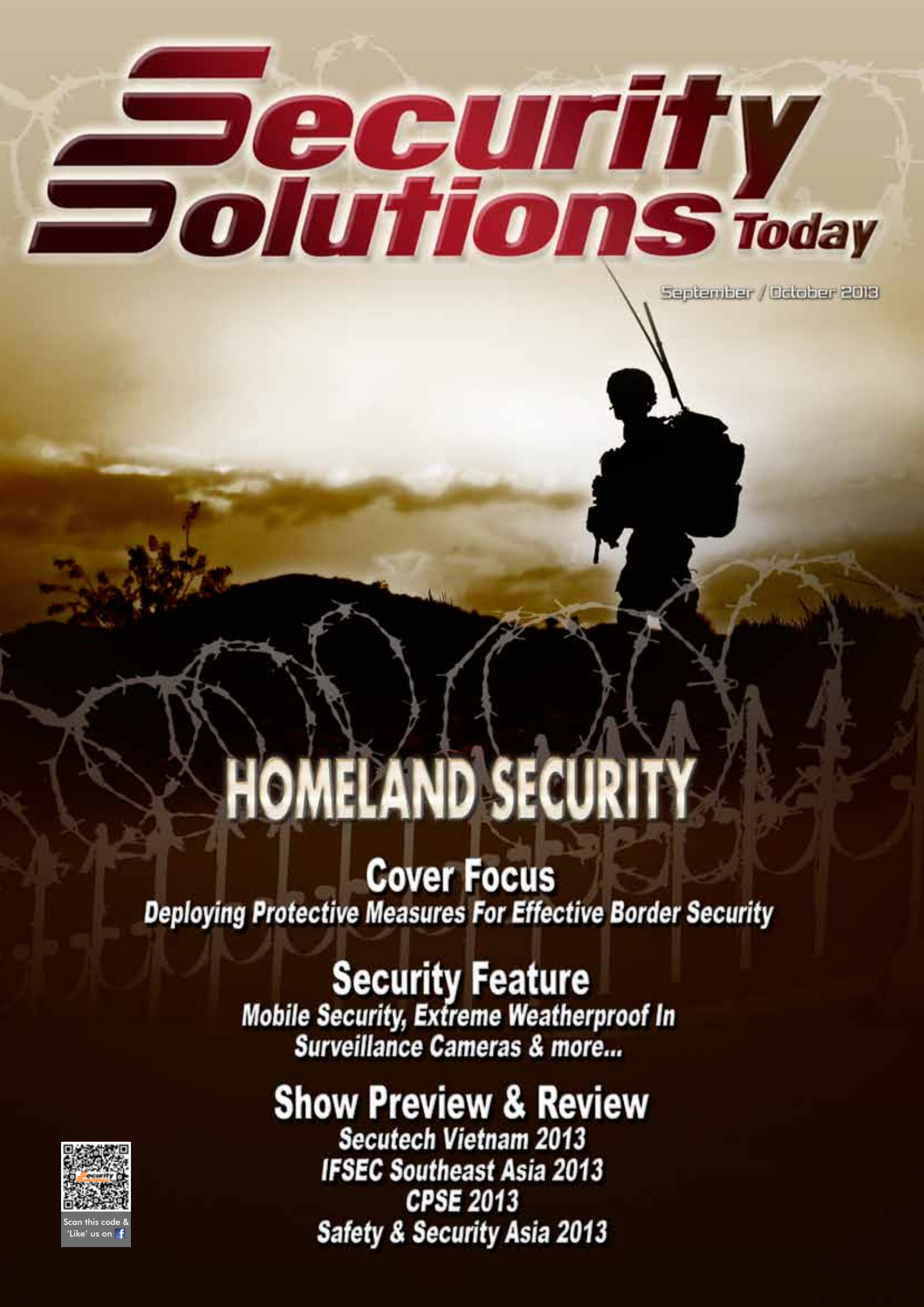
Security Solutions Today

September / October 2013



HOMELAND SECURITY

Cover Focus
Deploying Protective Measures For Effective Border Security

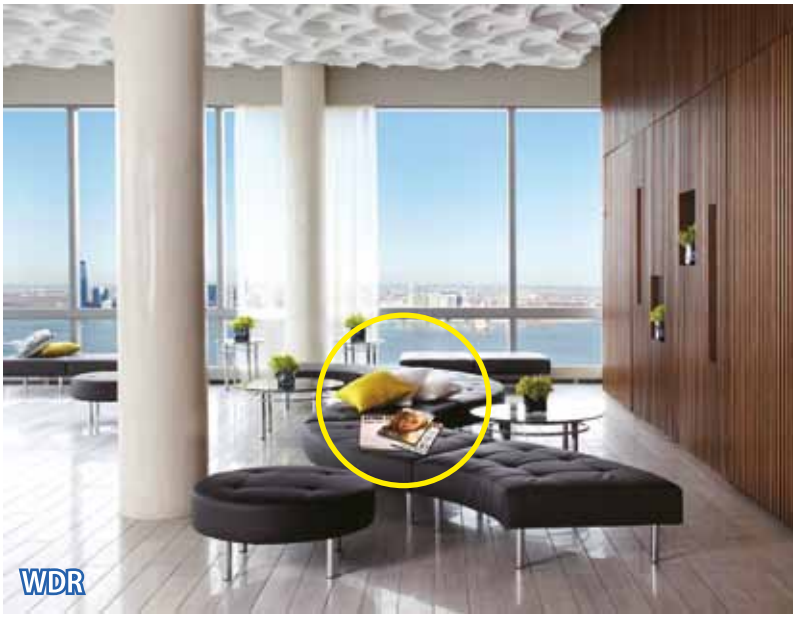
Security Feature
Mobile Security, Extreme Weatherproof In Surveillance Cameras & more...

Show Preview & Review
Secutech Vietnam 2013
IFSEC Southeast Asia 2013
CPSE 2013
Safety & Security Asia 2013

Scan this code & 'Like' us on

WDR

Dahua 1.3MP HD WDR Network Cameras



Features

- 1/3" 1.3Mp Aptina CMOS
- H.264/MJPEG & dual-stream encoding
- Max 25/30fps@1.3M(1280×960)/720p
- Lens: 2.8-12mm (Dome & Bullet)
- 128dB WDR, D&N(ICR), Auto Iris, Micro SD card
- DC12V(AC24V optional), PoE
- Wi-Fi (Box), IP66(Dome & Bullet)

IPC-HDB3101 / HDBW3101

IPC-HF3101

IPC-HFW3101C

Dahua Technology also launched Vari-focal Motorized Lens Network Cameras, please go to www.dahuasecurity.com for the detail.

CE FC UL RoHS ISO 9001:2000

IFSEC Southeast Asia
COMMERCIAL SECURITY · FIRE · SAFETY
11–13 Sep 2013 Kuala Lumpur, Malaysia
Booth: D109

DAHUA TECHNOLOGY CO., LTD.
No.1187 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

www.dahuasecurity.com

THE ALL NEW MicroDome™

- Ultra Low Profile Design
- True Day/Night with Mechanical IR Cut Filter
- All-in-One PoE and Integrated Lens
- Integrated Microphone
- Pixel Binning Mode on 3 and 5MP Models
- Wide Dynamic Range Available on Some 1080p and 3MP Models
- Dual Encoder H.264/MJPEG
- Casino Mode™ Maintains at Least 30fps on Some 1080p Models

World's Smallest All-in-One H.264 Day/Night 1.3–5 Megapixel and WDR Dome IP Cameras.

Arecont Vision introduces MicroDome™ megapixel IP cameras. These small, ultra low profile cameras offer the great features of Arecont Vision megapixel technology like superior image quality, excellent compression and fast frame rates. An innovative spring arm design makes installation a snap: simply slide the camera through the hole and secure the magnetized cover ring with a single screw. Every model comes equipped with a mechanical day/night switcher, and pixel binning on 3- and 5-megapixel models deliver excellent low-light capabilities. Add optional true Wide Dynamic Range and difficult lighting conditions are overcome with MicroDome™. Sometimes smaller is indeed better!

Dome

SCHEDULE A DEMO AT YOUR LOCATION!

+1.818.937.0700 | 877.CAMERA.8 | avsales@arecontvision.com

Made in the USA

Arecont Vision

10 Years 2003 - 2013

www.arecontvision.com

Celebrating 10 Years of Leading the Way in Megapixel Video

CONTENTS

September - October 2013

Make sure the bad doesn't happen so the good can. Anywhere. Anytime.

When you're responsible for the safety, security and everyday function of a big city, you have your hands full making sure the bad doesn't happen so the good can. At Axis, our deep experience in city surveillance gives us invaluable insight into the complexity of what you're facing every minute of every day.

That's why you can rely on Axis city surveillance solutions for dependable, crystal-clear HDTV video in real time anywhere you need it.

It's easy to coordinate your whole surveillance system centrally – and even share live video. Plus, as the world leader in network video, rest assured Axis brings you a future-proof solution that's ready for today's smart technology as well as tomorrow's.

Axis city surveillance solutions – securing everyday life.

Get the Axis picture. Stay one step ahead.
Visit www.axis.com/citysurveillance or email contact-sap@axis.com for more information.

