WV-SFV781L Can provide a 12M Pixel output at 15Ffps.



WWW.PANASONIC.NET/SECURITY

Panasonic

PROFESSIONALISING THE SECURITY INDUSTRY

The New Zealand Security Association (NZSA) is the largest industry representative body for the security industry in New Zealand.

TOP REASONS 10 TO JOIN THE NZSA



ENHANCE YOUR REPUTATION through membership with a recognised, professional association which maintains an established Code of Professional and Ethical Conduct and business Codes of Practice.

GET RECOGNISED. Become recognised as a security industry professional through the NZSA accreditation program and use the NZSA logo to promote your business. Your business will be listed as an accredited provider on the NZSA website with a link to your own website. Accredited membership is accepted by the PSPLA as proof of competence for the licence categories of Security Technician and Private Investigator.

NETWORKING OPPORTUNITIES. Improve your contacts, knowledge and access to others by attending NZSA events held across the country and the annual Awards Dinner and Exhibition.

SAVE MONEY. We offer a number of member benefit programs including the NZSA Mobil fuel card which offers a 16c/litre discount at 329 Mobil card sites nationally and preferential insurance rates and advice from an NZSA appointed insurance provider.

BE HEARD. Benefit from the NZSA's position as the voice of the security industry, engaged at all levels, across all areas of security legislation, acting on behalf of and in the best interests of the industry.

BE INFORMED of changes in legislation and training requirements, access live news feeds and information on global security industry trends through the NZSA website and regular NZSA newsletters.

COMPLAINT MANAGEMENT. Utilise the NZSA disputes resolution service to act as a mediator in resolving disputes between NZSA members and third parties.

EXPERT ADVICE and support to members on compliance, technical, business and industrial relations issues. Our senior management team have many years experience across a wide range of security backgrounds and can provide valuable advice and guidance.

SOCIAL MEDIA. We encourage members to follow us on Facebook and LinkedIn to receive latest news updates and engage with our consumer awareness campaign.

NZ SECURITY MAGAZINE a bi-monthly magazine which provides timely information to security professionals. Free subscription and reduced advertising rates to all our members.

FOR FURTHER INFORMATION:

Email: nzsa@security.org.nz

Ph: +64 9 486 0441 / Fax: +64 9 486 0442

www.security.org.nz

Connect with us



THE NZSA HAS YOU COVERED



MEMBERSHIP SECTORS

The New Zealand Security Association is committed to the highest standards of professional and ethical conduct at all times.

Members include security companies ranging from large multi-nationals to sole traders.

**OUR VISION - SETTING
STANDARDS AS THE AUTHORITY,
CREATING VALUE FOR THE
MEMBERS AND CUSTOMERS.**

**Alarm Installation
Alarm Monitoring
Guarding
Event Security
Security Patrols
Alarm response
Cash in Transit
IT Security
Private Investigators
Security Hardware
Security Consultants
Locksmiths
Document Management
Document Destruction
Security Training
Banking Industry
Insurance Industry
Government Agencies**

FOR FURTHER INFORMATION:

Email: nzsa@security.org.nz

Ph: +64 9 486 0441 / Fax: +64 9 486 0442

www.security.org.nz



Christchurch a case study in crime prevention through environmental design (CPTED)

New Zealand recently paused to mark the fifth anniversary of the 2011 Christchurch earthquakes, the devastation from which the city is still recovering. While the ongoing rebuild has sought to replace what the earthquakes had taken away, it has also sought to create a legacy that improves on what was there before.

Ironically, the destruction wrought by the earthquakes has provided the city with an opportunity to rise again more resilient than before, and to incorporate into its rebuild world leading design. In this article we review the application of Crime Prevention Through Environmental Design (CPTED) principles into the rebuild from the perspectives of two relevant authorities: the Christchurch Central Development Unit (CCDU) and the Christchurch City Council (CCC)..

The face of the future Christchurch is mapped out in The Christchurch Central Recovery Plan and Blueprint, released in 2012, which set out the vision

for a modern, accessible and safe central Christchurch. The Recovery Plan placed importance on buildings and public areas incorporating CPTED principles.

The plan's anchor projects include: The Frame, Earthquake Memorial, Te Puna Ahurea Cultural Centre, Te Papa Ōtākaro/Avon River Precinct, The Square, Retail Precinct, Convention Centre Precinct, Health Precinct, Justice and Emergency Services Precinct, Performing Arts Precinct, Central Library, Residential Demonstration Project, Metro Sports Facility, Stadium, Cricket Oval, Bus Interchange, and Innovation Precinct.

Christchurch Central Development Unit

The Christchurch Central Development Unit is part of the Canterbury Earthquake Recovery Authority responsible to the crown agency responsible for rebuilding the central city, and for operational activity including post-earthquake building demolition, security and related



Don Miskell, Deputy Director, CCDU Development, Design, Planning and Commercial Strategy

land clearance operations in the greater Christchurch area. It is also responsible for governance oversight of the infrastructure repair.

According to Don Miskell, Deputy Director, Development, Design and Planning at the CCDU, the Recovery Plan set out the vision for a modern, accessible and safe central city. "Crime Prevention Through Environmental Design (CPTED) principles," states the Plan, "needs to be considered during the design and development of buildings and public areas to make central Christchurch more inviting and a safer place to be – day and night."

"These principles have now been used during the design process for projects in the Avon River Precinct, the Bus Interchange and the East Frame Residential Project," said Mr Miskell, "and will continue to be used as other projects progress."



Image courtesy Canterbury Earthquake Recovery Authority

“The thinking behind CPTED has been around for decades, and has been cemented in New Zealand through the Ministry of Justice’s National Guidelines for Crime Prevention through Environmental Design published in 2005. This outlines a focus on natural surveillance, street designs that increase pedestrian and bicycle traffic, and windows overlooking sidewalks and parking lots.”

According to Sue Ramsay, Metropolitan Community Advisor at Christchurch City Council, the Council has committed to have CPTED considered in all new/redesigned public facilities and public spaces throughout the city. “The Council also provides the Design Out Crime Advisory Service free to community organisations, developers and design professionals, to ensure that CPTED is integrated to the fullest extent in the rebuild,” she said.

Where CPTED is springing up

CPTED principles, Mr Miskell said, have been used throughout the design of public realm features in central Christchurch seeking to reduce fear of crime and fostering positive interactions among legitimate users of space. In the Avon River Precinct, for example, this has been achieved through lighting along the river, across bridges and in spaces that connect night-time activities.

According to Ms Ramsay, on larger projects, such as the Avon River Precinct and the Coastal Walkway, as well as many others, CPTED advisors have worked

alongside design teams throughout the design process to ensure that every aspect of the completed design has CPTED embedded within.

“A lot of it does seem like simple common sense,” concedes Miskell, “but it is important to avoid large dead-end spaces and nooks and crannies that are enclosed and/or not well lit,” he stated. “We want to make places that people are attracted to, not places to just pass through.”

Crime prevention and safety has been built into the East Frame design by ensuring there are no dark corners and making sure features like plantings are kept at certain heights to facilitate visibility and avoid undesirable screening. Manchester Street will be widened to form a boulevard that will run parallel to townhouses and apartment blocks and the greenway linking Armagh Street to Lichfield Street. “This will be a well-lit area overlooked by hundreds of residents in 900 residential units. Instead of relying on CCTV, these well-lit populated areas will have natural surveillance,” said Miskell.

The Bus Interchange, the central transport facility for the city, partially opened in May 2015, was funded by a construction budget of \$53 million and led by the CCDU. Architectus and Aurecon were appointed as the architects and engineers via an open tender process. Throughout its design, a total of 44 separate CPTED recommendations were provided to the interchange’s design team, approximately 80% of which were ultimately included in the design.

This is evident in the strong relationship between the interior of the interchange building and the street, which provides for natural surveillance both internally and externally. Once deeply recessed entrances are now shallow, thus eliminating entrapment zones.

Its veranda is constructed of glass sheets, allowing light fall on the entire footpath, according to a case study of the Interchange authored by Ms Ramsay. “It is especially important to have optimal pedestrian lighting in this location, because both the Interchange and the adjacent late night entertainment precinct each have elevated risk profiles and high pedestrian counts.”

Public toilets within the Interchange have also been redesigned based on CPTED/IPTED (injury prevention through environmental design) recommendations. “Cubicles have their own hand washing facilities and the foyer is visible from the concourse through the automatic glass doors, providing excellent natural surveillance.” Glass entrance doors allow users to ‘see ahead of travel’, “so that they can exercise a choice not to enter if the foyer doesn’t appear safe.”

As a result of this intentionally planned approach to the redesign of the city’s public places and spaces, Christchurch is increasingly seen as a centre of best practice in CPTED and has been attracting interest from around the world, claims Ms Ramsay. “Few cities have the opportunity to fully integrate CPTED into such a major rebuild, and the quality of CPTED practice in the city is seen as being of a very high standard.”



Image courtesy Canterbury Earthquake Recovery Authority

CR Kennedy hosts Netgear IP surveillance boot camp

CRK's Mount Wellington showroom was the venue in March for a well attended Netgear technical training session. Xavier Lleixa from Netgear Australia was on hand to deliver a comprehensive session covering an introduction to IP networks, VLAN, QoS and PoE, designing an IP network for surveillance, and an overview of the Netgear portfolio.

Xavier, an experienced sales engineer with over ten years' experience in deploying and planning wired, wireless and storage networks in Europe and Latin America, put participants through their paces in the four-hour-long technical tour de force.

IP surveillance has become a viable option for organisations of any size due to the increasing affordability of IP video and recording devices, and the fact that most enterprises already have installed IP networks to which surveillance video transmissions can be added. It's no longer merely an option just for the big players.

According to Duncan Cook of CRK, however, there remains a real skills gap while businesses transition over to IP. The 10 March session was the first in a series of upcoming training sessions designed to impart knowledge on areas such as VLANs and to provide the skills to allow participants to harness the new technology.

"It's technology that's been around for a while, but it's new to the security industry," states Duncan. "VLAN is used within the IT industry as a way of segregating networks, and the benefit of a VLAN in the security industry is that it provides security boundaries that protects the cameras and the recorders that are on it. You also get an increase in performance because you're just having the surveillance products on the network within that VLAN.

"Because surveillance is becoming more technical with IP products, we need to have a good foundation in networking,



so this was the first course," says Duncan. In this session, products and concepts around VLANs and IP and networks and Layer 2 and Layer 3 devices were discussed. It also went into some detail in relation to how a VLAN can be used to essentially create separate switches within a multi port switch so that the ports used for a security VLAN can remain invisible to the other ports.

"We also covered multicast as well," he recalls. Instead of having multiple connections to a single camera, which can cause a lot of congestion on the network, multicast uses a broadcast-type approach. This means, for example, that multiple operators using a VMS can view the same camera via its multicast address as opposed to numerous unicast connections that stress the resources of the camera and increase network congestion.

Network congestion, says Duncan, results in dropped frames and jumpy recordings, and this is why getting the network foundation is crucial to a successful and reliable surveillance system

"The next course will be more advanced and hands-on," he says. Due to be run around the middle of May, the next session will see participants configuring devices and setting up their own networks and VLANs.

According to Duncan, plans for the training series are open ended. "We're getting feedback from our customers and they will tell us what they require and how often they require it."

"We want to run more sessions with Netgear," suggests Duncan. "We've been working with a number of networking products since working in IP installations and it's fair to say that not all IP products are equal. With Netgear we get a lifetime warranty and a good quality product, and that's why we're proud to be distributing the Netgear product range."

Integrators, installers, people project managing CCTV installations, and anyone involved at a technical level in security networks who would like more information can visit the Netgear website for product information or get in touch with CRK about upcoming training sessions via cctv@crknz.co.nz.

Competent or Confident?

You decide

Investing in staff is investing in your business. But why should you invest beyond the minimum requirements?

With new OSH legislation starting in April 2016, it's a good time to assess your training goals for your workforce, and whether you will train above and beyond the new requirements.

We understand common objections to training beyond the minimum requirements, including 'what if we train them then they leave?' Business owners are afraid of their training investment simply walking out the door. But what if we asked 'what will happen if we don't train them and they stay?' What impact will workers who only meet minimum requirements have on your business?

Sadly, most of the security industry chooses to adhere to minimum requirements. These businesses will find themselves playing catch-up rather than being on the front foot with training.

So why train above minimum requirements? There are simple ways to see a return on your investment.

Reduced risk to your business. Better qualified staff make better choices in the heat of the moment. Make sure you don't become front page news.

Win new customers. Show your clients that you're committed to protecting their assets and their businesses. Training levels can set you apart from other providers pitching for the same work.

Become a leader in the industry. Attract and retain the best staff in your business. Staff generally work harder for you if you work harder for them.

We believe a comprehensive training plan will set your business up for success. Take time as part of your planning process to think about your staff investment.

If you want to find out more about training on offer, contact The Skills Organisation on 0508 SKILLS (0508 754 557), or email support@skills.org.nz today.

Wayne Abel
Industry Manager – Security
The Skills Organisation



Achieve long term business success

Invest in workplace training

skills.

The Skills Organisation
0508 SKILLS (0508 754 557)
skills.org.nz

Dahua Security **Solution** for SHOP N SAVE in Fiji

Dahua Technology, a world-leading manufacturer of video surveillance products headquartered in Hangzhou, China, provides security solution for SHOP N SAVE in Fiji.

Shop 'n Save was founded in 1979 as a grocery store in Belleville. The chain now includes thirty-eight stores in the St. Louis metropolitan area, and three additional stores in Springfield, Illinois.

In 1983, the retail chain was acquired by Wetterau, Inc. Nine years later, in 1992, Wetterau was acquired by SuperValu, and Shop 'n Save has been a subsidiary of SuperValu since. Recently, Shop N Save Supermarkets becomes the fastest growing supermarket chain in Fiji which runs 16 supermarkets, serving the major towns and cities in Viti Levu and Vanua Levu - the two major islands of Fiji. The Company's trading name "SHOP N SAVE" is an identifiable brand name in the supermarket industry in Fiji known both for the quality of its service and products.