HDTV quality • Excellent zooming capabilities • Rugged outdoor cameras • Vandal-resistant • Sharable live video • Future-proof

AXIS COMMUNICATIONS

Bosch Introduces Integration Partner Program
- Simplifies Interoperability of Video Products

Bosch Security Systems, Inc. is moving to a whole new level of interoperability with the launch of its Integration Partner Program. The program provides partners with powerful development tools and dedicated resources to ensure support of Bosch video products within third-party solutions. A new web portal and solution advisor also helps integrators identify the compatible software and products that are right for their video projects. The result is greater flexibility for end users to utilize Bosch IP video devices with the software and storage platforms that best address their security surveillance needs.

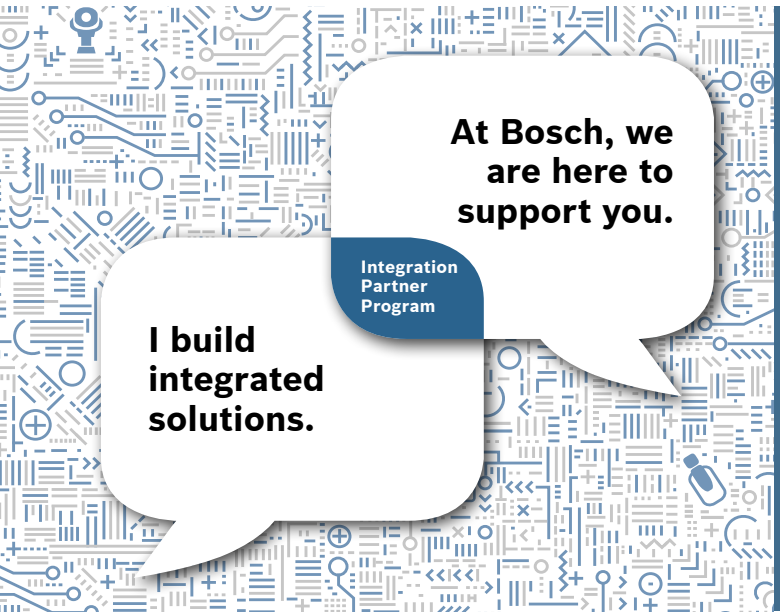
"The security market is extremely diverse, and we are making it easy for customers to leverage Bosch's unique video products and features using their preferred software and storage platforms," said Rudolf Spielberger, Head of the Integration Partner Program at Bosch Security Systems. "We're providing an excellent resource in enabling and supporting the integration of our products into comprehensive solutions that meet the specific requirements of the end user."

As part of the program, developers gain a comprehensive library of reusable software components and sample code to facilitate faster integration of Bosch IP devices into their applications. Bosch engineers also help optimize support of video product features for more complex projects.

For integrators, immediate access to the latest information on the compatibility of Bosch devices with other video management systems or storage products makes it easier to design best-of-breed solutions. For end users, stringent testing of all third-party solutions listed in the web portal ensures seamless integration of Bosch IP devices and simple operation.

"Bosch IP Imaging devices are packed full of intelligent technologies such as Intelligent Video Analytics (IVA) and Content Based Imaging Technology (CBIT) that adds significant value even when used in tandem with third-party video and security management systems." said Adrian Tan, Integration Manager, Singapore, Bosch Security Systems. "Regardless of your industry and application, you will find many opportunities and avenues to see a live demonstration of how this all comes together. Our products are readily found in our partner's booths at various exhibitions including Milestone MPOP and EMC security Week in the Asia Pacific region. In addition, permanent demo showcases in selected countries are also setup at dedicated partner facilities such as EMC, Dell, Axxonsoft and more."

Bosch solutions are designed to be integration-friendly. All Bosch IP cameras and encoders are ONVIF conformant and run one firmware, allowing partners to support dozens of products at the same time. And now, with the new Integration Partner Program, Bosch is presenting its technology in an even more transparent way. Learn more about the Integration Partner Program at http://ipp.boschsecurity.com/



"The security market is extremely diverse, and we are making it easy for customers to leverage Bosch's unique video products and features using their preferred software and storage platforms."

Rudolf Spielberger
Head of the Integration Partner Program
Bosch Security Systems

We need compatible video products to create the best solutions for our customers.

Integration Partner Program

At Bosch, we integrate with even more video management software and storage providers.

New **integration** possibilities

Check out our Integration Partner Program. Working with industry partners allows us to deliver you new possibilities. Get access to Bosch Security Systems products and integrate into your preferred video management software or storage providers. Leverage unique features like Intelligent Video Analytics, Dynamic Transcoding and more. See for yourself how everything just works.

ipp.boschsecurity.com

BOSCH

Invented for life

CONTACTS

September - October 2013

Publisher
Steven Ooi (steven.ooi@tradelinkmedia.com.sg)

Editor
Sharon Kaur (sst@tradelinkmedia.com.sg)

Group Marketing Manager
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

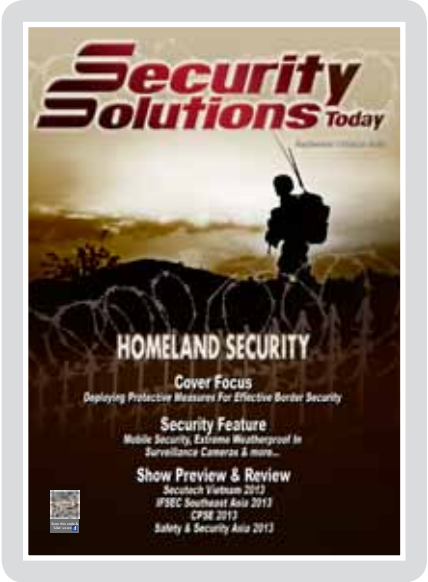
Marketing Manager
Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

Marketing Executive
Catherine Koay (catherine.koay@tradelinkmedia.com.sg)

Head Of Graphic Dept/ Advertisement Co-ordinator
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

Graphic Designer
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

Circulation
Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)



Designed by Fawzeeah Yamin

Printed in Singapore by KHL Printing Co Pte Ltd.

Security Solutions Today
is published bi-monthly by
Trade Link Media Pte Ltd
(RCB Registration No: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399.
Tel: 65-68422580
Fax: 65-68422581

The magazine is available free-of-charge to applicants in the security industry who meet the publication's terms of control. For applicants who do not qualify for free subscription, copies will be made available, subject to the acceptance by the publisher, of a subscription fee which varies according to the country of residence of the potential subscriber in the manner shown on the right.

The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

ANNUAL SUBSCRIPTION:

Surface Mail:
Singapore - S$40 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:
Malaysia/Brunei - S$80
Asia - S$120
Japan, Australia, New Zealand - S$150
America/Europe - S$150
Middle East - S$150

ADVERTISING SALES OFFICES

Head Office: Trade Link Media Pte Ltd.
(RCB Reg. No: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399.
Tel: 65-68422580; Fax: 65-68421523, 68468843, 68422581.
Email (Mktg): info@tradelinkmedia.com.sg

India:
Mr. Avneet Singh
Mark Excellence Business Management
C317 / 8 Inlaks Nagar, C.H.S. 15 Yari Road
Versova, Andheri (West)
Mumbai
India
Tel: +91-22 325 81 747
Fax: +91-22 263 96 204
avneet@markexcellence.com

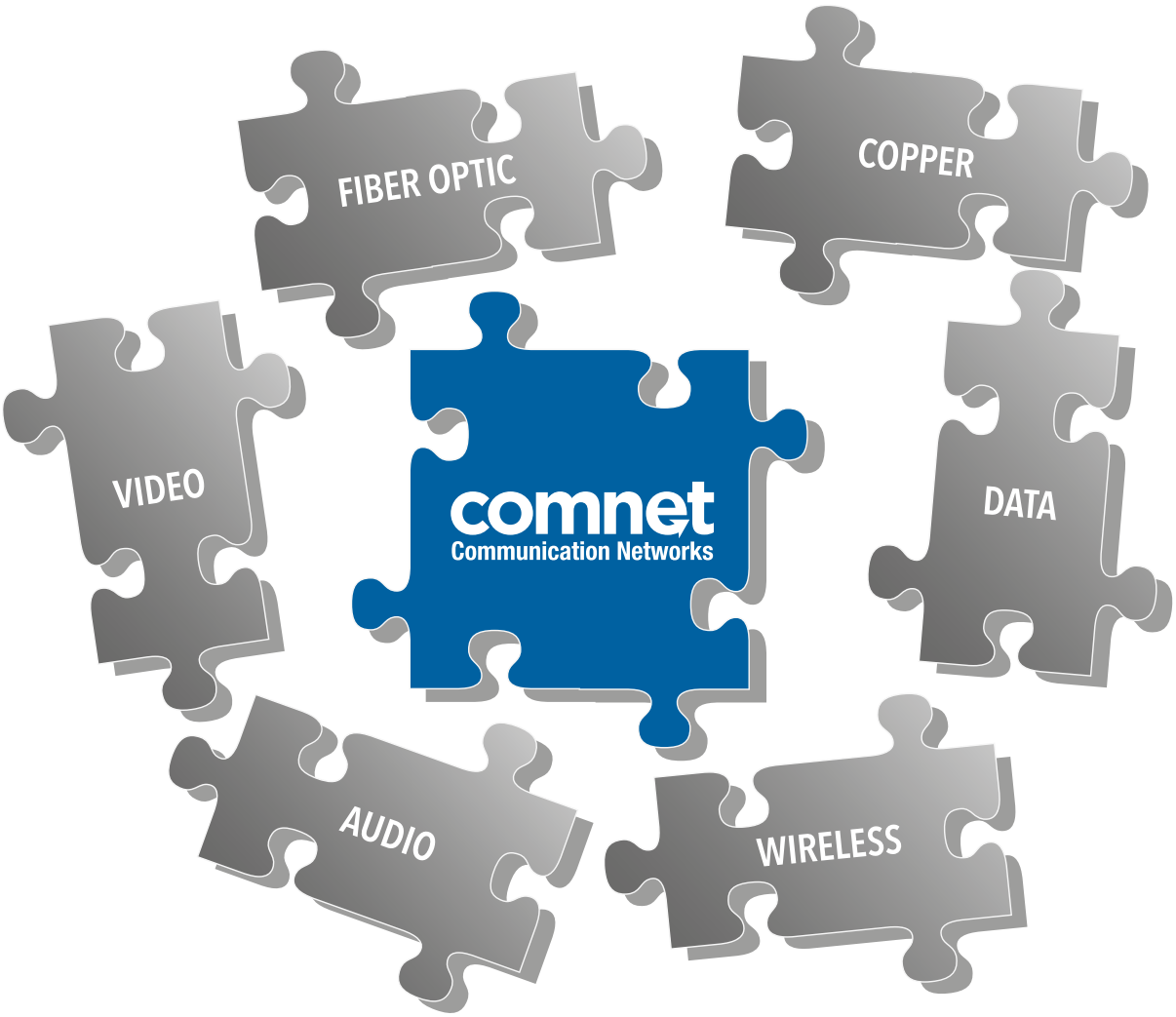
Korea:
MCI
Rm. 103-1011,
Brown Stone, 1330,
Baeseok-dong, Goyang-si,
Gyunggi-do,
Korea 410-907
Tel: +82 2 730 1234
Fax: +82 2 732 8899

Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: 81-3-32635065
Fax: 81-3-32342064

Italy/Switzerland:
Arch. Aldo Cacchioli
Publistein di
Galli-Cacchioli & Co.,
Via Borghese 11
CH-6600 Locarno
Switzerland
Tel: 41-91-7516910
Fax: 41-91-7517109
info@publistein.com

THE SINGLE-SOURCE SOLUTION FOR ALL YOUR TRANSMISSION PRODUCTS

Only One Company Can Put All The Pieces Together



No Matter What You Need to Transmit, ComNet has Your Solution with the Industry's **Most Complete Line** of Transmission Equipment

Fiber Optic, Wireless or COAX/UTP

› **Fiber Optic Audio, Video & Data**

› **Fiber Optic Ethernet**
Managed Ethernet Switches and Media Converters with or without PoE+

› **CopperLine® Extenders**
Ethernet over UTP/COAX Distance Extenders

› **NetWave™ Wireless Ethernet**
Point-to-Point and Point-to-Multipoint

comnet
Communication Networks

See us at IFSEC South East Asia
Malaysia | September 11 – 13 | Hall 5/Stand K506

www.comnet.net

sales-asia@comnet.net

+44 (0)113 307 6400

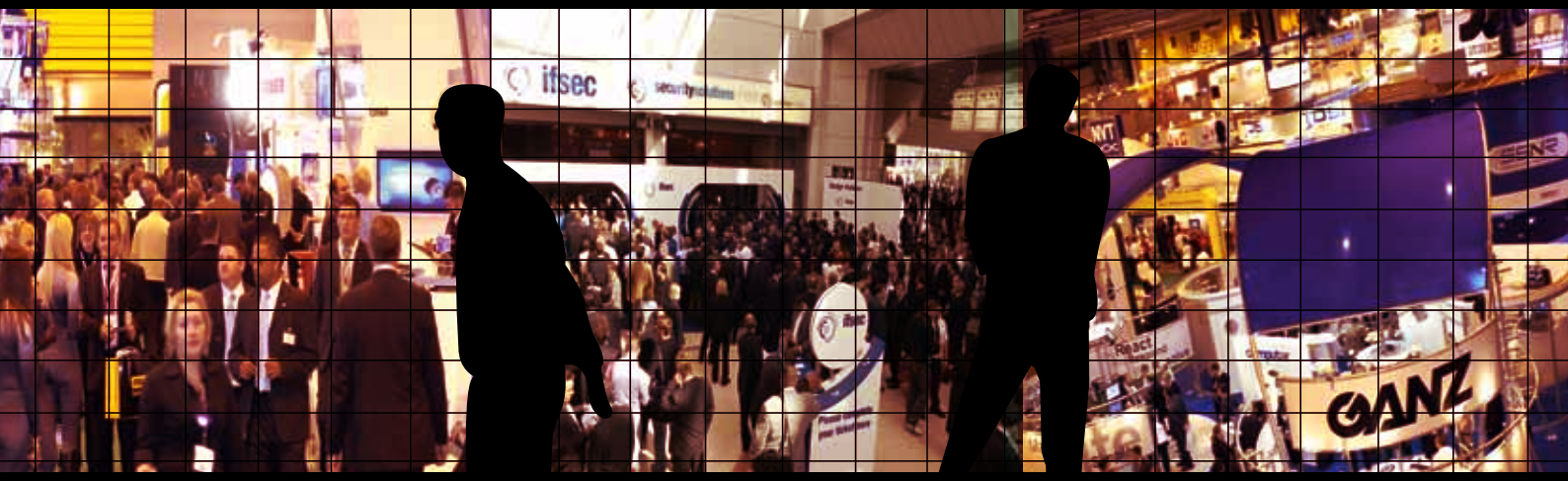
› Free Design Center Application Support

› Pre & Post Sale Technical Support – USA Based

MADE IN THE USA

LIFETIME WARRANTY

Calendar Of Events



Secutech Vietnam 2013

Date: 8 – 10 August 2013
Venue: Saigon Exhibition & Convention Centre (SECC), Ho Chi Minh City, Vietnam
Contact: Sandra Chen
Organiser: Messe Frankfurt New Era Business Media Ltd
Tel: +886 2 2659 9080 ext. 761
Email: stvn@newera.messefrankfurt.com
Website: www.secutechvietnam.com

CAMSECURITY & FIRE 2013

Date: 10 – 12 September 2013
Venue: Diamond Island Exhibition & Convention Centre (DIECC), Phnom Penh, Cambodia
Contact: Richard Yew
Organiser: AMB Events Sdn Bhd
Tel: +6 03 4041 9889
Email: richard@ambexpo.com
Website: www.expocambodia.com/camsecurity13/

IFSEC Southeast Asia 2013

Date: 11 – 13 September 2013
Venue: Kuala Lumpur Convention Centre, Malaysia
Contact: Rina Fadzil
Organiser: UBM
Tel: +6 03 2176 8788
Email: Rina.Fadzil@ubm.com
Website: www.ifsecsea.com

BMAM Expo Asia 2013

Date: 19 – 21 September 2013
Venue: Hall 5 – 6, IMPACT Exhibition Center, Bangkok, Thailand
Contact: Ajinveat Vhongthong
Organiser: UBM
Tel: +66 0 2833 5210
Email: ajinveatv@impact.co.th
Website: www.maintenance-asia.com

CPSE 2013

Date: 29 October – 1 November 2013
Venue: Shenzhen Convention & Exhibition Center, P.R. China
Contact: Cindy Chen
Organiser: Shenzhen CPSE Exhibition Co., Ltd
Tel: +86 755 88309126 | 88309123
Email: cindy.chen@cps.com.cn
Website: www.cpse.com.cn

Intersec 2014

Date: 19 – 21 January 2014
Venue: Dubai International Convention and Exhibition Centre, Dubai
Contact: Andreas Rex
Organiser: EPOC Messe Frankfurt GmbH
Tel: +971 4 389 4500
Email: andreas.rex@uae.messefrankfurt.com
Website: www.intersecexpo.com

Secutech Taiwan 2014

Date: 19 – 21 March 2014
Venue: Nangang Exhibition Center, Taipei Taiwan
Contact: Echo Lin
Organiser: Messe Frankfurt New Era Business Media Ltd.
Tel: +886 2 2659 9080 ext. 761
Email: Echo.lin@newera.messefrankfurt.com
Website: http://www.secutech.com

Safety & Security Asia 2014

Date: 28 – 30 April 2014
Venue: Marina Bay Sands, Singapore
Contact: Chloe Tan
Organiser: Conference & Exhibition Management Services Pte Ltd (CEMS)
Tel: +65 6278 8666
Email: chloe@cems.com.sg
Website: http://www.safetysecurityasia.com.sg

Panasonic

Clearer Visibility Even in Rain

Superior performance against rain and dirt with rain-wash coating

Rain-wash-coated PTZ Dome Camera Lineup (weather-resistant type)

Network Cameras | Analog Camera

WV-SW598 NEW
- 1080p HD images up to 30 fps
- 360 degree endless Panning
- Advanced Auto Tracking
- Ambient Operating Temperature –50 °C ~ +55 °C

WV-SW396A NEW
- 720p HD images up to 30 fps
- 360 degree endless Panning
- Advanced Auto Tracking
- Ambient Operating Temperature –50 °C ~ +55 °C

WV-SW395A NEW
- 720p HD images up to 30 fps
- Panning with auto flip function
- Auto tracking
- Ambient Operating Temperature –40 °C ~ +50 °C

WV-CW590A/WV-CW594A NEW
- High resolution: 650 TV lines
- High sensitivity with Day/Night function
- Auto tracking
- Ambient Operating Temperature –50 °C ~ +55 °C

i-PRO SmartHD | MEGA Super Dynamic | RAIN WASH COATING | NO LUBRICATION | 24/7 IR removable | IP66 standard | ONVIF

SD6 Super Dynamic | RAIN WASH COATING | 24/7 IR removable | IP66 standard

Effects of rain-wash coating

Fewer rain droplets

Less dirtying

Droplet formation prevention	Visibility can be ensured even in rain due to droplet prevention effect.
Reducing dirtying	Dirt is easily washed off dome cover by rain water due to self-cleaning effect.
Advanced coating technology	Long-term effect is maintained due to advanced coating technology.

http://security.panasonic.com http://www.facebook.com/PanasonicNetworkCamera

Panasonic Systems Asia Pacific
2 Jalan Kilang Barat, Panasonic Building Level 7, Singapore 159346 Tel: +65 6270 0110 Fax: +65 6276 0330 E-mail: biz.prod@sg.panasonic.com

Editor's Note

Dear Readers,

Welcome to this year's September/October issue of Security Solutions Today!