Supermarkets are among the places where supervision and security is vital but yet extremely difficult to be maintained. A supermarket is usually enormous in size with racks and partitions being literally everywhere. Shop 'n Save in Fiji needed a more advanced security solution for its protection. Because of the diversity of areas that need protecting in Shop 'n Save, Dahua offers dome camera and bullet camera for the front-end and Beneficio series NVRs for storage-end.



Dahua IR bullet cameras were installed in the entrances, exits and sales floor to prevent potential crime. Besides IR bullet cameras, the IR dome cameras were installed in the cash desk area to provide a high zoom area to capture every detail with a maximum of 20fps@3M to support the security staff in their work.

Dahua 3-Megapixel full HD network water-proof IR bullet camera with a delicately designed 2.7-12mm fixed lens features excellent picture quality. IP66-rated weatherproofing and dust-proofing ensures the cameras can withstand even the harshest weather environments. Furthermore, IK10-rated vandal-proofing can effectively prevent violent destruction.

The cash desks are monitored with Dahua IR dome cameras with wide zoom areas which are able Dahua 3-Megapixel



full HD water-proof & vandal-proof network IR dome camera supports H.264 & MJPEG dual-stream encoding with 13-Megapixel effective resolution. The maximum IR LEDs Length up to 30-meters.

The cameras are mounted in all critical spots which allows you to manually follow events in the store, if a detective is involved for example. For recording, Dahua provides its Beneficio NVRs series including 16CH 2U 16PoE network video recorder and 16CH 1.5U 16PoE network video recorder. The Beneficio series recorder is user-friendly, reliable and has a high recording performance in real-time. Data is compressed to H.264 which ensures a longer recording period.

About Dahua Technology

Dahua Technology Company Limited is a world-leading manufacturer of professional security and surveillance equipment. Over the past 15 years, Dahua Technology has invested heavily into the Research and Development of innovative solutions that improve public safety. Dahua's solutions are designed to be scalable and modular to provide flexible configuration options. The company is ranked 5th in the Security 50 rankings from A&S International for 2015. Dahua enjoys the world's second largest market share according to the IHS 2015 report. Visit www.dahuasecurity.com to learn more.

Normal

Starlight

Light Up in the Darkness

With using Dahua in-house ISP & hardware solution, starlight series camera provides incredible image in the night.

- Low illumination 0.002lux/F1.2 (color)
- High frame 1080P@60fps
- True WDR up to 120dB
- Smart features
- Remote focus lens



CE FC CCC UL RoHS ISO 9001:2000



DAHUA TECHNOLOGY CO., LTD.

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com



Add: Unit G 701 Great South Road Penrose
Auckland 1642 New Zealand
E-mail: andrew@swl.co.nz
Web: www.swl.co.nz

DAHUA TECHNOLOGY AUSTRALIA PTY LTD

Add: Unit 8, 39 Herbert Street St Leonards, NSW, 2065
E-mail: sales.oc@global.dahuatech.com

Introducing the **Health and Safety** at Work Act 2015

The *Health and Safety at Work Act 2015* comes into force on 06 April 2016 replacing the current *Health & Safety in Employment Act 1992*. The following summary of key aspects of the Act is an abridged version of material prepared by NZSA director of training, Stewart O'Reilly, who presented a more comprehensive overview of the new legislation at the 01 April NZSA networking event.

Purpose of the Act

The main purpose of the Act is to provide for a balanced framework to secure the health and safety of workers and workplaces by:

- (a) protecting workers and other persons against harm to their health, safety, and welfare by eliminating or minimising risks arising from work or from prescribed high-risk plant;

Note: Many will be familiar with the Hierarchy of Control from the previous Act. This Act still requires the PCBU to eliminate the hazards and risks to health and safety, so far as is reasonably practicable. If this cannot be done then they have a duty to minimise risks, so far as is reasonably practicable. However the term "isolate" has been removed from the current hierarchy of control.

- (b) providing for fair and effective workplace representation, consultation, co-operation, and resolution of issues in relation to work health and safety; and
- (c) encouraging unions and employer organisations to take a constructive role in promoting improvements in work health and safety practices, and assisting PCBUs and workers to achieve a healthier and safer working environment; and
- (d) promoting the provision of advice, information, education, and training in relation to work health and safety; and
- (e) securing compliance with this Act through effective and appropriate compliance and enforcement measures; and
- (f) ensuring appropriate scrutiny and review of actions taken by persons performing functions or exercising powers under this Act; and
- (g) providing a framework for continuous improvement and progressively higher standards of work health and safety.

Duty Holders

A duty holder is a person who has a duty under the Act. The Act identifies four types of duty holders: (a) PCBUs, (b) officers, (c) workers, and (d) other persons at workplaces.

Duty Holder A: PCBU

A PCBU is any Person conducting a business or undertaking for profit or gain, in which business is defined as an activity carried out with the intention of making a profit or gain, and undertaking is defined as an activity that is non-commercial in nature. For example certain activities of a local authority.

In most cases the PCBU will be an organisation (for example, a business entity such as a company) but an individual, such as a sole trader, can also be a PCBU. PCBU does not include volunteer associations (with no employees), home owners, and workers in a business

Duties of a PCBU

A PCBU is to do everything reasonably practicable to ensure the Health and Safety of workers and others in the workplace. If there are multiple PCBUs on a site then they are to consult, cooperate and co-ordinate. They are to provide and maintain the work environment, safe plant and structures, safe systems including emergencies, handling and storage, facilities including accommodation for workers, information and training, and the health of workers by monitoring.

PCBUs also include "Upstream" PCBUs, which are defined as a business or undertaking who designs, manufactures, imports or supplies plant, substances or structures, or who installs, constructs or commissions plant or structures (Note: 'design', also includes the design of part of the plant, substance, or structure; and the redesign or modification of a design).

Examples from the security industry would be manufacturers, consultants, installers, and integrators. All must take reasonably practicable steps to ensure the (design, manufacture, supply, installation) is without risk to anyone who may handle, use, store, construct, maintain, and/or clean the device(s). They must provide information concerning its purpose, the results of any calculations, analysis, testing, or examination; and any conditions necessary to ensure that it is without risks to health and safety when used for a purpose for which it was designed

Duty Holder B: Officers of a PCBU

"Officers" are those who have a very senior governance role in the PCBU that allows them to exercise significant influence over its management; for example directors, chief executives, partners and CEOs. Officers do not include a person who merely advises or makes recommendations to an officer of the organisation.

Duties of Officers

Officers have an obligation to exercise due diligence to ensure the organisation is complying with its health and safety obligations. This places a positive duty on people at the governance level of an organisation to actively engage in health and safety matters, reinforcing that health and safety is everyone's responsibility.

Officers will need to be able to demonstrate they took reasonable steps to:



- 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

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



ALLEGION

www.allegion.co.nz

- Acquire knowledge of health and safety matters relevant to their operations
- Ensure the organisation has and uses the right resources and processes
- Verify that resources and processes have been put in place and are being used.
- Keep a track of, and review, resources and processes to ensure they are, and remain, fit for purpose

Duty Holder C: Workers

A worker is an individual who carries out work in any capacity for a PCBU; that includes employees, contractors, volunteer workers, labour hire, apprentices, work experience

The Duties of Workers

Workers must take reasonable care of their own Health & Safety. No act or omission by the worker should affect the Health & Safety of others. They must comply with reasonable instructions, and they must co-operate with policy or procedure. Workers have the right to stop/refuse dangerous work

Duty Holder D: Other persons at the workplace

A workplace is defined as a place where work is carried out, or is customarily carried out, for a business or undertaking. This includes any place where a worker goes, or is likely to be, while at work. Responsibility of others (visitors, customers) in the work place includes taking reasonable care of their own Health & Safety and complying with reasonable instructions. No act or omission on the part of the 'other person' should affect the Health & Safety of others.

Participation

A critical focus of the Act is around worker engagement to facilitate the development and implementation of health and safety practices and strengthens existing requirements for worker engagement and participation in work health and safety matters.

A PCBU must "engage" with workers to ensure that relevant information shared in a timely manner, workers are given a reasonable opportunity to express their views, raise issues and contribute to decision making, that their views are taken into account, and that they are advised of the outcome in a timely manner.

Engagement with workers is required in relation in the following circumstances:

- (a) when identifying hazards and assessing risks to work health and safety arising from the work carried out or to be carried out as part of the conduct of the business or undertaking;
- (b) when making decisions about ways to eliminate or minimise those risks;
- (c) when making decisions about the adequacy of facilities for the welfare of workers;
- (d) when proposing changes that may affect the health or safety of workers;
- (e) when making decisions about the procedures for the following:
 - (i) engaging with workers;
 - (ii) monitoring the health of workers;
 - (iii) monitoring the conditions at any workplace under the management or control of the PCBU;
- (iv) providing information and training for workers;
- (f) when making decisions about the procedures (if any) for resolving work health or safety issues at the workplace;
- (g) when developing worker participation practices, including when determining work groups;
- (h) when carrying out any other activity prescribed by regulations for the purposes of this section.

If the workers are represented by a health and safety representative, the engagement must involve that representative.

In the next issue of NZ Security we continue our focus on the Health and Safety at Work Act, looking at worker representation and the role of Health and Safety Representatives and Health and Safety Committees. We will also look at the infringement offences and fees under the new regulations.

The CCTV Industry's generosity helps protect **Koru School**

A group of leading security industry companies have banded together to donate their time, expertise and sixteen CCTV surveillance cameras to Koru School, a decile 1 primary school in Auckland's Mangere. A New Zealand first, the program has big plans to help out one-to-two deserving New Zealand schools with their surveillance camera needs each year.

To make it all happen, Axis Communications a market leader in network video joined forces with its New Zealand distributor Channel Ten, integrator Focus Digital Security Solutions, video management software (VMS) specialist Milestone, and DivioTec, who threw in the switches. They reached out to the New Zealand Police, who were only too happy to put forward a list of the most deserving schools.

Ten of the cameras came from Swinburne University in Melbourne, and six were Axis ex-demonstration stock with updated firmware. Swinburne University upgrades its CCTV cameras every five years, and requires its used cameras to find a new lease of life in schools.

According to Axis Communications' Sargon Yousif, the cameras used are discontinued models, but even after their university service they still have



Koru School Principal Stanley Whata demonstrating the Milestone software and Axis Camera footage to Inspector Jason Hewett.

another 10 years of life left. “When Axis take them back [from the university] we recondition them,” said Yousif, thus ensuring that they are at the top of their game when they enter the schools.

With the majority of cameras having come from Australia, the process involved some impressive logistics. The Swinburne cameras crossed the Tasman to Auckland following reconditioning, while the balance received their new componentry via Axis’ Wellington headquarters.

According to Inspector Jason Hewett, Area Commander Counties Manukau West, “schools are very vulnerable to burglary, theft and wilful damage,” and Koru school in particular was a very frequent victim of crime prior to being fully fenced a couple of years ago. The placement of the cameras and associated signage will serve to further deter crime occurring after hours.

“Ex-students are often involved in school burglaries. Their knowledge is often used to target the “high value items that schools can ill afford to lose,” said Inspector Hewett.

CCTV can play an important role not only in deterring would-be thieves but importantly in identifying perpetrators after the event, particularly given the local gang and ex-student element.

Unfortunately, only a small percentage of schools have surveillance cameras. Funding is a big barrier, particularly for schools in low decile areas.

According to Koru School principal Stanley Whata, the newly installed cameras have already made their mark. He noted that several staff work after hours, and the new cameras have provided to them a greater sense of security and safety.



This is one of the 16 Axis vandal resistant dome cameras installed throughout the school

Installation of the 16 cameras took crews of three to four workers a number of weeks during the school holidays to complete. According to Graham Zuill, Director of Focus Digital Security Solutions, members of his team were even prepared to undertake the work in their own time to ensure the work was completed. “Among staff the thought was there,” he said.

“From a school perspective it is very humbling that there are people out there thinking of us,” echoed Principal Whata in response, noting that the company had reached out to Mangere from its base in North Shore’s Albany.

“From a policing perspective it aligns well with our philosophy of prevention first. Our ultimate mission is to make New Zealand the safest country in the world. We can only do this by working together,” commented Inspector Hewett.

Sergeant Kelly Brown, Counties Manukau West school community services supervisor agreed, reiterating the continued close involvement of police



The Milestone VMS (Video Management Software) used to capture footage

with schools throughout the area through initiatives such as the Cops in Schools program.

According to Clint Morris of Channel Ten Security Imports, the CCTV donation to Koru School is to become an ongoing program, with his band of industry colleagues looking to fix one-to-two schools with surveillance cameras per year going forward. It looks like many more schools in most need are set to benefit from the group’s generosity.

This is one of those stories that NZ Security takes particular delight in reporting. The equipping of the Koru school with CCTV surveillance means that there is now one less low decile school providing an easy target for thieves.

This is, no doubt, a win for the school, its students and teachers, and also the community it services. It is, furthermore, a win for the reputation of this country’s security industry and the mission that it surely shares with the NZ Police – that of making New Zealand the safest country in the world.



Inspector Jason Hewett seized the opportunity for a photo with a Koru School student who was proudly wearing his own little police uniform.



Contributors to the Koru School CCTV project from left to right, Clint Morris (Channel Ten Security imports), Graham Zuill (Focus Digital Security) Stanley Whata (Koru School Principal) Inspector Jason Hewett, Sergeant Kelly Brown & Constable Priscilla Tauleva (NZ Police) and Sargon Yousif (Axis Communications).

Australia's New Driver's License & Card Management System

The State Agency of Australia



One Of The First ISO 24727 Driver's Licenses In The World

- Simple customer-managed process to introduce additional services/applications on the card and to the citizen
- PKI enabled for next generation capabilities

Flexible Multi-Application System

- Five applications currently integrated into single program and growing
- Robust platform for adding new services and applications as needs evolve

Citizen-Centric

- Provides a single convenient platform to provide multiple and evolving services to the citizen
- Manages content updates from multiple sources without requiring reissuance of cards
- Lost cards can be canceled and their digital identities revoked centrally

Creating A Next-Generation Driver's License

In 2008, a State Agency of Australia entered into a contract to replace its early-generation laminated driver's license cards with an advanced, multi-purpose smart card and card management system that would take the program to the forefront of ID management. Their vision was a fraud-resistant card that could flexibly evolve to meet a multitude of future requirements. HID Global's ActivID® business was selected for the project as a preeminent provider of comprehensive and advanced ActivID card management solutions.

The Business Issue

The state's previous driver's licenses were easily counterfeited and could not be updated once issued. In addition to the cost and administrative benefits of introducing a fraud-resistant, updateable card, the State Agency of Australia wanted to couple the new credential with post-issuance card management capabilities to provide a flexible platform for a continually evolving card application portfolio. The new solution was designed to incorporate support for cards in the field, handle updates to both customer data and on-card applications, and accommodate potential new functions. This required an innovative and comprehensive ID solution integrating customer-directed card design and content delivery, plus complete cardholder management.

Requirements:

- **Highly secure digital identities:** Provides counterfeit-resistant, durable and updateable electronic ID cards and a comprehensive approach to security in the card management system.
- **Customizable for evolving card services:** Delivers multiple functions and services to citizens through a single card management system via a single updateable card, and supports customer-driven evolution of the card contents.
- **Scalable:** A card management system that can handle both the card population and throughput required; can functionally grow with the state's evolving needs; and can be augmented with application upgrades or future applications for other citizen services.
- **Post-issuance support:** Manages cards throughout their entire lifespan for increased return on investment; easily makes personalization data updates and card application upgrades, or adds card applications.
- **Custom integration:** Backed by a card management system vendor team that is extremely familiar with the ecosystem and best practices (enrollment systems, credentialing systems, cards, card applets, service bureaus) and brings a holistic solution approach to the program.
- **Open standards:** Strict adherence to open standards to ensure a "vendorless" integration approach.

An Innovative and Scalable ID System

The pioneering efforts of the State Agency of Australia have placed the new system at the forefront of the driver's license market. The agency played an integral role in defining and evolving a new standard, resulting in one of the first ISO 24727 smart driver licenses in the world. Via a single applet suite, the system also supports marine licenses, combination driver and marine licenses, proof of age IDs, and person of authority IDs (independent authorities such as taxi, truck drivers, bus drivers and other services).

To optimize the program's functionality and return on investment, the State Agency of Australia contracted with HID Global for the delivery of its industry-leading ActivID® Card Management System (CMS) for National ID. The CMS provides issuance support

and enables post-issuance updates of card personalization data as well as expansion into new on-card applications and services. The system updates citizen data such as addresses or license details, or manages identity updates such as renewal of PKI certificates that provide digital proof of the cardholder. By investing in this Card Management System, the government now has the capability to continually evolve the solution – even after the card is in the citizen's hands.

The CMS is deployed in the state's facilities, providing the State Agency of Australia with the authoritative store of cardholder, card, application, and credential information. The ActivID Card Management System's unique and secure remote update capability enables the State Agency of Australia to securely update cards from readers in remote field locations while cards are still in the possession of cardholders. The system is designed to operate remotely, centrally and/or through interaction with one or more service bureaus.

The CMS implements and supports a broad suite of specifications from GlobalPlatform, the leading provider of open card management standards, supporting the GlobalPlatform Messaging, System Profiles, Scripting, and Card specifications to facilitate a customer ecosystem integration that does not lock the customer into a specific CMS product or implementations.

Flexible Identity Assurance

The Australian Driver's Licence program is designed to evolve over time, which requires not only platform scalability but also the capability to adapt to possible technology, security, services, and applications changes. HID Global's ActivID platform and team of experts provided authorities in the State Agency of Australia with the confidence that their evolving needs would be met through a flexible approach and HID Global's commitment to customizable, innovative solutions. By helping governments find cost savings through inter-agency synergies in service delivery, the ActivID CMS for National ID is leading the way in delivering robust and scalable identity assurance solutions for today's complex realities.

HID Global Government ID Solutions

Dedicated to delivering highly secure, custom government-to-citizen ID programs worldwide, HID Global's Government ID Solutions offer government customers an end-to-end source for their most demanding state and national ID projects. The complete portfolio of solutions includes expert professional consulting services, as well as Genuine HID® data capture, card management and issuance solutions, world-leading credentials and e-documents, readers, inlays, prelamines, LaserCard® optical security media technology, FARGO® card printers and ActivID. ActivID is a global leader in identity assurance including strong authentication and smart card solutions that are relied upon by more agencies, including the U.S. Department of Defense, than any other provider. ActivID has issued more than 100 million credentials to enterprise, government and commerce customers. With Genuine HID, customers benefit from the industry's broadest portfolio of trusted, interoperable secure identity solutions across all aspects of the government identification market. Genuine HID solutions are designed and built in ISO 9001 certified facilities; include worldwide agency certifications; and are backed by global product warranties.

HID Solutions Proven Worldwide

- U.S. Green Card Program
- Saudi Arabia National ID Card Program
- Italy National Police (Carabinieri) ID Card Program
- India State Vehicle Registration Cards
- Angola National ID Card Program
- Spain e-Passport Program
- Germany Prelaminates for National e-ID Card and Health ID Programs
- Ivory Coast Driver's License and Prelaminates for National e-ID Card Program
- UAE Dubai Health ID Card Program
- US Department of Defense Common Access Card Program
- US Federal Agencies PIV Program
 - General Services Administration Managed Service
 - Department of Health and Human Services
 - Department of Veterans Affairs
 - Department of Agriculture
- UK Metropolitan Police ID Card Program

Customer-Centric

- Centrally managed from customer facilities
- Customer possesses an authoritative store of card information
 - Applications on chip
 - Physical condition/ context (in cardholder possession/lost./ stolen/ damaged etc)
 - Centralized tracking of capabilities and data stored on card
 - Centralized tracking of cardholders, cards, applications, and credentials, their respective lifecycles, and managing the changing bindings between these concepts
- Potential for increased government efficiencies through shared resources across discrete entities and use of a single scalable card platform



Fast Facts

- + One million cards issued
- Deployed through 199 total sites:
 - 57 State Agency of Australia customer service centers
 - 20 rural government offices (QGAPS)
 - 122 police stations

Beyond the **perimeter**

Ensuring business continuity through a multi-technology approach

Perimeter security is often considered in isolation to the wider business environment, seen primarily as an effective method to deter, detect or delay intruders or escapees. But those who stop there could be missing a vital opportunity in business continuity planning.

Steve Bell, Chief Technology Officer for security developer, Gallagher says a multi-technology approach to perimeter security can play a fundamental role in meeting ongoing operational requirements.

“Perimeter security is the first point of access control to a site, where businesses have the unique opportunity to ensure compliance and best practice at all levels,” says Bell.

By combining perimeter security solutions with electronic access control, you can determine not only who, where

and when, but most importantly: why? Why is this person here, are they in line with our internal policies and compliances, and are they authorised to be where they are?

Sharing information at the physical access point about inductions, required permits or licenses helps protect people, saves down time and prevents stoppages due to inadvertent site access, damage and injury.

“Shutting down operations due to accidents, or intentional damage, is extremely costly to any business,” says Bell. “Having the capability to prevent harm to people or equipment through a multi-technology perimeter solution is hugely valuable.”

Gallagher leads the way in layered, highly integrated perimeter solutions, with a range of customised electric fencing, taut wire and disturbance options.

Their electric fencing system is one of the safest forms of perimeter protection available, designed to comply with international safety standards and deter potential intruders without causing injury. Taut wire technologies such as tension and disturbance sensors provide perimeter detection suited to a wide range of security applications. They act as a strong deterrent and immediately send notifications of any disturbances on the perimeter.

Gallagher is recognised as an award-winning industry leader in the design and development of safe, effective perimeter security systems. With a strong focus on safety and innovation, Gallagher aims to redefine what’s possible for their customers and the security industry as a whole. Visit security.gallagher.com for more information.



With security comes safety

Our electric fence systems provide a powerful deterrent in the safest way possible.

Designed to comply or exceed international safety standards, they're installed safely by certified technicians. They're safe to operate. And thanks to a short, high voltage pulse they're even safe to touch (although you wouldn't do it twice).

To find out more about our industry leading perimeter security solutions, call a Gallagher certified channel partner or see our website.

security.gallagher.com/securityfencesafety

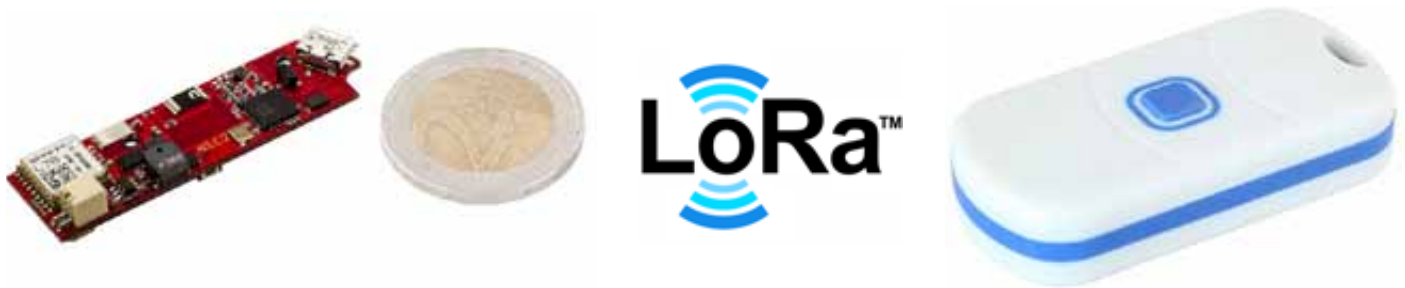
RETHINK SECURITY

security.gallagher.com



KCS TraceME TM-901 / N1C2

GPS/RF-module / OEM-version



The TM-901 / N1C2 is a budget product line member of KCS' advanced TraceME track and trace modules. The TM-901 is targeted for remotely tracking and tracing a variety of objects, even livestock, and for personal use.

The TM-901 offers excellent long range RF coverage and is equipped with a low-power GPS receiver.

The module is equipped with multiple on-board sensors, low-level I/O-connectivity and a solar (*) rechargeable integrated battery. It offers accurate location based position data to be connected to any existing worldwide server application.

Key Features

- Excellent satellite coverage
 - GPS
 - Glonass/GPS (*)
- Very small, only 53 x 15mm
- Lightweight: 3 grams for a fully equipped PCB
- Standby battery lifespan of more than 10 years.
- OEM version
- Excellent GPS accuracy, internal antenna.
- Integrated 2.45GHz. radio for special functions and peripherals.
 - Short range, up to 30m (*)
 - Long range, over 1 km range, line of sight
- LoRa™ technology
 - 868MHz. / 915MHz. (*)
 - Up to 60km line of sight at 25mW and with integrated antenna.
- Excellent indoor and outdoor performance with accuracy up to 1.5m
- Up to 3 LEDs for user interaction.
- 1 switch for user interaction.
- Onboard sensors:
 - Temperature sensor (±0.5°C)
 - 3D accelerometer (up to 16g) Optional: (*)
 - Humidity sensor (±2%RH)
 - Baro-/Altitude meter (±10cm)
 - Compass/Magnetometer(1-2°)
- Wide operating range: -25°C ... +85°C
- Multiple watchdog levels for maximum stability.
- Solar cell powered (*)
- Versatile interfacing:
 - Digital I/O
 - Analog input
 - Serial, 3V
 - iButton™ / 1-Wire™
- Buzzer (*)

- Event based free configurable module to fit any job.
- Remote maintenance. Both firmware and configuration files can be updated over the air.
- Supports integration into third party networks.

Applications

- Object protection, up to 10 years of standby on a single lithium AAA-battery.
- Logistics, M2M
- Animal tracking, asset monitoring
- Security and surveillance
- Remote control and diagnostics
- Anti-theft

Ordering information

- TM-901F - Full version (Long-range RF, optional Solar-charger)
- TM-901B - Basic version (TM-901F without: GPS, Buzzer, Sola-charger, ANT/ANT+)

(*) Optional, please contact sales for more details

Product Summary

Equipped with a state-of-the-art GPS receiver, the KCS TraceME TM-901 / N1C2 module provides reliable and accurate navigational data.

The full version module (TM-901F) is equipped with different technologies for traceability (e.g. GPS/Glonass, LoRa™, Bluetooth LE, ANT/ANT+ and proprietary RF), which can all be combined dependent of the application. The low-budget basic version module (TM-901B) is equipped without GPS while still offering the highly intelligent traceability functionality.

The combined LoRa™ and 2.4GHz. RF technologies offers tracing of the module over a wide area up to 60km. The rough tracing from 60km down to 300 meters is done by LoRa™, while the short-range tracing is done by the proprietary RF-

technique. This technique offers excellent indoor and outdoor tracing with an accuracy up to 1.5 meters. Traditional national telecom costs are avoided because of the absence of GPRS/SMS.

An intelligent 'Listen before talk' algorithm makes it practically impossible to locate the module which secures the valuable vehicle or asset. It enables stolen object recovery and thereby offers insurance premiums reduction possibilities.

Multiple on-board sensors (temperature, acceleration and optional: humidity, baro-/altimeter and compass/magnetometer) as well as buzzer, LEDs, I/O-functionality and pushbutton enable the integration of TraceME into a variety

of custom specific (M2M) applications. With a minimal size of 53 x 15 mm, weight of only 3 grams and a battery lifespan of more than 10 years, the module offers endless OEM integration possibilities.

The functionality of the module can be remotely programmed to fit any job. From basic/general functionality to advanced/low-level application specific detailed functionality.

All of the necessary server-side scripts to process and store data from these units are available for registered distributors and resellers. If you do not want to host data and maps yourself, you can use the hosting services of one of our partner companies.