Let me start by introducing myself. My name is Sharon, the new Editor for SST.

There are a number of things that you can look forward to in this issue of SST, which is themed 'Homeland Security'.

We have included a wide array of case studies to bring to light the growing importance of implementing proper protective measures for homeland security (pg. 30). Our cover story discusses 'Deploying Protective Measures For Effective Border Security' and is written by Joshua Kwai, a regular article contributor for this magazine (pg. 20).

This issue also contains our usual product showcase section (pg. 79) where we feature a large variety of products for your reading pleasure. We have also included four informative Security Feature articles that will keep you up to date on the latest trends in the Security Industry.

Do also keep an eye out for our 'Show Preview' and 'Show Review' Section where we cover shows such as Secutech Vietnam 2013 (pg. 92), IFSEC Southeast Asia 2013 (pg. 94), CPSE 2013 (pg. 96), and Safety & Security Asia 2013 (pg. 98).

In our 'Pundit Perspective' section (pg. 24), you can expect insightful perspectives from high-ranking security experts about why it has become increasingly important to implement protective measures for effective border security.

Have a great read!

Sharon Kaur
Editor

No more trash talk

Full coverage in just 2 lenses.

The Double Vari-Focal solution. Cover all focal lengths from wide to tele with 3-Mega-Pixel resolution using just 2 lenses.

The new IR-corrected Mega-Pixel lens series from Tamron features a focal length range of 2.8 to 50mm in just two lenses covering 126.1° to 6.8°horizontal field of view with use of a 1/2.7" camera. A new optical design uses glass mold aspherical lens elements and a special optical coating that ensures 3MP high resolution even under IR light and a clear image.

The simple choice for better security imaging. Tamron's Double Vari-Focal solution.

DOUBLE VARI-FOCAL
The Simple Choice

Model:M13VG288IR
1/2.7" 2.8-8mm F/1.2

Model:M13VG850IR
1/2.7" 8-50mm F/1.6

Tamron Industries (Hong Kong) Ltd
Unit 927, 9/F , KITEC, 1 Trademart Drive , Kowloon Bay , Hong Kong
Tel. : (852)2620 9033 Fax:(852)2620 1631
email:cctv@tamron.com.hk http://cctv.tamron.com.hk

TAMRON
New eyes for industry

Bosch Security Systems Launches Integration Partner Program

Bosch Security Systems is moving to a whole new level of interoperability with the launch of its Integration Partner Program. The program provides partners with powerful development tools and dedicated resources to ensure support of Bosch video products within third-party solutions. A new web portal and solution advisor also helps integrators identify the compatible software and products that are right for their video projects. The result is greater flexibility for end-users to utilise Bosch IP video devices with the software and storage platforms that best address their security surveillance needs.

"The security market is extremely diverse, and we are making it easy for customers to leverage Bosch's unique video products and features using their preferred software and storage platforms," said Rudolf Spielberger, head of the Integration Partner Program at Bosch Security Systems.

As part of the program, developers gain a comprehensive library of reusable software components and sample code to facilitate faster integration of Bosch IP devices into their applications. Bosch engineers also help optimise support of video product features for more complex projects.

For integrators, immediate access to the latest information on the compatibility of Bosch devices with other video management systems or storage products makes it easier to design best-of-breed solutions. For end users, stringent testing of all third-party solutions listed in the web portal ensures seamless integration of Bosch IP devices and simple operation.

Bosch solutions are designed to be integration-friendly. All Bosch IP cameras and encoders are ONVIF conformant and run one firmware, allowing partners to support dozens of products at the same time. And now, with the new Integration Partner Program, Bosch is presenting its technology in an even more transparent way. SST

HID Global Awarded Several New Gesture-based Access Control Patents

HID Global, a worldwide leader in secure identity solutions, recently announced that the U.S. Patent and Trademark Office granted several patents for the company's innovation related to gesture-based methods of using three-dimensional (3-D) motion sequences to increase privacy, security and convenience when using RFID-based devices such as smart cards and NFC-enabled smart phones for a broad range of applications. These patent additions strengthen HID Global's IP portfolio of over 1,000 pending and issued patents and protect the company's intellectual capital.

HID Global's latest inventions allow a user to define a series of hand motion sequences or gestures to be used to control operation of an RFID-based device, introducing the notion of a new authentication factor. For example, when incorporated into a RFID smart card, a user can present the card to a reader, rotate the card 90 degrees to the right, and then back to the original position to enable the card to be read, greatly minimizing the possibility of a rogue device surreptitiously stealing the user's RFID credential in a "bump and clone" attack.

"We are excited to see these patents issued as they confirm the industry's recognition of HID Global as an innovator of secure identity technologies," said Dr. Tam Hulusi, senior vice president of strategic innovation and intellectual property with HID Global.

The invention opens up a new field of gesture-based authentication and is particularly pertinent when incorporated into an NFC-enabled mobile phone. Apart from the benefits of convenience and speed, the user can define gesture-based passwords to easily add an additional factor of authentication (e.g., something you know in addition to something you have) to the phone-based transaction. These user-defined gesture-based passwords can also work in a two-dimensional mode similar to a combination lock, or they can also include 3-D motions such as moving to the left, right, forward and backward.

HID Global's invention can also be utilised to unlock Apps, lock and unlock a door similar to the way a mechanical key is used to lock and unlock a door, or allow the user to secretly signal that he is using his card or phone to gain access but is under duress. SST

Cable Transmission Solutions

WWW.AAS.COM.TW

HD CCTV | Network, IP | Analog | UTP Cable

UTP BALUN®

WWW.UTPBALUN.COM

▲Sorry, We only serve to Distributors and OEM Partners.

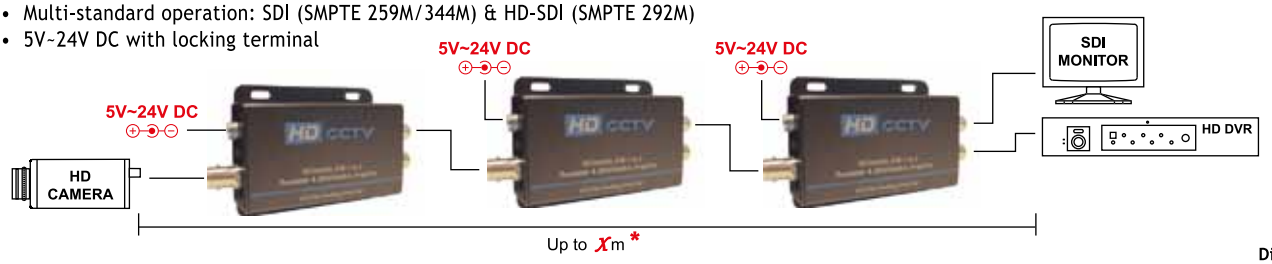
Seeking for Country Distributors

SD/HD/3G-SDI 1 to 2 Repeater & Distribution Amplifier with Re-clocking Function

Full HD 1080 | HD CCTV

HD-SDE-122R Single Device

- Max data rate up to 1.485 Gbps; HDTV Compatible
- Re-clocking Function -- unlimited repeater connection
- Multi-standard operation: SDI (SMPTE 259M/344M) & HD-SDI (SMPTE 292M)
- 5V~24V DC with locking terminal



Price is good for Sample Test only.

$49.00 + shipping

It is below our cost.
▲Limit One for each Distributor or OEM Partner.