Specifications KCS TraceME TM-901

Data communication

LoRa™	Semtech SX1272 transceiver
Frequency	868/915 MHz. (*)
Protocol	LoRaWAN 1.0 and custom LoRa™ protocol
Transmitting power	up to +20 dBm
Sensitivity	-137 dBm
RF 2.4GHz.	Nordic nRF81422 (BLE only) optional nRF51422 (BLE/ANT)
Frequency	2.45 GHz.
Protocol	BLE 4.0, ANT and custom 2.4 GHz. protocol
Transmitting power	up to +20 dBm (with on-board amplifier)
Sensitivity	-93 dBm (BLE), -90 dBm (ANT)

Navigation (*)

GPS Receiver	Quectel L70 GPS module optional L76 GNSS (Glonass + GPS) module	
Frequency	GPS L1 1575.42 MHz. C/A Code, 48 search channels Glonass L1 1598.0625 ~ 1605.375 C/A Code	
Sensitivity	Acquisition Reacquisition Tracking	-148 dBm (typical) -160 dBm (typical) -165 dBm (typical)
Horizontal Position Accuracy	<2.5 m CEP	

Electrical

Power supply	Internal Lithium AAA primary cell Optional external +5VDC ±10% (micro USB-connector)
Typical power consumption	2mA GPS low power tracking 100mA BLE/LoRa™ transmission 13 uA standby, sensors, timer and I/O active, no transmissions

External Connections

Power connector



Pin	Description
1	3.4 - 4.5V Battery (+) connection
2	Ground

Power connector (*)



Pin	Description
1	3.4 - 4.5V Battery (+) connection
2	Ground
3	External +4.5 ... +5.5VDC, or optional: Solar cell 5V

Micro-USB



Pin	Signal	Type	Description
1	USB VCC	VCC	+4.5 ... +5.5 VDC Charge input, max 600mA
2	Serial IN	I	Serial input or digital input (2..31V for active high) ~ 50k pulldown
3	Serial OUT	O	Serial or digital output, open collector (max 31V/10mA/100mW)
4	Analog IN	-	Analog input (0..44V)
5	GND	GND	GND for charge and I/O

About KCS BV

KCS BV, founded in The Netherlands in 1984, develops and manufactures electronics in-house for industrial applications, medical purposes, broad-casting solutions, etc.

Support

Visit our support page at: www.trace.me

Sales

Contact us by email: Trade@trace.me

Final notes & certification

We certify that Kolff Computer Supplies BV, Dordrecht, The Netherlands does not make any hardware or IMEI modifications to the QUECTEL devices as used in the TraceME track & trace device. All software modifications are restricted to official firmware upgrades as provided by Quectel Wireless Solutions Co., Ltd.

Warning

- The device should be turned off in vicinity of petrol pumps, chemical, flammable or hazardous environments where ignition of flammable atmospheres is possible.
- The module and antennas shall be operated at a distance greater than 20 cm from the human body.
- The device is to be operated in accordance with the user instructions or manufactured recommendations.

Disclaimer

KCS BV reserves the right to make changes without further notice to any products herein to improve reliability, function or design. KCS BV does not assume any liability arising out of the application or use of any product or circuit described herein; neither does it convey any license under its patent rights, nor the rights of others.

KCS is ISO 9001:2008 and ISO 14001 certified since 1999.

KCS TraceME Limited

Kuipershaven 22, 3311 AL Dordrecht, The Netherlands

Fax 1: +31 (0)78 6312659 • Fax 2: +31 (0)20 5248130 • E mail: Trade@trace.me • URL: www.trace.me • ©2016 KCS BV

KCS
Trace ME

KCS Trade PTY Limited

13 Mons School Rd, Mons Queensland 4556, Australia

Fax: + 61 733 197 302 • Email: krijn@kcs-trade.com.au • Web: www.trace.me

Burn Support Group Charitable Trust

Statistics tell us that there are over 500 children a year are admitted into hospital with Burn Injuries serious enough to require hospital admission!!

Burns are traumatic injuries for both patients and their family/whanau. Burn patients can be faced with many losses – their usual physical appearance, sometimes their home, income, and perhaps they are also grieving the loss of a family member or colleague involved in a fire. This is often experienced whilst also enduring a long hospitalisation period. Children who are severely burned often require many operations and special treatments over extended periods of time and have to deal with life-long consequences of disfigurement from their burn injuries. Clearly the emotional and social costs of burns to our children is just too high.

The Burn Support Group Charitable Trust is a non-profit organisation founded in 1987. Burn Support Group is committed to offering individuals who have experienced burn injuries and their families/whanua, emotional and practical support during recovery and beyond.

- Visiting patients and their families in the Hospital Environment.
- Improving patient care through the funding of equipment to help burn patients, services over and above that are funded by the health service.
- Offering to accompany and support children who have burn injuries when they return to school.
- Providing opportunities for mutual support for burn survivors, workshops, coffee groups and Annual Burn Support Children's camp for 7-18 year olds. Funded completely by Burn Support Charity.
- The once in a life time opportunity to attend the Phoenix World Burn Congress held annually in the U.S.A. Visit website for information on submitting application forms, www.burns.org.nz.
- Creating burn prevention awareness by attending appropriate community events with our display stand and relevant resources.
- Working with community groups such as NZ Fire Service, Safekids and Kohanga Reo. Providing free resources to interested schools, clubs and kindergartens.

The Burn Support Group Charitable Trust relies solely on the generous support of the public and different organisations who have and continue to donate generously to the Charity which is very kindly appreciated. We believe Burn Support Charitable Trust Group is making a difference in the community.



Burn Survivor Sunday

(Auckland) - Sunday 13th March
- Sunday 19th June
- Sunday 18th September

Baby Show

- Friday 19th-23th August

Fire Protection Conference

- 10th-12th November
- A.S.B. Stadium, Akld

Phoenix Society World Burn Congress 2016 (Providence Rhode Island, USA)

- 19th-23rd October

Charity Race Night @ Alexandra Park Raceway

- Friday 18th November

Burn Support Christmas Party

- Sunday 4th December

2017 CAMP AWHI-NZ Children's Camp

- January 23th-27th

Yes I want to make a difference to the lives of burn survivors and their families

Please accept my donation of \$

Details:

My email address is:

I'd like to donate by:

Online at www.burns.org.nz OR

Enclosed cheque made payable to Burn Support Group Charitable Trust. (PO Box 97164, Manukau City, Auckland 2241)

Please contact me about:

Making regular donations

Leaving a bequest in my will

All donations to the BSG are tax deductible and receipted. Charities Commission No: CC48691.

Continuous Development Brings Benefits

Since 1991, a planned process of continuous development has seen the range of LOKTRONIC electromagnetic locks progressively refined in both quality and function. This process clearly does not stop and at a recent interview, Peter Calvert, consultant at Loktronic Limited, outlined the latest round of design, function and aesthetic qualities.

The LOKTRONIC slimline series of electromagnets is widely known to incorporate the most sophisticated Magnetic Bond Sensor (MBS) on the market. Utilising two paired sensors rather than the industry standard one sensor, the Loktronic end-to-end MBS is sensitive to three parameters, voltage, alignment and interference between the electromagnetic face and the armature. Should any of these factors change, a signal is created. In New Zealand, with many commercial doors being wooden framed, the alignment between the armature on the door and the electromagnet on the frame can change with variations in humidity leading to a lock insecure signal being created. Not anymore! Loktronic now provides wider steel stock for armature manufacture, the extra 6mm width trebling the allowable variation before a lock insecure signal is created.

A Problem solved

Another feature of Loktronic electromagnetic locks has been the incorporation of a Door Position Switch (DPS) with the driver magnet glued into a slot on the armature's end. Steps were incorporated into the armature to remove steel in close proximity to the DPS magnet and thereby improve its performance. Nevertheless, on occasions these magnets have been prised out by vandals thereby compromising security. Loktronic have sourced high performance rare earth magnets and fitted these into custom made aluminium housings which are in turn secured to the armatures by stainless steel fastenings.



New, wider armature (lower) and previous model (above)

Clever thinking!

The companion DPS reed switch component was traditionally fastened to the end of the electromagnet with a high performance cyanoacrylate compound. Whilst very strong, the bond could potentially be broken with side force. In the latest generation of locks, this switch is secured on a flexible mounting which will absorb almost any pressure yet return to the original position when the pressure is removed.

Guaranteed for 10 years

Finishes are important for several reasons, functionality, longevity and aesthetics. Loktronic has upgraded the plating on the armature from blue passivated zinc to electroless nickel, the same finish as that on the electromagnet face. The benefit is that because both mating faces are plated with the same metal, the potential for galvanic interaction is removed. These long life products are now further enhanced, so you are ensured that not only will they work correctly for a long time they will look good too.

Nice one, Loktronic!

Not content with these upgrades, Loktronic has improved the aesthetics of the housings so that all aluminium components are now bead blasted before being anodised to give a uniform finish.

Having given the lock range all these upgrades, attention was focused on the Z/L brackets often used in conjunction with the lock on inward opening doors. Redesign involved commissioning a new tool for extruding the grooved aluminium profile. The vertical face has been increased in height by 6mm and the sex nut position shifted higher up. This has two benefits. Firstly, it more than accommodates the increased width of the new armature and secondly, it means that the Z/L bracket can be used with the wider profile Loktronic FFC gate locks. To ensure that the aesthetics are uniform, the Z/L brackets are bead blasted before anodising too.

Loktronic continues to improve its products based on your valuable feedback. If you have a suggestion, they welcome your feedback on 0800 FORLOK or mail@loktronic.co.nz.

Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

HOLD ON A MINUTE

...OR AN UNRIVALLED 10+ YEARS!

Not all products are created equal.
Take Loktronic's premium quality Fire
Door Holding Electromagnetic FDH40...
they are simply the best in their field.



PLAY IT SAFE AND LOCK IN
Loktronic quality, every time



FDH40S: Standard, floor mounted



FDH40SS: Flush mounted



FDH40SS: Surface mounted



Designed, tested
and produced in NZ
to AS4178

10 year guarantee*

Unbreakable
universal mounting

Floor or wall
mounting options

Superior quality
materials
and fastenings

Full and immediate
on-shore support

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

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

*Standard terms & conditions of sale apply.

CCTV surveillance in the **command & control** continuum

CCTV expert Peter Houlis spoke on his experiences of implementing early safe city schemes in the UK as part of the seminar series at last November's New Zealand Security Conference and Expo. The February edition of NZ Security featured the first of a two-part series based on his presentation, "Lessons learnt in implementing early safe city schemes: An integrator's view".

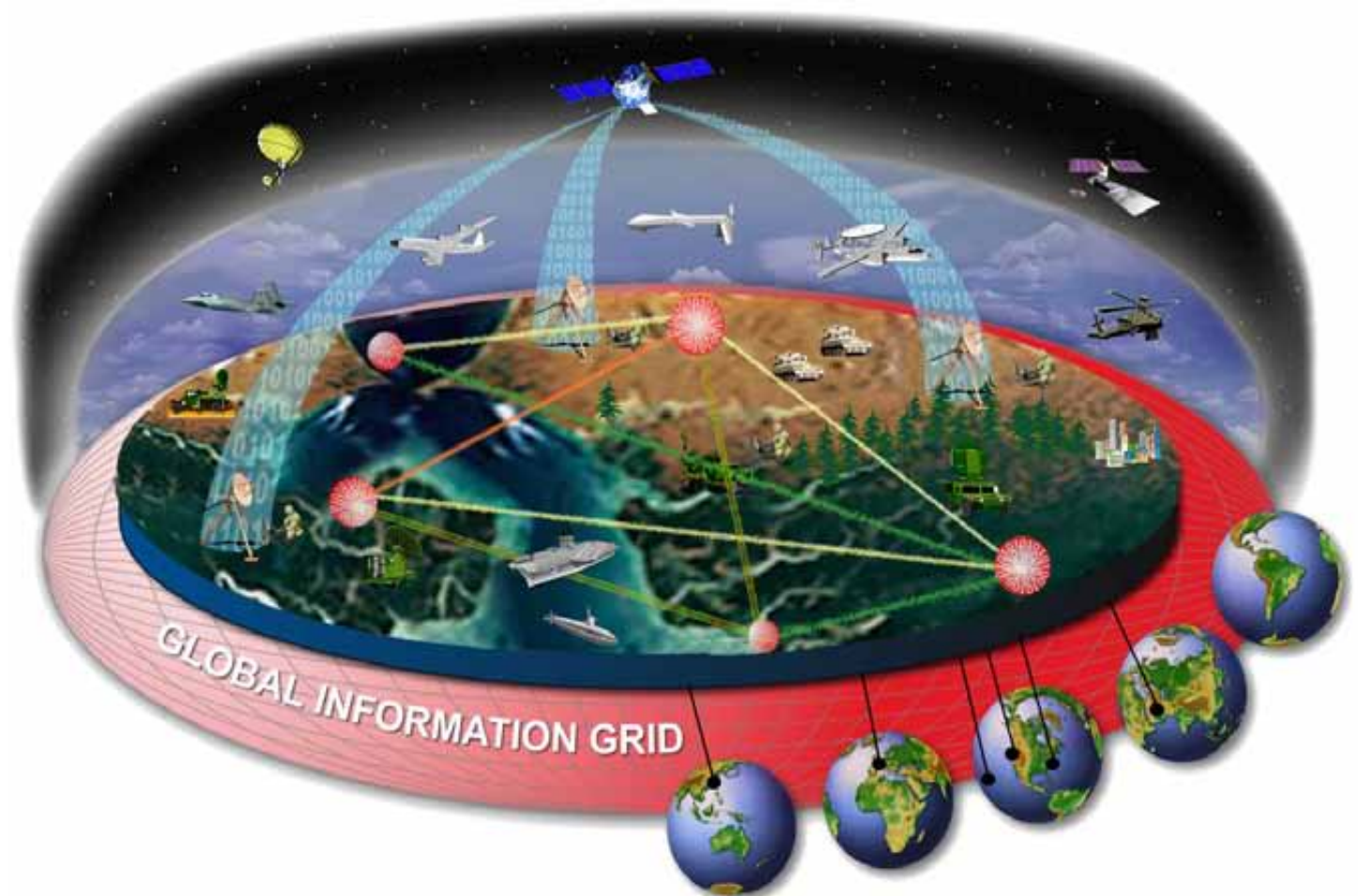
This is the second article of the series. Aimed at drawing from Peter's involvement in early CCTV-led safe city schemes, we look into lessons learnt from the integrator perspective, and gain an understanding of the role of surveillance through the military concept of C4i.

Cameras as part of C4i

C4i has its origins as military terminology, which began as C2 – 'Command and Control', a well known operational and tactical concept that refers to the ability of commanders to direct and hold the reins of their forces. C4i extends this principal to command, control, communications, computers and intelligence.

It is, stated Houlis in an article in IFSEC Global, "a complex 'system of systems' generally using high technology commercial 'off the shelf' equipment and devices (COTS) which can be applicable in both military and civilian life." It's a life that in many population centres is increasingly associated with escalating threats of crime and terrorism.

Basically, it's about information superiority and the ability to use it to elicit the most appropriate response in a given scenario. "Technology and human resources are used to gather relevant information and accurately communicate this information to appropriate human and technology assets," he wrote, "thereby increasing situational awareness in order



to realise the application of appropriate responses and control measures to an event based on up-to-date intelligence.”

According to Houlis, information superiority wins wars, and this translates well into safe cities. “It’s all about situational awareness, and what decisions the information leads us to make.”

C4i and the city

The threat landscape has changed since the 1980s. Global events have changed perceptions of security, and the public demands – and has a right to – a safe environment. Interestingly, through mobile technology, the public is also increasingly playing an active role in incident response.

Houlis offers the example of a bomb explosion on a street. “A police commander will take charge and have authority to make decisions and call in the bomb disposal team; he might delegate some control to a senior paramedic and may allocate some power to the fire chief and to the senior response officer if the perpetrator is still in the vicinity.”

“Witnesses’ information then needs to be corroborated with footage. Their story can then be corroborated with the information gathered by the various technical systems. This delivers a high level of intelligence upon which informed decisions can be made.

It’s about making the information relevant, using such things as map overlays. It’s about detecting and reporting exceptions to the norm.

In the example of the London riots, he says, “most of the arrests came about as the result of people videoing it on a mobile phone.” Creating a safe environment in the contemporary context is everybody’s responsibility. This then begs the associated question of how capabilities such as privately owned mobile phones and drones might be integrated into the first response.

In terms of the control room, it’s about having the monitoring tools to quickly identify exceptions to rules: the build up of crowds (a precursor to violence), trespassers, one-way traffic flows, panic button triggering, vehicle identification, “and – when we can get it working correctly – facial recognition.” All of these things, states Houlis, make a control room operator’s job considerably easier, although it comes down ultimately to the specific skills of the operator in identifying exceptions.

The control room approach, he argues, has to be more proactive and go beyond the control room. It would be useful for the responder, for example, to have a

tablet and see what they’re meant to be responding to, and how the situation is developing en route, and assess resourcing requirements. “Information needs to go with people – with the requisite authority – to make decisions on how to respond, particularly in relation to shootings and terror events.”

According to Houlis, social media is very useful in the safe city scenario in terms of disseminating positive information. Text or email alerts can provide people with the information they need to make decisions to avoid dangerous situations.

“Safe cities are about big data; collecting it and analysing it and passing it on to the people that need it. It’s about knowing what’s going on so you can do something about it. What you need to know not to get caught out.”

Identifying the right people

Houlis is staggered by how much politics is involved in city surveillance systems. Government priorities are continuously changing in relation to threats, funding and votes. Even councilors chasing votes, he observes, affects the placement of cameras.

“The reason why Newcastle and Edinburgh [safe city surveillance projects] were so successful is that they had a very very strong project champion: someone prepared to stand up and be counted, who had the authority and strength of character to drive the project forward.”

“Also needed is a strong project manager to back the project champion up and keep everyone in check.

The next problem, he suggests, is stakeholders. “You need to identify all stakeholders involved. You need to define the roles of all stakeholders very clearly. It’s very surprising how quickly people lose interest in a safe city scheme. Their everyday roles take over. If they don’t have a very clear MOU then things can quickly go off the rails. If they fail to uphold their obligations, you have to have ability to react accordingly. It only takes one stakeholder to spoil a project.

“On the delivery side, you need to have stakeholders experienced in delivering large scale systems. You need to develop good relationships with systems designers and consultants and those responsible for power, civil works, etc.

“You need good experienced integrators who can advise on all aspects of the technologies and give you a good idea of budgets, but they’re probably not the best people to analyse the risks.” This is where the police have an important role to play.

GREAT NEWS!

**NZ’S
finest
electromagnetic
locks
are now
possibly the
world’s
best
with our...**

4

**point
2016
upgrade.**

**Simply
the best!**

**Buy Loktronic.
Made in New Zealand.**

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

21516



A bank of CCTV cameras keep watch in London's Royal Docklands

Last but not least, one has to take into account the network and therefore IT companies. It's also important that the integrator can provide the IT company with a clear understanding about what is required around handling volumes of data.

Managing scope creep, managing budgets.

Set clear objectives. "You need to know what you're putting the system in for, what is the objective, and why," says Houlis. "What is the information you want to capture, how do you want to see it and in what detail? Where do you want to collect that information from, when do you want to collect it? Who wants it, who needs it?"

By way of example, he suggests that one wouldn't install a camera for anti-terrorist purposes and expect it to provide information on retail. Cameras on poles generally won't provide the footage of the shop front that you need due to the presence of overhanging shop canopies.

According to Houlis, it's about understanding the threat landscape. "Once you have identified the threats based on operational requirements, then the technical requirements can be matched to it in terms of camera specifications, etc."

But the threats and the vulnerabilities change. The world of IP has made video transmission easier and more cost effective, but it has also brought with it security problems. CCTV networks, for example, need to be made secure from hacking. "In 2010, the 120,000-camera Moscow surveillance system was compromised by someone who fed pre-recorded footage into the system", he notes.

Then there are aspects such as predictive crime analysis, where one needs to look at legislation that protects the general public – who watches the watchers? "It's about building trust and cooperation between all parties."

The SNAP framework

In light of the above challenges, Houlis developed SNAP, a framework for quickly deciding whether a CCTV surveillance system is the right solution to a problem – and whether it will be legal. SNAP divides decision making into four key areas:

Sustainability – this involves questions around such things as operational costs, funding for repairs and maintenance, etc. Are capital funds required and are they available to implement any proposed surveillance scheme? Are the operational costs and streamed revenue funding budgeted for management, supervision and monitoring staff realistic? Is funding for ongoing maintenance and post-warranty service and repairs available? Is the project partnership funded?

Necessity – is CCTV really necessary? It's not the panacea against all evils, and one needs to ask the question why. What is the system's scope? (ie. prevention and detection of crime, public safety, etc). What are the areas to be covered, and what degree of coverage is required? Ultimately, are there other options?

Accountability – this covers the legal implications of introducing video surveillance. We're all governed by encroaching legislation, which places increased responsibility on those operating and using video surveillance. What controls are in place, who will monitor the footage, and does it comply with the relevant legislation?

Proportionality – is CCTV appropriate given the location and environment and the problem to be addressed? Have other solutions been investigated and discounted? Is the solution proportionate to the problem? How many cameras will it take, how will the images be transmitted? What about costs, power, and the extent of civil works required for installation. Is the lighting suitable or will additional lighting or IR lamps be required? Have local planning regulations been addressed?

The factors that go into the making of a safe city are infinitely varied, and the range of stakeholders and their interests are more variable still. Despite the myriad of challenges involved, Houlis' experiences are clear evidence that the vision of the surveillance-enabled safe city is possible... and the expanding technologies of C4i are indeed broadening the notion of just what is possible.



Peter Houlis

A Chartered Security Professional, Peter boasts a 35-year career that includes a meritorious track record of designing ground breaking, high end CCTV, access control and integrated security solutions. For over two decades he has been MD of the multi award winning security system integrator 2020 Vision Systems, having kicked off his career as security systems and fire alarms engineer at the age of 16.

He is also a member of the Security Systems and Alarms Inspection Board (SSAIB) a UKAS accredited Certification Body, and has represented them on the British Standards Institute (BSI) technical committee responsible for drafting European CCTV Standards. He is a member of the Security Institute and Security Leaders Technology forum and has authored a number of published security articles.

NZSA Chairman sets out 2016 vision

At a breakfast networking event in Takapuna, new NZSA Chairman Doug McCormick laid out his vision for the organization for 2016. His presentation was made just prior to an NZSA board meeting scheduled for the same day.

The vision included improving communication with association members, targeting member support services, appointment of a full-time CEO, a review of the organisation's value proposition to members, achieving the organisation's strategies and goals, and resolving structural and governance issues.

On the membership front, Mr McCormick suggested a number of new initiatives to grow and support membership, including engaging with the majority of people in the industry who remain non-members, promoting the value of membership to security industry end-customers, promoting NZSA membership through non-security industry publications, raising general public awareness and continuing the organisation's role in political lobbying.

Also up for review was the various member purchasing schemes, including the Mobil fuel card, n3 trade card and insurance. Despite a membership that represents 85% of the country's total security workforce, the NZSA's membership represents only a small fraction of the businesses within the industry, and thus the value proposition of the association to the majority of individual non-members must be explored.

Mr McCormick also signaled an intent to grow the NZSA's training business, promoting NZSA training to a wider audience and ensuring a high quality benchmark.



Doug McCormick the NZSA Chairman

In terms of the association's governance structure, rules and by laws are to be reviewed, as is its operations manual. Delegated authorities are to be clarified and restructured to meet current needs.

The 2016 vision also includes a re-look at the association's media and conference strategy, including an evaluation of various online engagement models, such as social media and email newsletters. Those in attendance articulated the need for targeted engagement that acknowledged the diversity of the industry's varied segments.

Also to be considered would be the way in which the NZSA utilises paper publications going forward, such as NZ Security. While the value of the magazine's editorial and advertising features to the industry was widely acknowledged, he suggested that the association may also look to promotion in non-security publications in order to reach a wider audience.

Mr McCormick also took views from the floor in relation to the validity of the existing annual New Zealand Security Conference and Expo format, suggesting that alternative formats designed to make the conference more engaging and less 'inward-looking' needed to be explored.

The NZSA Board Chairman, Doug McCormick, is pleased to announce on behalf of the Board, the appointment of Gary Morrison to the position of Chief Executive Officer of the NZSA.

Gary has been acting CEO for the past 3 months.

The Board followed a careful process and after interviewing applicants, decided upon Gary for the position. We know that Gary will bring both his managerial experience and his extensive knowledge of the security industry to the position.

Gary is well aware of the strategic direction that the Board wishes to embark upon, his sense of where we need to be is in alignment with the Board's expectations.

Under Gary's management, we are confident that the NZSA will not only continue to provide quality services to NZSA members and the industry as a whole but also improve upon these existing services as well as add new support initiatives to benefit our membership.

To anyone associated with the security industry, look out for Gary, he wants to meet with you, to listen and to answer your questions!

Loktronic

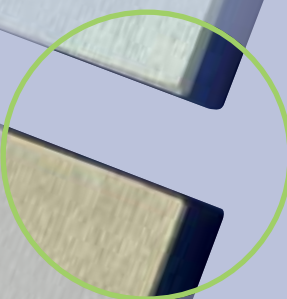
SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL**

1

The 6 mm **wider armature** allows for a greater margin of misalignment in the vertical plane. PLUS, the MBS will not falsely report misalignments.



Standard features include:

- Field-selectable 12 & 24 VDC options
- 550 kg holding force
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless sex nut
- Full protection against transients.
- Door Position Switch
- End-to-end Magnetic Bond Sensor

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 21516

Gary Morrison the newly appointed NZSA CEO: Q&A

Gary Morrison joined the NZSA on the 1st February as acting CEO and has just received confirmation of his appointment to the CEO position effective from the 1st April. Although his appointment is recent, it's not the first time he's played a key role within the association. NZ Security recently talked with Gary about his new role in implementing a number of new breakthrough directions from the board.

An accountant by trade, Gary has been in the security industry most of his life. Commencing with Armourguard on the financial side, he moved to operational management, ultimately serving five years as general manager for New Zealand and Fiji. Following a couple of ownership changes and disagreement with the direction being taken by the parent company, he decided after 20 years with the company to "get out and do something different".

With a business partner he bought a business and rebranded it as Icon Security. He grew it over 12 years into one of the largest privately owned manpower providers in the country. Subsequent to selling Icon, he has spent the past three years doing consulting work, primarily with Serco and including involvement with Mount Eden Corrections Facility.

Gary has had an interesting background with the NZSA. One of their biggest supporters, he sat on the board for many years, but then resigned as a member while with Icon. He'd gotten "a little older and a little more pedantic around an issue of fees", and after talking to the CEO at the time who brushed his concerns off, he left the association, hoping that he might get a call to sit down and discuss the issue.

The call never came, and it left him with something of a bad taste in his mouth. But rather than sour grapes, it has given him a passion about coming to his new role, and a goal to get out and talk to as many members, non-members and customers as he can.



Gary Morrison, is the new CEO of New Zealand Security Association effective 1st April 2016

NZSM: So what is the mandate you've been given by the board as CEO?

GM: From the board there was approval given to look at making some changes. Some of them I can talk about, some of them are awaiting board approval. There is one fundamental issue that we've talked about and three directional changes that I've put forward, which I've been given the mandate to evaluate further.

The real issue is that there is a feeling that as an association we've become disengaged from the membership, and this predominantly comes back to poor communication rather than the association not having done the work behind the scenes. We've been achieving certain things but not communicating these and making sure that the membership is aware of what we've been doing and the value that they actually get from it.

Examples of this include the complaints process and the audited accreditation process, which is where we audit members to the code of practice. The processes are there, and a lot of work has gone into them, but we haven't gone out there and really sold them to the membership or even told them how it works.