*The distance depends on the quality of the SDI signal from the HD camera source and also the Coax Cable & Connector

** The application diagram above shows HD-SDE-122R connected to 2 additional repeater devices.

SD-2

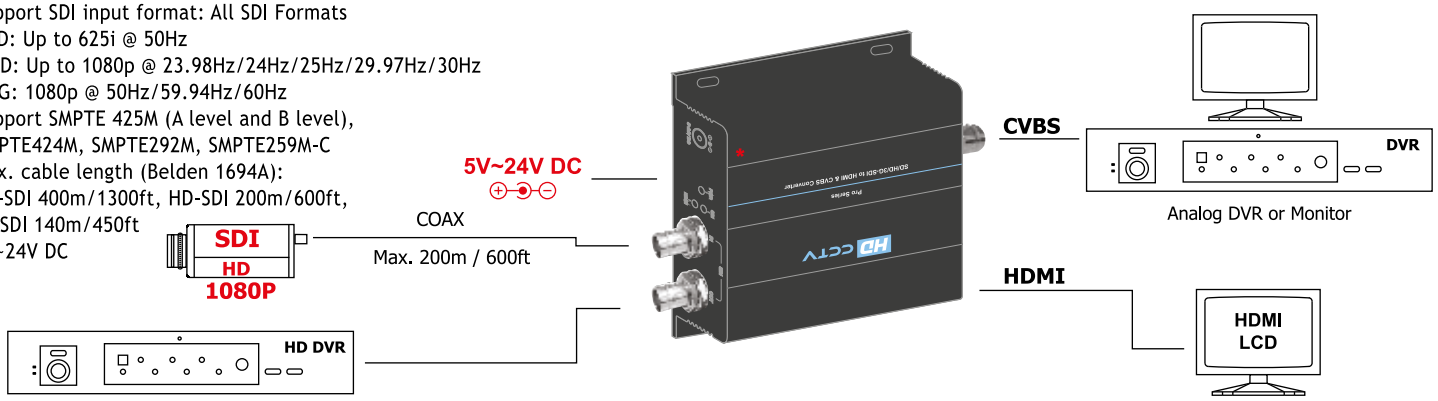
SDI to HDMI & CVBS Converter

Full HD 1080 | HD CCTV

HD-SD-HDMI-PRO

No Delay for Image

- Support SDI input format: All SDI Formats
  SD: Up to 625i @ 50Hz
  HD: Up to 1080p @ 23.98Hz/24Hz/25Hz/29.97Hz/30Hz
  3G: 1080p @ 50Hz/59.94Hz/60Hz
- Support SMPTE 425M (A level and B level), SMPTE424M, SMPTE292M, SMPTE259M-C
- Max. cable length (Belden 1694A): SD-SDI 400m/1300ft, HD-SDI 200m/600ft, 3G-SDI 140m/450ft
- 5V~24V DC



*The distance depends on the quality of the SDI signal from the HD camera source and also the Coax Cable & Connector

SD-8P

Power Guarantee 12V DC High Power Series

UTP Cable

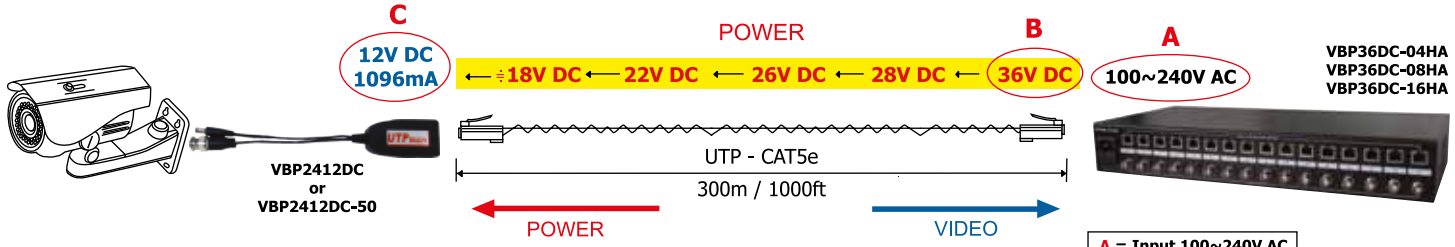
VBP2412DC Step Down 12V DC Receiver - Camera Side

- Use an Cat5e/6 Cable (UTP) to transmit video signal and delivering power to camera.
- Step down power stabilizer to 12V DC.

No More Power Drop! Each camera's power is guaranteed to have 12V DC, 1000mA up to 300m/1000ft!

VBP36DC-16HA Power Hub

- Output Regulated 36V DC, 8.8A
- Input 100V~240V AC (50Hz/60Hz)
- Transmission distance up to 300m / 1000ft



Also Available in 4CH: 36V DC, 2.8A and 8CH: 36V DC, 4.2A

A-13-12V
A-16H-16CH

PoE over Coax Extender Kit	3.5" LCD Service Viewer w/ Wristband	Passive Video Balun	Passive Video Balun w/ Power & Data	PC Balun VGA Extender	Active Balun
					
N-1	T-82	A-1	A-4	B-17	A-8

OEM

**Specifications and appearances are subject to change without notice.

Due to time difference, the best way to contact us is by E-mail: SALES@AAS.COM.TW

TAIWAN TEL: (886) 70-1080-6868 | USA TEL: (1) 510-279-9992

Please download our Product Application Catalog & Company Profile on our website

Honeywell Chairman And CEO Dave Cote Selected "CEO Of The Year" By Chief Executive Magazine

Honeywell recently announced that Chief Executive Magazine named chairman and ceo Dave Cote "2013 CEO of the Year," an honour that recognizes an outstanding corporate leader nominated and selected by peers. The award recognizes the transformation of Honeywell under Cote's leadership over the past decade. During that time, Honeywell has increased sales by 71 percent to $37.7 billion, pro forma EPS1 by 197 percent to $4.48, and delivered a total shareowner return of 240 percent, consistently outperforming the S&P 500 during that timeframe.

Today, Honeywell is a global company, with 54 percent of sales coming from outside the U.S. versus 41 percent ten years ago. Since 2003, Honeywell has made more than 75 acquisitions and 50 divestitures, building great positions in good industries around the world.

"Chief Executive Magazine is proud to recognize Dave as CEO of the Year," said Bob Nardelli, founder and ceo of XLR-8 and a member of the magazine's selection committee. "He has led a remarkable transformation at Honeywell, executing on a vision and rebuilding trust and credibility over the past decade. Not only is Dave a respected leader in the business community, but he is also a leading voice for business in Washington".

Nominations for CEO of the Year were garnered from Chief Executive Magazine's 124,000 readers. The ten most frequently cited nominations were evaluated and a winner was voted upon by a peer Selection Committee consisting of CEOs from leading global corporations. SST

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

Projects

Commercial / Complex

Factory

Condominium

DesFire Reader

Dual Redundancy Module

Plato Reader - Slim Card Reader

600+ readers ward access & security system on SQL Server for hospital and many more ...

1800-570-8832 (Singapore) | 1300-88-3925 (Malaysia)

enquiry@microengine.net

www.microengine.net

Our Office

GlobalGROUP ISO 9001 UKAS QUALITY MANAGEMENT 039

REG No. 44831281647

IndigoVision Announces Launch Of Geoquip Integration System

IndigoVision has launched its latest Integration Module enabling data to be seamlessly integrated between Geoquip perimeter protection and detection systems and IndigoVision's complete IP video security solution.

By allowing perimeter alarm information from the Geoquip system to be managed in the IndigoVision solution, total security management is made incredibly easy.

Events and alarms from the Geoquip system automatically trigger live video or move PTZ cameras within the Control Centre, IndigoVision's software user interface, to focus on a position where suspicious activity has been detected. Recordings and sending of notification emails can also be activated.

"As with all of the IndigoVision Integration Modules, everything is automatic and all alarm information is easily managed in a single user interface ensuring action and response is quicker and evidence is recorded at the highest quality." stated John Semple, IndigoVision's head of Product Management.

"IndigoVision has focused on making security management as easy as possible for not only the security manager, but more importantly for the people who use it on a daily basis, the security operator. The IndigoVision Integration Modules are a significant part of that approach. With the recent release of IndigoVision's Control Centre 4.8, we have created a security user interface like no other. Control Centre is highly advanced but incredibly easy to use, making operator response faster no matter where the camera is located. When you add Control Centre's client licence free pricing structure it can be installed any number of times with no additional cost. It's clear to see why IndigoVision is the solution of choice for completely integrated security projects." Concluded Semple SST

Siemens New Magic Mirror Detector Technology

Siemens recently announced the launch of new passive infrared motion detectors, which utilise the patented Magic Mirror technology from the company.

According to Siemens these new devices are less susceptible to false alarms, set new standards in detection sensitivity and include an extremely compact design.

Magic Mirror is an enhancement of Siemens black mirror technology and provides a number of important improvements. The innovative dual mirror design increases the focal length, which gives the detectors more homogeneous detection sensitivity, especially for wider areas. A new white-light filtering system reduces false alarms caused by external light sources such as the car headlights or lamps. Optional models with integrated anti-masking technology are available.

Magic Mirror models with a range of 12 or 18 metres are currently available. They share the same low-profile housing so intruders cannot tell the type of detector they are faced with. According to Siemens, this has proven to be an effective deterrent. Thanks to their inconspicuous design, the detectors are suitable for indoor use, even in formal spaces.

For the first time, the same bracket can be used for all Magic Mirror models for wall or ceiling mounting. The integrated walk test simplifies and speeds up installation while the flexible end-of-line concept allows fast and error-free connection to the control panel.

Thanks to energy-efficient electronics, all Magic Mirror detectors consume significantly less power than comparable models. The devices also meet all relevant national and international standards and safety approval regulations.