Effectively the outcome of this is the three main strategies I'm now working on: (i) improving our communication, (ii) growing our membership, and (iii) addressing concerns around fee structure.

NZSM: How will the association look to improve its communication?

GM: For the first two months and whilst in the "acting" role I set myself the goal of talking to as many members and non-members as possible. And I think the feedback from the non members has been as important if not almost more important than the views of the members because they're the ones who've been disillusioned and who've taken some convincing. They're also the ones who have quite strong views that are often historic and can be talked around.

One of the things that's come back is that we've got a very, very diverse membership. Our members have very different interests, and what they see as the value they can gain from the association is quite different too.

We've got a number of members who say "don't give us fuel cards and all that; all we want to see is lobbying and getting changes to the statutory side of things," through to those saying "my membership fee is being paid for by my Mobil card, so I'm happy with that as long as you continue to do other things as well." So there are different drivers we need to be mindful of, and what it's reinforced to me is that we need a broad package.

For the past five to eight years our membership has been static. What is obvious to me is that we don't have a strong membership with business sizes between 30 to 200 staff. These are important businesses that provide a lot of employment, and they are very significant players particularly in provincial areas.

Our membership fee is structured rightly or wrongly on staff numbers, and it's making it very unattractive to become a member if you have more than

30 staff unless you are one of the few multinational companies.

NZSM: So how is this resolved?

GM: I put to the board a recommended change to our membership fee structure designed around making it more attractive to those businesses in particular. It involves increasing the fee band sizes (covering that group) from what it is currently so that we now have bands covering 31 to 100, 101 to 200 and over 200. This significantly lowers the membership fee for those businesses with over 30 staff but less than 200. The feedback I've had from businesses is that it makes it far more attractive to them and removes a significant barrier to membership.

This is an interim step, and I think that longer term we need to look at a different model. Most associations have a three or four tier membership, and you get specific benefits associated with your tier. That to me is a more sensible model long term but it's not one you can implement immediately without assessing how it would work out for everybody.

NZSM: What else are you looking at?

GM: Another key area is the conference/exhibition/awards dinner, which has traditionally generated funds for the organisation as well as being a focus point for recognising excellence. What has come through very strongly from the members and non-members is that the conference has probably become a bit of an outdated model.

The concerns that have come out quite strongly is that it has become very much Auckland-based, and that there is difficulty in arranging speakers who can cover the topics that people are interested in. We've spent a lot of money bringing in international speakers, and I've had a lot of members say that the topic wasn't specific to them.

We are so diverse and the range of interests is so extreme that you can't cater for it in a conference over two days. The reality is that we had 40 attendees last year, and it's been a dwindling number no matter what effort has gone into it. I think the writing is on the wall that we need to review it and look at doing something different.

There is however a lot of support for recognising excellence in the industry and doing that through an awards dinner, particularly if that dinner can be taken to the provinces. You've got the benefit

of making it a destination of choice, such as Rotorua, where people can take their families or senior management team and make it a bonding exercise.

The format we're looking at is to hold two educational workshops on the Friday afternoon and on general themes of relevance to almost everybody who will be there, followed by an awards dinner in the evening. The idea is to recognise the outstanding performers from a people point of view, not businesses, and putting in place a broader classification of awards to better reflect the breadth of the industry.

NZSA: Where does that leave the exhibition?

GM: Holding an annual Exhibition is still very important for us. We have strong ideas about partnering with other similar organisations or associations in relation to the exhibition so that we've got a broader appeal and we can share the costs and the expertise. That's still a work in progress, but we've made some strong inroads in planning for that.

It will be a generator of funds going forward, but it will be a far more risk averse model that will have broader appeal to the membership.

NZSA: Where does the provision of training sit within the association's 2016 vision?

GM: Part of the strategy is to revisit and put some planning around our training division. It's one I can't say a lot more about for now as it is commercially sensitive, but it's one where we see that our involvement does add value to the industry. We can set standards, we can help facilitate training – both mandatory and at a more personal level – throughout the industry.

The challenge we have is that we've got a fixed cost structure with a variable revenue income. Ultimately training is vital to our industry and it is significant to the association's future direction.

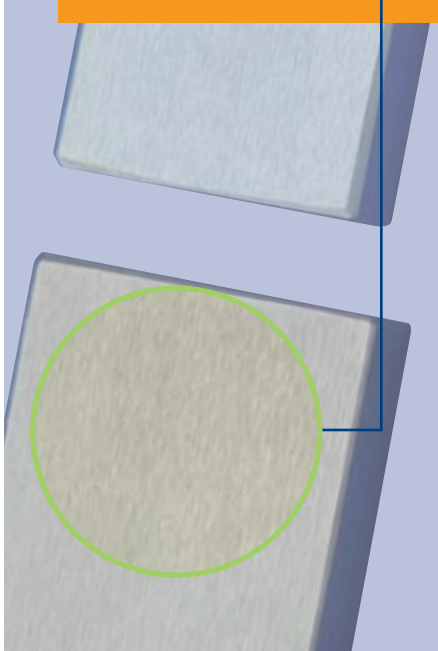
Other things we're revisiting are the networking meetings, potentially taking them more into the provinces or otherwise making them easier to access by the members, and having more relevant topics. We are looking to increase our awareness of social media and online media, how we market and promote ourselves, and being more visible in the media. It's planning in progress on these issues but we already have some traction with a breakfast session scheduled in Rotorua and the developing of closer relationships with the press.

Loktronic
SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL 2**


Unightly galvanic
action on plates is
eliminated through
BOTH Electromagnet
and Armature being
**Electroless Nickel
Plated.**



Options include:

- 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

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


21516

Removing the ‘What ifs’: Baggage security on international flights

Many of us are hit by a feeling of dread the instant we part with our baggage at check-in or bag-drop.

Knowing that it will be many hours before we are next reunited with our bags just moments before undergoing customs checks at a foreign airport leaves us with the unnerving question: what if the bags are tampered with?

Thankfully, we’re not the only ones who think about this sort of thing. Legislators, airports, security providers and start-ups alike are also involved in the business of maximizing baggage security in transit. While news reports remind us there remain gaps in the system, a number of innovative solutions have also emerged to keep security-conscious baggage owners on the right side of the law.

Unisys to secure baggage on New Zealand flights

Unisys Corporation announced late in January that 16 international airlines operating to and from New Zealand have signed a four-year agreement for Unisys to continue providing an advanced baggage reconciliation system for international flights operating from Auckland, Christchurch, Queenstown and Wellington airports.

The baggage reconciliation system links passengers with their bags, tracking both as they move through the system to help the airlines comply with aviation industry security requirements.

Each year the participating airlines secure and validate bags for more than two million passengers on flights departing New Zealand.

When passengers check in, each bag receives a barcode, which is then





scanned and reconciled with a passenger record before the bag can be loaded onto the aircraft. As the airline has a record of the baggage loading order, bags can be quickly identified and recovered if passengers fail to board. This process is designed to prevent a mismatch of passengers, crew and baggage, and to enhance security levels by avoiding the possibility of unaccompanied baggage being loaded on the flight.

The Unisys baggage reconciliation system helps airlines comply with the Hold Baggage Authorisation (HBA) regulations, also known as Account And Authorise (AAA) regulations, for baggage handling defined by the Civil Aviation Authority of New Zealand.

“The Unisys baggage reconciliation system helps our member airlines comply with industry-mandated security requirements for baggage handling, while providing efficient processing to quickly find or remove baggage to help prevent delays,” said John Beckett, executive director, Board of Airline Representatives New Zealand.

Intrude-A-Lock keeps luggage secure

In case, like many people, you're not totally satisfied with leaving the security of your luggage to good fortune and the good will of baggage handlers and fellow passengers, you may look to additional forms of protection. There is the traditional approach of combination locks and padlocks, or wrapping your bags in layers of cling wrap – designed to frustrate baggage owners as much as would-be-baggage interferers – and now there is Intrude-A-Lock.

Eight New Zealand student teams made up of 38 young entrepreneurs have just spent six weeks of their summer building startups from scratch as part of the Venture Up program. They converged on Auckland in February to pitch the businesses they had spent the previous six weeks building.

Leading New Zealand youth entrepreneurship accelerator Venture Up hosted the Showcase at the City Gallery. It was the final pitch event to wrap up its immersive entrepreneurship program aimed at 16-24 year olds. One of the student teams in particular has received media interest for their innovation – the Intrude-A-Lock.

The Intrude-A-Lock is a smart device that can be placed inside cargo or luggage shipments in order to detect when illicit activity has occurred in transit. According to the Intrude-A-Lock website, detection is sensed through the recording of movement and light levels. These are sent to the user's phone through a proximity-based bluetooth protocol with a date and time stamp of when these activities may have occurred.

The application can also send the log of activity directly to travel authorities as evidence of innocence... a definite step up from cheap padlocks and wrap.

The Intrude-A-Lock site claims that although it is often perceived that the chances of having one's luggage compromised is low, it is reported that more than 3.4 million suitcases are damaged, tampered with or stolen each year. Passengers are often forced to take legal responsibility for any content that has been illicitly placed in their suitcases due to their lack of ability to prove that the content had been placed in the luggage by someone else.

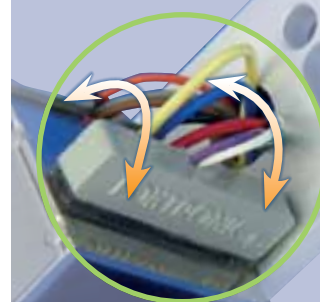
Loktronic

SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

UPGRADE DETAIL 3

Dislodging of the **Door Position Switch** is now almost impossible through the **flexible** (non-rigid) **fastening** technique adopted.



Standard features include:

- Field-selectable 12 & 24 VDC options
- 550 kg holding force
- Slimline styling
- Instant release
- Stainless steel fitting hardware
- Through hardened, polished stainless sex nut
- Full protection against transients.
- Door Position Switch
- End-to-end Magnetic Bond Sensor

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 21516

Frontline: **Guarding** in the news



The man who punched Sydney bouncer Fady Taiba, leaving him in a coma for 19 days and with lifelong injuries in 2013 will spend a minimum of three years in jail. James Ian Longworth, 35, was sentenced in the NSW District Court on 18 February to a maximum of four years and 10 months' imprisonment.

Mr Longworth had embarked on a heavy drinking session with mates at the Concourse Bar, near Wynyard station on the night of 06 September 2013.

Mr Taiba, a father-of-four, was working as a bouncer at the front of Bar 333 when he observed Longworth

stumbling and refused him entry. Security footage captured Longworth walking away before rushing back moments later and striking Mr Taiba to the head.

Last October, a jury found Mr Longworth, an employee of UBS investment bank, guilty of recklessly inflicting grievous bodily harm but not guilty of the more serious charge of intentionally inflicting grievous bodily harm.

In handing down the sentence of four years and ten months, Judge Richard Cogswell said Mr Taiba's injuries were

in the upper scale of grievous bodily harm, but that the court could not find the punch was premeditated. "The act was not accompanied by planning or calculation, but nor was it immediate or instinctive," Judge Cogswell told the court.

The court heard that the 35 year-old Mr Longworth was suffering from depression at the time due to his father's death and the misplacing of his ashes.

Mr Taiba was left with serious brain damage and suffers frequent seizures. Mr Longworth will be eligible for parole in three years – February 2019.

Hagley Oval marching orders

In another case of alleged heavy-handedness by security guards, news media has reported that Police will not be acting on a complaint laid by a spectator after he was pushed in the face by security during day four of the second cricket test between New Zealand and Australia at Christchurch's Hagley Oval on 23 February.

Australian expat Luke Geldard claimed that the action taken by the security guard was assault.

According to a Stuff.co.nz report, Mr Geldard had been told by security that he had received a number of warnings in relation to his behavior, and attending police who ultimately escorted him from the park had assessed him as being drunk and argumentative.

Mr Geldard, a Christchurch resident, claimed reports, was to be defending unrelated assault charges against him in court this month.

The Red Badge Group provided security for the event.

Eden Park red card

In other guarding news closer to home, one of two men removed from Eden Park by security after streaking during 26 February's Super Rugby game between the Blues and Highlanders has filed a police complaint against one of the guards.

The man chose to remain anonymous.

After being apprehended by three guards, the man claims that he was assaulted by one of them following his removal from the field and after he had been taken away from public view. He required several stitches after he claims he was punched several times by the guard.

Eden Park has taken the matter up with its contracted security company, Platform 4 Group.

Security struck by car after manhandling shopper

In a recent Christchurch District Court trial, 69-year-old Richard John Hewitson pleaded guilty to a charge of reckless driving causing injury in relation to an incident in which he reversed his car into a security guard.

According to press reports, the man had earlier been approached by the plain clothes security officer in St Martins New World supermarket at about 5pm on 01 July 2014. The officer had confronted him after he had allegedly placed a small packet of cheese into a satchel he was carrying and had attempted to leave the store without paying for it.

Security video footage apparently showed Mr Hewitson being held by either his shirt or throat and pushed against a wall by the security officer.

The incident continued in the car park following the confrontation. It is there that Mr Hewitson reversed his vehicle into the security officer, leading to the latter being pinned between the reversing car and another passing vehicle.

The security officer sustained a crush injury to his leg, requiring hospital treatment and six months of physiotherapy.

Judge Emma Smith accepted defence claims that Hewitson had been "somewhat manhandled" by the security officer but that he had acted recklessly in reversing his car into him.

Mr Hewitson was ordered by Judge Smith to undertake 200 hours of community work and to pay \$1,000 emotional harm reparations to the security officer. He was also disqualified from driving for 13 months.

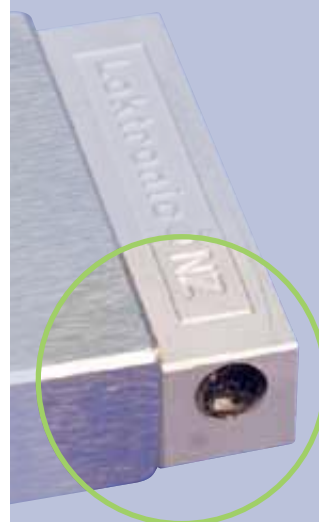
The cheese was never found.

Loktronic
SECURITY • TECHNOLOGY • RELIABILITY

your
electromagnetic
lock

**UPGRADE
DETAIL 4**

Substantially improved
DPS Reed Magnet
fastening is extremely
secure, making the
product much more
Vandal proof.



Options include:

- 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

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 21516

IP opens doors to a new world of physical access control

Contributed by Axis Communications



1. A revolution at the door

It is no exaggeration to say that network video has revolutionized the world of CCTV. Now the access control industry is on the verge of a similar, groundbreaking development. Once again, the driving force is the transition to TCP/IP-based systems.

Since the introduction of the first network camera by Axis Communications in 1996, digital network video surveillance systems have developed fast and now delivers a wide variety of advanced features that never could have been attained by solely relying on analog technology. Today, distributors, integrators and, not the least, end users have come to expect a wide range of useful functionalities, such as remote accessibility, high image quality, event management and intelligent video capabilities along with easy integration, better scalability, greater flexibility and cost-effectiveness.

IP versus traditional access control

The migration of access control systems to a digital environment is sure to bring many comparable benefits, i.e. lowering installation costs, facilitating configuration and management, while simultaneously enhancing the versatility of the systems and opening up for integration with other security products.

Of course, IP-technology is not totally unknown to or unused in the access control industry. But existing systems have not been able to fully exploit the advantages of IP.

Typically, a legacy access control system is dependent on having each device – card reader, handle, door lock, door position switch, etc. – hard wired with RS-485 cable into one central unit or central server. Besides being proprietary systems, which confines the end user to one single provider of hardware and software, these solutions often tend to be very complex and require expert personnel to handle installation and configuration.

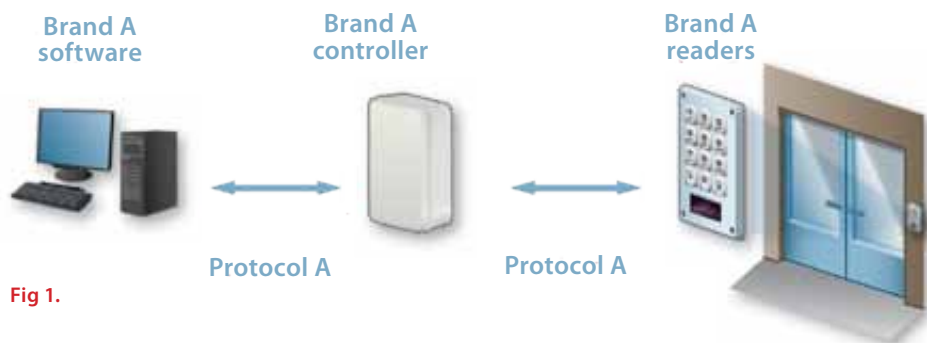


Fig 1.

Fig 1. A typical legacy access control system built around a proprietary technology from one single supplier.

Further more, when expanding traditional analog systems the process is complicated by the need to consider that a typical central controller is built to accommodate a certain maximum number of doors, normally 4, 8, 16 or 32. Not only does this limitation make the system inflexible but also makes it difficult for the end user to match his requirements with products available, e. g. if there is a want for access control at, say, 9 or 17 doors. The lack of flexibility also brings high marginal costs, which can make the addition of one extra door unjustifiably expensive.

2. Small basic systems

All in all, conventional access control products and systems are normally designed and optimized for large installations with a lot of doors and maybe thousands of credentials (cardholders). The actual market looks very different. According to Sales & Security Integrator gold report (2013),

the average installation consists of 10 doors and have about 128 credentials. Only about 20% of the installations have more than 10 doors.

Without the need for hard wiring to a central control unit or central server, IP-based systems enable installations that are non-proprietary, flexible and scalable. This means not only a more versatile solution, but also a more cost efficient one. Freed from the constraints of enlarging the system in certain multiples, a network-based system can - should it be necessary - be enlarged by one door, and one reader, at the time.

Furthermore, TCP/IP enables “edge” solutions. An edge solution has one controller for each door, which then is connected to the existing local Ethernet through a regular network switch. Since IP networks now are ubiquitous in offices, stores, factory plants and similar facilities the cost of adding an IP-based door controller would be minimal, as opposed to

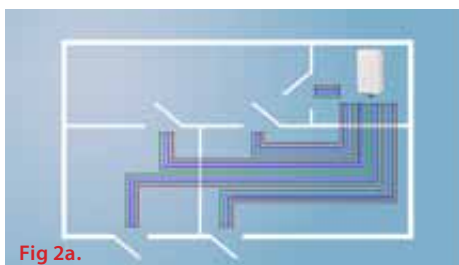


Fig 2a.

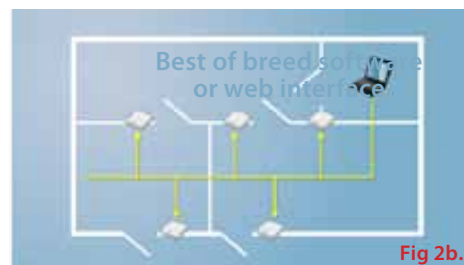


Fig 2b.

Fig 2a. Traditional installation with one central unit and proprietary cabling to the accessories at the door.

Fig 2b. IP Solution with network switch. AXIS A1001 Network Door controllers are placed at each door with cabling to door accessories.

multiple serial connections wired back to a central server. Cabling work can be even further facilitated. By employing a PoE (Power over Ethernet) supported controller at each door, the need for separate power cables for door equipment such as locks and readers can be eliminated. This reduces the total installation cost. In addition, support for Uninterruptible Power Supply (UPS) makes it possible to avoid having battery back-up for door equipment.

3. Large and more advanced systems

The transition to IP-based solutions will make implementation of access control systems far more attractive. It will also resolve many of limitations of existing traditional systems, and bring additional functionalities that go far beyond conventional door control. Integration with video is one example of a very common requirement which will be much easier to meet with IP-based solutions. In fact, a common, standardized digital environment has the potential to create countless opportunities to integrate other systems such as intrusion detection, fire detection, and so on into uniform, manageable and user-friendly systems.

High security requirements do not make the system less manageable. On the contrary, IP-based access control systems enable remote management, which clearly is an advantage on very large or dispersed sites. This ability also makes it easier and simpler to configure, test and verify a whole new or partly new system, as adjustments can be made from the closest network connection.

Deploying systems – regardless of their size – is therefore quicker and less labor-intensive than installing a corresponding analog system.

The distributed “intelligence” of such a system makes it less vulnerable to power shortages and network failures. Uninterruptible Power Supply (UPS) and local buffering of events in combination with encrypted communication contribute to the highest degree of reliability and security.

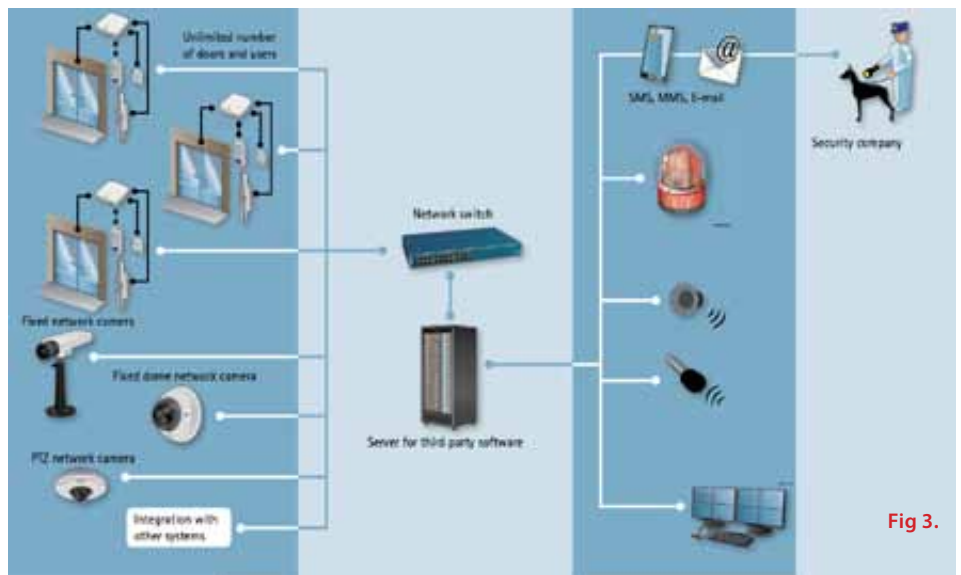


Fig 3. A schematic view of possible integrations between an access control system and a network video surveillance system and other IP-based third party applications. Note that also management functions can be distributed.

4. Benefits of standards

Very much like in the video surveillance market a shift into IP in the access control industry will surely also mean a transition from proprietary systems to open solutions. And these solutions will most likely be based on international industry standards.

Open solutions and standardized interfaces are a prerequisite in any industry that want to establish their own equivalent of “plug-and-play”. There are many gains from such development also in access control. It will allow end users to freely pick and choose between components – reader, door controller and software – that best satisfy their needs and preferences. This freedom of choice makes the system future-proof and means the end user no longer has to rely on a single brand or supplier. Equally important, it can also enable integration with other security related systems and third party applications, without the need for costly hardware boxes to make the “bridge” between the different systems.

In the network security systems market there is already a clear trend to develop open or standardized application platform interfaces (APIs), which can be used by all competing market

participants on fair, reasonable and non-discriminatory terms. Naturally, this will increase supply and promote competition and bring a new level of innovation to the industry, while simultaneously making it even easier for end users, system integrators, consultants, manufacturers and others to take advantage of the different possibilities offered by network solutions.

For example, the Open Network Video Interface Forum (ONVIF), which is a global and open industry standards body with the goal to facilitate the development and use of IP-based security products, announced in 2010 an extension of the organization’s scope of standardization to cover physical access control. Ideally, access control devices from manufacturers that comply with the ONVIF standards will in the near future interoperate effortlessly and seamlessly with each other, as well as with other video surveillance products and systems conformant with the standard.

5. New business opportunities

Making access control systems based on TCP/IP will bring new and exiting business opportunities. Integrators will, for instance, appreciate the easy installation and the possibility to integrate access control with other systems. Distributors will find new markets and new customers when they are free to bundle different components from different manufacturers to create useful and attractive business offers. And end customers, finally, can take advantage of an affordable, yet flexible, future-proof and adaptable technology that can help to secure and protect valuable assets.

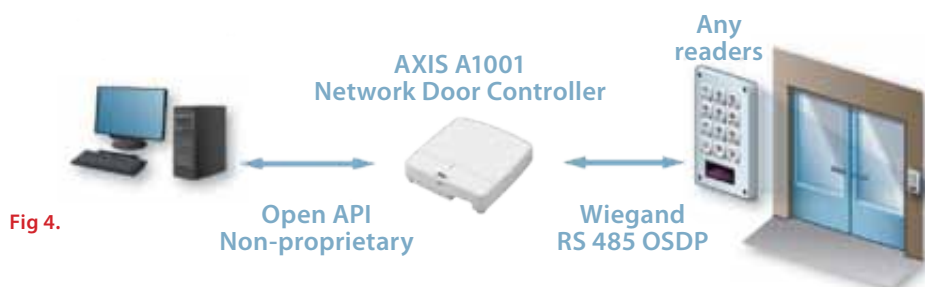


Fig 4. An example of a non-proprietary access control system.

Australia Round-up

ACSC 2016 Conference, Canberra, 12-14 April 2016

Due to the success of the 2015 conference, the Australian Cyber Security Centre (ACSC) conference will be held again in April 2016. The conference provides a key forum for keeping up-to-date with the latest trends, mitigations and advances in cyber security.

The conference will be held 12 – 14 April 2016 at The National Convention Centre, Canberra. More information is available on the conference website acsc2016.com.au. Registrations are now open.

ACSC 2015 Cyber Security Survey: Major Australian Businesses

The results of the first Cyber Security Survey conducted by the Australian Cyber Security Centre (ACSC) to better understand the cyber security posture and attitudes across some of Australia's systems of national interest have come in.

Industry data was collected from major Australian businesses that partner with CERT Australia, the national computer emergency response team. The businesses surveyed, says CERT, “underpin the social and economic welfare of Australia by delivering essential services such as banking and finance, defence industry providers, communications, energy, resources, transport and water.”

The survey results demonstrate that cyber security incidents continue to be commonplace and recurrent. Half the respondents reported experiencing at least one cyber incident that compromised the confidentiality, integrity or availability of a network's data or systems in the last year.

Organisations are being targeted by a broad range of threats – particularly those designed to elicit money. While reported ransomware incidents have drastically increased, most other threat types have remained stable.

50% of respondents have experienced at least one cyber incident in the past year. There has been a significant surge in the number of ransomware incidents with four times the number of respondents reporting in 2015 (72%) as compared to 2013 (17%). Ransomware is the threat of most concern amongst respondents (72%),

followed by theft or breach of confidential information (70%) and Advanced Persistent Threats (66%).

IT security awareness and practices of general staff appear to have improved since 2013. However, many cyber threats now feature well-crafted socially-engineered emails that make it difficult for the user to determine legitimacy, regardless of training.

77% of respondents have cyber security incident response plans in place with 37% of these regularly reviewing it. 56% of respondents increased expenditure on cyber security in the last 12 months – a significant increase from 2013, when only 27% of respondents reported an increase.

100% of respondents reported using anti-virus software and all but one respondent reported using network based firewalls. 82% of industry organisations use external IT security standards or frameworks.

The findings also demonstrate that industry organisations are yet to be convinced of the benefits of reporting incidents. 43% of respondents chose not to report incidents as there was no perceived benefit to them.

ASQA Report: Training in security programs in Australia

The Australian Skills Quality Authority published the findings of its national strategic review of training for the security industry on 28 January.