Even before their official market launch, Magic Mirror detectors from Siemens received the prestigious "Red Dot Award: Product Design" for their innovative and attractive design. SST

FLIR

Safety is not expensive it's **priceless**

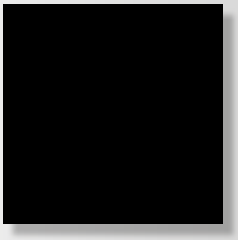
NEW

NEW

FLIR Thermal imaging cameras

Today, the challenge to CCTV professionals is to make sure that video footage is effective on a 24/7 basis, 365 days a year. Securing an area during the daytime is one thing. But what happens during the night? And in weather conditions like fog, rain and snow? What can be detected if CCTV cameras are blinded by the sun?

FLIR Systems offers a wide range of thermal imaging cameras to maximize your perimeter protection in practically all weather conditions such as heavy rain, fog, snow and even in the darkest of nights.



Normal vision

Thermal image

ONVIF

If you want to have more information about the FLIR FC-Series S or any other FLIR thermal imaging camera please contact:

FLIR Systems Co., Ltd
Rm 1613-16, 16/F, Tower II,
Grand Central Plaza,
138 Shatin Rural Committee Road, Shatin,
New Territories, Hong Kong
Tel.: +852 2792 8955
Fax.: +852 2792 8952
e-mail: flir@flir.com.hk

www.flir.com

Images for illustrative purposes only.

VIVOTEK Cameras Help Ensure Security And Compliance At S. African Gaming Authority

The National Gambling Board (NGB) is subject to strict security requirements, as it is the agency within the Department of Trade and Industry (DTI) responsible for the oversight of matters related to casinos, gambling, betting and wagering in South Africa. In order to achieve compliance with the DTI's standards and requirements, the NGB approached the SBD Group, an existing partner of the NGB, to install a turnkey security solution in the NGB's new offices.

SBD, provided with the specifications for the project, proposed a complete solution that included access control, a biometric system, and comprehensive audio-visual facilities including video conferencing in the NSB's main boardroom. The foundation of this comprehensive system lies in the video cameras. SBD turned to Miro, VIVOTEK's official distributor in South Africa, for the cameras as well as the switches and software required to run the installation. Viewing the clarity of the cameras' video, the sustainability of the solution and the good service provided, the NGB opted for VIVOTEK and Miro.

For this project, VIVOTEK's fixed dome, speed dome, fisheye and bullet style network cameras were adopted. VIVOTEK's range of cameras deliver extremely clear and detailed images, making them perfect for an environment like the NGB offices. Ideal for locations and situations requiring accurate identification, their cameras support tamper detection, which detects data loss from camera tampering in real time. When the camera is blocked, redirected, or spray-painted, security staff will be alerted immediately in accordance with the camera settings. SST

Morse Watchmans Key Control Solutions Deployed at Phoenix Sky Harbor International Airport

Phoenix Sky Harbor International Airport recently put in place key control systems from Morse Watchmans, a premier manufacturer of key control and asset management solutions in the industry to maintain strict security procedures for the safekeeping and access of facility keys. Installed throughout the airport complex for use in all back of house operations (i.e. mechanical, fleet pool, maintenance, etc.), the various KeyWatcher Illuminated key control cabinets enable controlled access to keys and provide forensic capabilities such as automated tracking, alarm and reporting functions.

"In today's airport reality, whether it's passengers, cargo or equipment, it's all about security," said Fernando Pires, vp Sales and Marketing, Morse Watchmans.

The automated KeyWatcher cabinets can be used to hold keys needed for access to secured areas of facilities that are restricted from the general public. Authorised users who have permission to enter these restricted areas can access keys which have been pre-programmed to use by entering their PIN code and swiping a pre-issued badge. If the criteria entered matches the information stored in the system database, the key cabinet will unlock and the necessary key can be removed or returned.

The KeyWatcher system offers an increased level of security and control by preventing unauthorised key access and reducing the incidence of lost or misplaced keys. All activity at Sky Harbor Airport is automatically recorded including user, date and time of key access/return. Scheduled email reports of what keys are in or out and who has/had them keeps security management informed and up to date. Requested reports can trace key movements by time, date and user code as well as audit reports that track keys in use, overdue keys and inconsistent key usage. When time is of the essence, the up-to-date and reliable information provided by a key control system can be accessed quickly, allowing personnel to proceed with established procedures regarding secure areas. SST

SMARTCORE Leverages Lumidigm Biometrics For South Korean Immigration Project

Lumidigm recently announced that foreign visitors entering the Republic of Korea will have to go through an immigration clearance process that features SMARTCORE multi-biometric acquisition stations (MBAS) with Lumidigm multispectral imaging sensors. Upon arrival to Korea's busiest airports and seaports, all foreign visitors have to proceed to Korea Immigration stations and submit their arrival card and passport to the immigration officer. They then place the index fingers of each hand on the two Lumidigm fingerprint sensors for simultaneous fingerprint verification. The MBAS also photographs the face of each visitor during the transaction.

Manufactured by SMARTCORE, a leading image processing and immigration solutions provider in South Korea, the MBAS is an ergonomic, integrated unit that captures both facial and fingerprint data at the Korean immigration stations. It minimises imaging time and acquires high-quality biometric data.

Because the fingerprint sensors use multispectral imaging technology, the MBAS is able to read fingerprints on the first try. Multispectral imaging collects information about both the surface and subsurface fingerprint to capture reliable data, regardless of whether a user's finger is dry, wet, dirty, slightly rotated, or difficult to capture. Data is captured on the first try every time, allowing tired travellers to enter the country as quickly and easily as possible. "When selecting a fingerprint biometric for the MBAS, we had to make sure every visitor could use the device," asserted Bong Kyu Choi, president of SMARTCORE. SST

CA Technologies And NTT Com Security Partner To Offer IAM-as-a-Service Using CA CloudMinder In Asia Pacific And Japan

CA Technologies recently announced that it has signed an agreement with NTT Com Security (formerly known as Integralis) to host CA CloudMinderTM Identity and Access Management (IAM) software-as-a-service solution in the Asia Pacific and Japan (APJ) region. This partnership enables CA Technologies to provide identity management, advanced authentication and single sign-on as-a-service locally.

NTT Com Security, a global information security and risk management solutions provider, will host CA CloudMinder via its Group Data Centres across the APJ region, helping local customers address data sovereignty policies in certain markets.

CA CloudMinder provides enterprise-grade IAM for cloud-based or on-premise applications in a highly scalable, multi-tenant, IAM as-a-Service solution. With extended out-of-the-box support for social identities and additional on-premise and cloud applications such as Microsoft Office 365, CA CloudMinder helps IT departments reduce the complexities of managing IAM. SST

Deploying Protective Measures for Effective Border Security

By Joshua Kwai

Border security management generally consists of a set of security control measures that is implemented with the objective of regulating human traffic, cargo traffic, vehicles, and so on, entering and leaving a country. To effectively place the borders under tight controls, multiple government security agencies such as customs, immigration, police, narcotics and so on are being co-located. Although borders are tightly controlled, and placed under close surveillance for detecting incriminating activities, and deterring undesirable persons and objects from entering and departing a country, occurrence of incidents of transnational crimes still persists.

For instance, it was reported that two individuals from Edinburgh and one from Fife were arrested by the Scottish Crime and Drug Enforcement Agency (SCDEA) for an offence of cross-border drug trafficking. In April 2011, law enforcers intercepted the criminal group. As a result, more than 16.5 pounds of heroin with an estimated street value of £637,000 was seized by the authorities.

In 2012, there were cases of human trafficking in Rwanda; a country that has been greatly affected by the trafficking of women and children who were exploited in domestic servitude. In one of the cases, two Ugandan girls were intercepted by the authorities at Kigali International Airport while they were en route to Malaysia. In another case an eighteen-year-old Burundian girl was arrested at the border to Rwanda.

She was supposed to travel to the East Asian country too.

Apart from criminal activities occurring at the borders, acts of terrorism are also a threat. In mid 2013, it was reported that two officers were injured during the attacks at the camp near the Southern Palestinian city of Rafah by a group of militants. In another incident, in July 2013, a group of gunmen opened fire on the car of a senior military commander in Sinai.

As borders are no longer being restricted physically, it is now even more challenging for law enforcement agencies to curb security threats posed by transnational criminals and terrorists. This is especially so in the cyber world. Does this mean that there are no measures to mitigate them?

Following is a set of strategies which law enforcement agencies around the world should consider adopting to effectively and efficiently detect, deter and curb cross-border security threats.

IMC Model

Conventionally, security measures deployed at borders come in the form of security manpower deployment, security technologies, and multi-agency check systems. To effectively exercise border security, it is recommended that protective measures go beyond traditional approaches.

In the following paragraphs I will introduce the IMC model which consists of intelligence sharing, multilateral legislative enforcement, and cyber impediment system.

Intelligence Sharing (IS)

Receiving information on the movement of cross-border criminal and/or terrorist's groups, hideouts, vehicles used, identification of their leaders, finances and so on, is paramount. Without these pieces of information, it is a tremendous challenge for law enforcers to effectively eradicate these threats.

To efficiently intercept any criminal activities and/or acts of terrorism at the borders, information once collated, affirmed, and analysed must then be quickly shared with all authorised information sharing network system stakeholders; state security agencies and counterparts from other countries, without any hesitation and information being withheld. IS ought to be carried out in the utmost transparent and sincere fashion in order to optimise its effectiveness and promptly place adversaries and their groups under arrest.

The question here is how best information can flow from the frontline to the backend analysts' desks accurately,

and then to the hands of the authorised recipients in time for them to make rapid informed decisions.