ASQA Chief Commissioner Chris Robinson stated that poor quality training and assessment and inconsistent licensing arrangements between states and territories were posing fundamental challenges to equipping licensed security personnel to safely do their jobs.

“A key driver of ASQA's review was concerns raised in successive reports by Coroners investigating the deaths of patrons during or as a result of restraint or intervention by security personnel in the course of incident control, particularly around licensed premises,” he said.

“ASQA's national strategic review has confirmed many of the issues raised by Coroners, and by other stakeholders in the vocational education and training (VET) sector.”

Mr Robinson said that although qualifications for security roles are national, the regulation of security licensing is state and territory-based, making it difficult to ensure consistency between qualifications and licensing requirements.

“Until the inconsistent licensing arrangements are fixed, people will continue to cross borders to attain licenses in jurisdictions with fewer requirements.”

Interstate security licensing loophole uncovered by ABC investigation

Given the above report, it is no surprise that, according to the ABC's 7:30 Report, up to 300 security guards per month in NSW are gaining their security license by apparently exploiting a loophole which fails to check an applicant's citizenship or English language ability.

A legal loophole allows applicants to qualify in Queensland and then transfer to the stricter jurisdictions of NSW or Victoria. Queensland allows people on holiday visas to become security guards.

The 09 March 7:30 Report piece found evidence “suggesting one NSW security license broker sold accreditation tests, with answers, to people who had not undergone any study or training.”

“The legal loophole, known as “license shopping”, exploits shortcomings in Queensland's industry regulations, which allow students to qualify for their security license then transfer to stricter jurisdictions, such as NSW or Victoria.”

The 7.30 Report investigation identified a Sydney security firm that has been selling Queensland tests and answers. It also found that just 48 percent of the NSW's security guard applicants are receiving the proper training and scrutiny.

AFP Operations Centre unveiled at Gold Coast Airport

According to a 04 March media release, the Australian Federal Police (AFP) has officially open its new Aviation Operations Centre at Gold Coast Airport. The opening marks the completion of

fourteen of seventeen new AFP aviation facilities to be opened across Australia's major airports.

The facility includes an Emergency Operations Centre, Airport Police Operations Centre, muster rooms and training facilities, exhibit handling facilities and interview rooms. AFP Assistant Commissioner David Sharpe said the enhanced facilities will consolidate the AFP's position as the primary law enforcement agency at Gold Coast airport.

"This new facility will allow the AFP to provide a more effective and visible policing service to Gold Coast Airport, and will help us continue to deliver world-class aviation policing services."

The AFP takes a whole-of-government approach to aviation security, working in collaboration with partner agencies such as the Department of Infrastructure and Transport, Australian Border Force, state and territory police and other key Airport industry stakeholders.

Next Generation of Banknotes: Plans for the \$5 design reveal

The Reserve Bank of Australia announced on 11 February that the new \$5 banknote would be issued from 1 September 2016. A core function of the RBA is to issue secure banknotes.

Australia has one of the safest and most secure currencies in the world. It has experienced relatively low levels of counterfeiting for many years. To ensure that this remains the case, the Bank continually researches new anti-counterfeit technologies and developments in banknote design. In recent years, the Bank has also put in place a program to upgrade the security of the country's banknotes.

The upgraded banknotes will incorporate a number of new security features. They will retain many of the key design elements of the current banknote series, such as the colour, size and portraits, but some design changes will be necessary to accommodate the new security features.

Considerable work has already been undertaken on this project, including the development and review of banknote designs and production trials of new security features. The new features are rigorously tested, and the RBA has also consulted extensively with relevant stakeholders to ensure that the banknotes continue to meet community needs.

The Bank intends to publish images of the new \$5 banknote on 12 April. The reveal of the \$5 banknote designs will be followed later in the year by a public awareness campaign to ensure the public are able to identify and use the range of new security features on the new banknotes when they are issued from 01 September.

Bra inserts lead to major bust: \$1 billion of 'ice'

According to a 15 February 2016 Australian Border Force, Australian Crime Commission, Australian Federal Police, NSW Police Force joint media release, four people have been charged by the Joint Organised Crime Group (JOCG) for their alleged involvement in the importation and manufacture of 720 litres of methylamphetamine with an estimated potential street value of more than one billion dollars.

On 8 November 2015 the JOCG established Operation OVCHARKA to investigate potential drug importation and supply from Asia, destined for the Australian market.

Between 23 and 30 December 2015 the JOCG executed four search warrants at storage facilities in Hurstville, Rockdale, Miranda and Padstow, locating around 530 litres of ice concealed in art supplies.

On 26 December 2015, ABF officers discovered 190 litres of ice concealed inside thousands of silicon bra inserts amongst an 86 box consignment from Hong Kong. On 14 January, the JOCG conducted a controlled delivery of the bra insert consignment to a storage facility in Burwood, where a 33-year-old Hong Kong national was arrested. He was charged with importing a border controlled drug.

On 25 January 2016, the JOCG uncovered evidence of drug manufacturing at two Sydney residences in Hurstville and Campsie, alleged to be linked to the ice seized in the art supplies in December. A 59-year-old male Chinese national, a 37-year-old male and a 52-year-old female Hong Kong national were arrested and charged with knowingly taking part in the manufacture of a commercial quantity of a prohibited drug.

Security guard brutally kicked in head: teenager charged

The family of a teenager accused of kicking a security guard in the head at a Perth music festival in February has lashed out at media and supporters of her son's alleged victim following his court appearance on 17 March.

18-year-old Martin Fulton is accused of kicking security guard Michael Rigby as he wrestled with an alleged fence jumper at the Good Life festival in the early evening of 29 February. Mr Fulton was charged with assault occasioning bodily harm and trespass after a disturbing video of the kicking incident was posted to Facebook.

The video features the security guard and a young man wrestling on the grass. Shortly thereafter, another teenager dressed in a white shirt approaches and kicks the man in the face. A crowd of bystanders gasp immediately in horror.

The security guard appears knocked out by the brutal kick, his body is slumped forward into the ground. The first teenager breaks free from the guard's hold and punches him then flees the scene.

The footage sparked a tirade of responses on social media in support of the guard and decrying the brutality of the incident.





Wireless IP Surveillance

- Cost effective high performance wireless access points for outdoor use
- Stockists of AirMax, AirFiber, AirVision, UniFi & mFi series products
- ITPLUS are a Ubiquiti certified and trained partner

Distributed by



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



Customized CCTV Kits

- We supply fully customized complete CCTV kits in form of Hybrid, Tribrid, IP, CVI etc
- Complete kits are a great way of reducing costs and getting the whole package from one place
- Receive FREE support* including remote connection assistance

Distributed by



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



Open Platform VMS

- Award winning best open platform VMS
- Advanced Built-in Video Analytics
- Micromodule crashproof software architecture
- Includes powerful features such as Modern GUI, Video Archive, Green Stream, Time Compressor, Interactive 3D Map, Autozoom etc.

Distributed by



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



ITRON SECURITY & AUTOMATION



Power supply cabinets

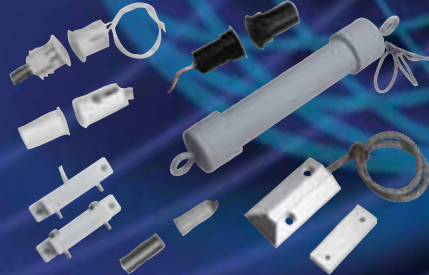
- Mounts for our 5 most popular models of power supplies; 6 key-hole anchor points for easier mounting
- Lift off hinged doors for added convenience
- Louvre ventilation on doors
- Roller ball reed switch provides anti-tamper to front and rear of cabinet
- 6 x 25mm knockouts, 2 each sides and bottom
- 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



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



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



Uniview IPC542E-DUG Starlight Camera

- 2.0 megapixel 1920x1080 @ 30 fps.
- HD starlight surveillance
- Day/night functionality
- Up to 120 dB Optical WDR
- 3D DNR (Digital Noise Reduction)
- H.264 High Profile, Triple streams
- ONVIF Conformance
- IP66
- Wide range of lenses available

iPhone, Android and Windows compatible.



Uniview IPC3234SR-DV 4 Megapixel Camera

- 4.0 megapixel 2592x1520 @ 20 fps.
- Day/night functionality
- Smart IR, up to 30m (98 ft) IR distance
- Up to 120 dB Optical WDR
- 3D DNR (Digital Noise Reduction)
- H.264 High Profile, Triple streams
- ONVIF Conformance
- IP66

iPhone, Android and Windows compatible.



Uniview 4 channel IP Kit

Uniview's easy to install and easy to use, this is a high-spec surveillance solution perfect for homes and businesses.

- 4 x 2MP IP66 IR Dome Cameras
- 1 x 8 Channel 201 series NVR*
- 4 x 18m cat5 cable
- 1 x HDMI Cable Included

iPhone, Android and Windows compatible.



Panasonic



(09) 414 5101 OR 0800 ITRONICS

SALES@ITRON.CO.NZ

WWW.ITRON.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 Securitron 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

20238_PDM

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 \$75.00 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

Cybersecurity perspectives from KPMG & PwC get airplay

In content featured on the NZ Herald website on 12 February, KPMG cyber security expert Philip Whitmore claims that the public sector is now leading the way in New Zealand cyber security - and private sector companies could learn some lessons.

According to the article, cyber security has been a major government focus in recent years in the wake of increasing cyber-attacks globally, national and international ramifications from a spate of incidents and a major review of security in the public sector. Government agencies will report for the first time next month on new Protective Security Requirements (PSR).

Whitmore says "New Zealand and the public sector was still a bit naïve then about how effective security was." Those incidents and subsequent review led to public service organisations having a stronger focus on security, including having senior people with clear security responsibilities.

"A lot of the tools the public sector has developed to support it becoming more robust have been made available to the private sector. I'd suggest the private sector should take the opportunity to pick up some of those tools and see how beneficial they are to their own organisations."

The importance of security, continues the article, extends beyond New Zealand's borders. "If New Zealand government systems aren't secure, it may impact our ability to interact on a global basis", states Whitmore. He sees the release of the Government's Cyber Security Strategy at the end of last year as demonstrating the government's commitment to ensuring New Zealand is secure and prosperous online.

In a media release two weeks later, Communications Minister Amy Adams asserts that the 2016 Global Economic Crime Survey from PwC underlines that the issue of cyber security belongs in the boardroom, not in companies' IT departments.

The PwC survey found that 40 per cent of New Zealand organisations have experienced cybercrime over the past two years, but only 45 per cent of all organisations have a cyber incident response plan. The report places New Zealand 19th out of 115 countries.

"The Global Economic Crime Survey is a welcome and valuable report for New Zealand businesses looking to better understand the range of threats in today's modern operating environment," Ms Adams says.

"The report is a sobering read and a call to action for chairs and chief executives to focus on managing the growing cyber security risk to their businesses.

"It's important that companies create strong security cultures with actively engaged boards, because ultimately this isn't an issue that directors can ignore."

Ms Adams said with 29 per cent of companies reporting a cybercrime incident, it's vital that New Zealand businesses understand what data they hold and create.

"Boardrooms around the country need to consider cyber vulnerabilities as a key business risk and address this as part of management processes."

In December, Ms Adams launched the refreshed New Zealand Cyber Security Strategy. It highlights the need for the corporate sector, including operators of critical national infrastructure, to have policies and procedures in place to mitigate cyber security threats.

"The Institute of Director's Practice Guide for Directors is an excellent resource for Board members to ensure they have a good sense of their responsibilities and cyber security best practice," Ms Adams says.

"New Zealand's first ever Cyber Security Summit in Auckland on 5 May will bring together leading business and government leaders and provide an opportunity for to demonstrate their collective commitment to cyber security."

FROM OUT OF THE BOX TO STATE OF THE ART. ID CARD PRINTING INNOVATION.

HID Global is leading the industry with the most robust portfolio of secure ID issuance solutions in the world. Our FARGO[®] line of printers and encoders provide governments, financial institutions and businesses of all sizes fast, efficient and reliable solutions that are as secure as they are affordable.

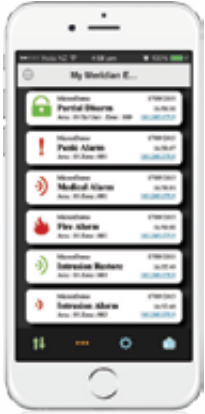
You'll call it innovation on demand. We call it, *"your security connected."*

YOUR SECURITY. **CONNECTED** | Visit us at hidglobal.com

The Market Leader in Security Innovation

EC-11 IP Capture Module

EC-11 Features



- Upgrade **any** CID reporting alarm to TCP/IP.
- Two inputs and two outputs.
- New **Micron Control App** for controlling **any alarm**.
- In-App, real-time event reporting for any brand of alarm panel.
- Real-time push notifications and email event reporting.
- Secure, in-App, installer programming connectivity **any place, any time!**
- PSTN/ATA pass thru for voice and up/download of any alarm brand.
- Multiple backup communication pathways (Ethernet, 3G, PSTN)

MINI WIFI 3G ROUTER

Provides a WiFi bridge to a router or 3G IP alarm communications on any mobile network.



New Micron Control App

- Download free for EC-11 control of arming, disarming and control of **any brand** of connected alarm panel.
- Register for alarm event push notifications to selected smartphones and access micron's real-time, cloud based event reporting log , **anyplace, anytime!**
- View the event logs for all registered EC-11 and Meridian customers within the App and connect to EC-11 and Meridian programming.
- EC-11 and Meridian dynamically update any change to their connected router's IP address in their real-time event log.
- Touch the IP address in the event log, enter the device username and password and connect.

\$109.00+GST
\$199.00+GST with 3G Router



Available on
 iTunes Google play

Designed & manufactured in New Zealand for 40 years.
Exported to more than 40 countries worldwide.

Micron Security Products Ltd, 13A Sultan Street, Ellerslie, Auckland
PO Box 11-339, Ellerslie, Auckland 1542, New Zealand
Ph: 64 9 378 6098 Fax: 64 9 378 6454 info@micronsecurity.com www.micronsecurity.com