Prior to addressing this issue let's take a look at it from another angle – the challenges of sending collected information to the analysts then to the stakeholders. These challenges are often centred around trust issues (unwillingness to release or relay information), deficiencies in communication, red tape in transmitting information and so on.

Here are a set of recommended measures to overcome these obstacles:

- Friendly forces should organise landward/seaward joint drills, and operations against transnational criminal and/or terrorist's groups frequently
- Table-top exercises should involve partnering counterparts to synchronize each other's capabilities and enforce a collaboration effort for common interests
- Organise dialogue sessions to involve all partnering alliances to exchange ideas on mitigating measures on a regular basis. This is to align the common objectives and interests of establishing the intelligence sharing network system
- Develop an electronic system where information can be uploaded with encryption, and disseminate it to all authorised partnering alliances through a wireless platform. Such systems must have a control function that allows certain pieces of uploaded information to be accessible to an authorised group of recipients

Multilateral Legislative Enforcement (MLE)

Many a time, legislations crafted against criminal activities and/or acts of terrorism are very much localized. Some of them are only applicable in a certain country but not in another. Even when there are similar legislations, the degree of punishment differs from country to country. This creates a loophole for adversaries to exploit and continue committing cross-border criminal activities and/or acts of terrorism.

To curb or deter these threats even before they can reach the border, I suggest that alliance countries should put in a joint effort to synchronize their anti-crime and counter-terrorism legislations including the span and depth of the punishments. Alliance countries may consider introducing legislations which are enforceable on an individual or group of citizens who have committed an offence overseas, in their home country.

There must be a close partnership developed among the alliance countries to enable each other to deport an individual or group of own citizens to their home country to receive the deserved punishment.

In order to better synchronize each other's legislations to fully deter criminal activities and/or acts of terrorism and introduce appropriate punishments on cross-border

adversaries, I recommend that alliance countries' legislative bodies work closely to co-develop laws which all partner countries can introduce and enforce.

Cyber Impediment System (CIS)

Borders nowadays are no longer limited to physical landscapes, airspace or water. It has gone beyond these physical characteristics into the cyber world. Transnational criminals and terrorists have also exploited this space to infiltrate a nation and promote criminal and/or terrorist ideology.

To effectively deter it from entering a country via this "borderless" space, it is suggested that stringent control measures be introduced. National teams of cyber security enforcement units should be created for placing cyber criminal activities and/or acts of terrorism under close surveillance and to exercise required course of actions whenever deemed necessary.

The course of actions should then be introduced multilaterally among the alliance countries. When a partner country has reported a cyber space violation by suspected criminals and/or terrorists, both the home country and host country should jointly shutdown the internet website that criminals and terrorists have exploited. The website hosting entities, website developers and/or owners should then jointly be taken to task by the legislative bodies in both the home and host country. These measures strongly discourage criminals and/or terrorists from disseminating their ideology, using the cyber space to recruit members, promote violence, and so on.

Conclusion

It is trusted with the introduction of IMC Model, borders, whether in a physical form or cyber space can be effectively and efficiently protected by keeping criminals and/or terrorists at bay. Apart from implementing the model at the governmental level, it is recommended that state security agencies work closely with security professionals in the private sector too, in order to have a wider reach in terms of curbing criminal activities and/or acts of terrorism. SST

About the Author

Joshua Kwai is the CEO & President of JK Consultancy Holdings Group that consists of both JK Consultancy Holdings Pte Ltd and ATCP Consulting Group Sdn Bhd. His fields of expertise are in Security Management Consultancy, Counter Terrorism Strategies, Anti-Terrorism Strategies, Business Continuity Consultancy and Security Training.

Email: joshuakwai@jkconsultancyholdings.com
Website: www.jkconsultancyholdings.com

Experts' Commentaries On The Importance Of Implementing Protective Measures For Effective Border Security

Protecting borders from the illegal movement of weapons, drugs, contraband, and people, while promoting lawful entry and exit, is essential to homeland security, economic prosperity, and national sovereignty. Border perimeters are normally several kilometres in length.

This often creates challenges on security management. Additionally, a high volume of users at the borders, including employees, travellers and contractors and sophisticated organizational structures may give rise to potential risks such as unauthorized entry using cloned cards.

One way to effectively provide security is by establishing multiple layers of security. This could include implementing security measures like checkpoints, canine searches, air marshals, cargo inspection and explosive material detection. Each layer of protection, on its own, is capable of preventing terrorist attacks. Together, the layers' security value is exponentially higher, creating a much stronger overall security system.

Lee Wei Jin
Director of Sales, ASEAN
HID Global

Another omnipresent layer of border security is access control. Controlling access to key border areas is a critical security task. For example, the latest access control systems enable access control level settings at critical entry zones and restrict entry to authorized employees only. At the same time, high frequency contactless readers and credentials offer enhanced system security using 64 bit diversified keys, mutual authentication, and data encryption technologies. Organizations can also create another layer of security by adding a custom authentication key and standardized card format to their access control system.

Raj Munusamy
Vice President, Global Public Sector,
Siemens Enterprise Communications

Effective border security is no longer possible without seamless communications. Effective border security is delivered within an always-on, highly interconnected, multi-agency environment. Often covering both surveillance and control duties, border security officers need to be able to respond to situations and emergencies rapidly – fully informed and able to act.

These incidents require seamless coordination within teams in the agency; across multiple ports-of-entry; and between multiple services – from homeland security, to police, to rescue services and even to the Defence Forces - this is no easy task. Collaboration, communications and instant information sharing between myriad command and control centres, and on-the-ground multi-agency teams are critical. In larger geographies, the duality of national and regional response targets adds a further dimension of complexity.

Given the multi-agency environment, assuring the smooth interaction between caller, call-taker and dispatcher is an absolute must; fusing information from multiple sources – including social media – is the only way to allow fast and accurate decision-making, while actionable intelligence must be created to effectively coordinate response teams.

However, rapid response is at risk when command and control centres aren't fully equipped to handle high volumes of calls, sensor triggers and alarms, in parallel.

Here are some common pitfalls:

- Inability of the call taker to handle and prioritize multiple calls, including those classified emergency
- Group calls can't take place to aid multi-agency collaboration
- Key personnel cannot always get through
- Misalignment among sources on operational processes
- Poor rapid switching between radio and voice calls
- The lack of a 'single pane of glass' experience, aggregating myriad information channels

This increases the pressure for border agencies to deliver an effective, fully collaborative and fail-proof communications environment - because in an emergency every second counts, every minute of every day.

Experts' Commentaries On The Importance Of Implementing Protective Measures For Effective Border Security

The border, the geographical boundary of the national sovereignty, is critical to a country's security. Hence, an advanced and complete security infrastructure with surveillance capacity at the borders plays an important role since it is not only able to secure the transit of travellers between countries, but also able to support the suppression of criminal activities such as illegal migration, drugs and weapon smuggling.

Moreover, in the past few years, terrorists' attacks have increased significantly on the global stage. The border, as a country's front line, is one of the important thresholds against the intrusion of terrorists.

The surveillance capacity with advanced and networked cameras for precise monitoring is turning out to be pivotal within the entire security infrastructure at borders. A high-Megapixel or thermal camera with network connection is especially required for supporting the authorities concerned and safeguarding national security since a network camera not only enables the delivery of superb image quality with efficiency for clear face or license plate recognition, but also enables the detection of suspicious criminals and illegal actions in advance, thus effectively enhancing the border security.

Steve Ma
Executive VP
VIVOTEK Inc.

Marc Handels
Chief Marketing and Sales Officer (CMSO)
SALTO Systems

National borders are a security issue globally. Vulnerable or insecure borders are one of many security risks given in the current economic landscape and the continuing threat from cross-border crime and terrorism.

Global governments are tasked with protecting their citizens, their economies and their resources. In order to achieve this and protect against crime and terrorism, steps must be taken to ensure all hazards and any potential threat stays beyond the border and does not penetrate into a nation.

One of the keys to this is securing gateways or points of entry, principally airports and ports. Many governments have declared that key national infrastructure such as these must have robust security and use the latest technology to control access to, within and around such facilities.

Such security has been proven to be most effective when a multi-layered approach has been adopted, beginning with perimeter protection and moving inwards to core facilities. This creates a much stronger overall security system.

Access control is a vital part of this mix and offers a versatile and cost-effective way to regulate those who require access to specific areas at specific times, denying admission to unauthorised persons with no right or reason for entry, without compromising security.

We would like to invite Security Professionals to share your opinions and perspectives for the Pundit Perspective section in the November/December Issue of SST! This issue is centred around the Residential, Educational & Institutional vertical market. The topic we would like you to comment on is this:

Why has it become so critical for schools to implement security measures to monitor staff and student movement within campus compounds?

Your submission must include
(A) Commentary on your perspective (not exceeding 200 words) with your Name, Current Job Title and Company name
(B) A high resolution image yourself

For Security Professionals who are keen on being featured in this section, please drop me an email with the above-mentioned details to the following email address: sst@tradelinkmedia.com.sg

MOBILE SECURITY

By: Andreas Indra
Director Consulting & Design – Network Infrastructure & Security, Siemens Enterprise Communications

Mobile change

Today's working world is changing, moving away from a sedentary nine to five office day toward jobs where employees are constantly on the move, regardless of the size of the company or the sector. Fixed workplaces are giving way to hot desking solutions and home offices. Desktop PCs are being replaced by notebooks, tablets and smart phones. Employees want to be able to employ a wide variety of devices to send and receive e-mails on the move, and to access the company intranet or internal services. Gone are the days when these mobile devices were regarded as gadgets for only a small group of employees – their use as key business tools is now widespread and increasing all the time. They are a natural part of everyday life for today's generation, the so-called digital natives.

Using communication devices on the move, however, exposes workers to potential security risks, including theft or loss outside of secure company premises. Notebooks can be left unattended in a car or conference room. And, left unsupervised, even a short period of time is sufficient to access any confidential data on a device. Damage can be caused by: unauthorized viewing of data (loss of confidentiality), unauthorized modification of data (loss of integrity) or impairment of functionality (loss of availability). These risks are further exacerbated as network and infrastructure boundaries become increasingly blurred. The upshot is that the data being transmitted has to be protected as well as the communication path itself.

Spanning company boundaries

From programs to apps

Originally, both programs and user data were stored on the actual device being used. Nowadays, these programs have been adapted for use on mobile devices as well, and the user data is stored centrally. These optimised programs are referred to as apps. Data is centrally stored using cloud technologies, with the advantages of it being constantly in sync and available from any location or device, while being highly secure.

Boundless communication

The desire to use the same apps on all devices applies particularly to communications applications, as outlined briefly below.

- Web conferencing: Collaboration in a virtual space with desktop sharing; in other words, shared display and processing of documents
- Social networks: Messaging, posts, blogging
- E-mail: Rapid delivery and access to all e-mails from different devices
- Telephony: Availability of contacts and user interfaces
- Video/teleconferences: Telephone calls with three or more participants, sometimes with video

Each of these types of communication requires suitable security measures to prevent eavesdropping on calls or interception of data.

The cloud as a social entity

Applications are moving increasingly to the cloud with data storage consequently being placed in the hands of

providers. However, this allows worldwide availability at the same time. Every data owner should pay special attention to data protection in this context as data is often stored outside national boundaries and therefore not covered by local data protection laws.

Social media platforms constitute a special domain of cloud services. Such platforms encompass a variety of networks such as Xing, LinkedIn, Facebook, Twitter, Yammer, YouTube, Wikipedia, Web Collaboration Portals, etc. They allow interaction between people at different locations and often also serve professional interests, such as finding business partners, employers and employees. These platforms are also of interest for social engineering.

Mobile Devices

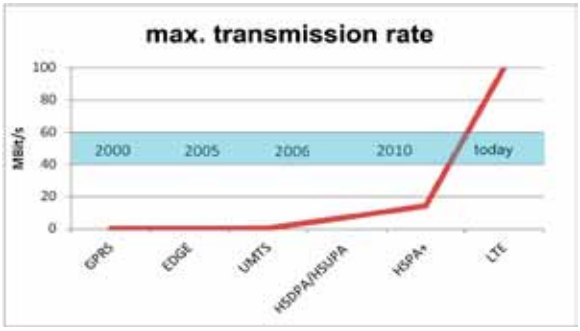
Nowadays, the vast number of applications that have become an integral part of everyday business life can be used on all sorts of different mobile devices. The most important of these include laptops, tablets and smart phones.

Networks galore

Users of mobile devices can now connect directly (VPN) or indirectly (Internet) to the corporate network and work productively anywhere and anytime.

Mobile radio

There are currently six methods of transferring data to mobile devices, and transmission rates have been significantly increased with each new standard. More than 60 percent of the world's population will be able to access 4G (LTE) mobile broadband technology by 2015. With faster connections and the additional opportunities this offers, mobile data traffic is increasing almost exponentially.



Methods of transforming data to mobile devices.

WLAN

WLAN design needs to cater for every user and all devices. Laptops, for example, differ significantly from smart phones in terms of their features. The network has to allow simple inclusion of all mobile devices and be able to manage the increasing number of these devices.

LAN

Because they are generally connected to the corporate network using WLAN or a mobile phone network, the LAN has diminished in importance with the advance of mobile devices. Laptops are integrated directly with the corporate LAN via docking stations. However, appropriate checks must be made before connection to the LAN as they could already be infected with malware as a result of their activities outside the internal company network or from private use (BYOD).

App-solutely secure?

The wealth of innovations, however, brings challenges to companies as well as benefits:

- Apps: Generally speaking, these are not designed for the levels of security required by companies
- Communication: Confidentiality and privacy are acutely at risk as professional and private boundaries at companies become blurred
- Cloud: Mobile data is adding a new dimension to data protection and security (Big Data)
- Social media: Everyone can speak to everyone - an enhanced sense of awareness is required here
- Devices: More options for everyone – also for hackers and spies
- Networks: One secure network (VPN) and many non-secure networks (WLAN, 3G/4G, UMTS possibly without VPN) – employees must use the "right" path

Hence, the existing security strategy has to be adapted to the new challenges.

Castles are outdated

Data security has focused traditionally on security measures that keep unwanted intruders out of the network. The new security strategy has to focus on protecting data and communication as well as ensuring network integrity. The question is not where a particular security measure should be implemented, but rather which security measures are relevant along the entire path.

"I picked up a little something on the way here"

In many companies, it's the top managers with their newly acquired high-tech phones who are the first to create gaps in the protective IT security walls that have been built up around corporate systems. Because they are used both within and outside corporate boundaries, these mobile devices

are beyond the administrator's control. They consequently require protection of their own against viruses and attacks of all kinds.

Mobile Security V1.1

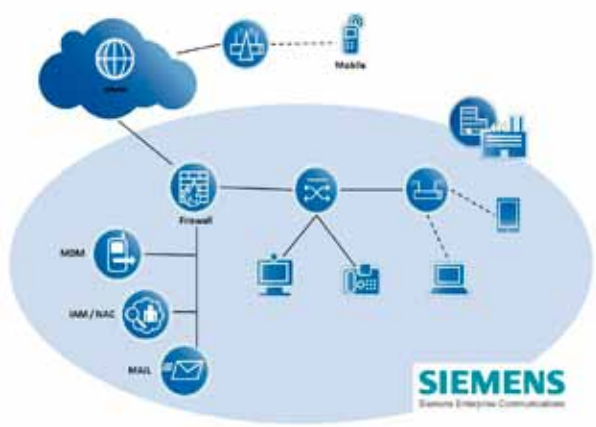
The challenge lies in integrating these various devices with the existing corporate infrastructure and being able to manage their operation securely, efficiently and with a minimum of administrative overheads. Conventional security concepts are based on the "castle" principle, i.e. building a strong perimeter defence against intruders. This involves powerful defence systems in the form of firewalls, anti-spam and anti-virus solutions, content filtering and reputation verification.

In addition to this, appropriate authentication solutions are often set up to regulate access to the company's most sensitive information and zones, which are located – to maintain the analogy – within the castle's "tower".

Authorised entry to the respective zone normally grants broad access to the relevant processes and information. The increasing use of mobile devices means that applications and identities are being used both inside and outside companies, leading to a blurring of professional and private boundaries.

Employees keep in contact with customers using blogs, social networks or twitter information on the move – the potential scenarios are many and varied and can scarcely be mastered using traditional security architectures. There is a definite trend toward an interaction and information-based protection model. Although traditional security solutions, such as firewalls will always remain in demand, additional new components are needed to alleviate the new security problems that are arising, and to keep the associated administrative overhead as low as possible.

Some promising elements of this extended security architecture are outlined briefly below.



Network Access Control (NAC)

NAC identifies devices and users and allows them to access network sections and services based on defined rules. NAC is now a must-have extension to the existing infrastructure, especially for companies with mobile devices.

Identity and Access Management (IAM)

Without effective rights management for every user, chaos is inevitable. However, in order to determine who actually has which rights to what, the users as well as the devices have to be identified. Professional IAM therefore precisely regulates which user can access which company applications and data using which devices.

Mobile Device Management (MDM)

"Mobile Device Management" (MDM) is used to efficiently implement and enforce the appropriate security guidelines. Its deployment becomes all the more crucial when confidential company data is stored on mobile devices. An MDM solution enables: Central management of mobile devices; Provision of updates and applications; Blocking of non-trusted apps and "Remote" deletion of data.

What impact does this have? What should I look out for?

Strategic implications

CIOs and IT managers are faced with a dilemma: They see an acute need for action in almost all mobility areas, but only rarely is strategic planning used to address these needs. This not only opens up potential security risks and endangers the efficiency of mobile employees; it also means that companies fail to turn mobile devices and applications into innovative business technologies. To be able to systematically cope with the growth of the mobile sector and tackle its infrastructure consequences, CIOs need a viable mobility strategy.

Faced with all of these new trends and opportunities, companies need to consider which strategy they want to follow in order to gain the maximum benefits.

Companies that do not have a long-term mobility strategy run the risk of their devices, platforms and applications proliferating to the extent that they become difficult to control and tough to integrate efficiently with the existing infrastructure.

The first step to consider is how to control the adoption of mobile devices within the company. Decisions need to be made about the types of devices that are to be supported, and about the feasibility and impact of a Bring-Your-Own-Device strategy at the company. The companies should also have a good idea of the services to be used and how these fit in with the corporate strategy. External aspects, such as customers, should also not be ignored. This means that corporate IT must adapt so that customers, partners and employees, together with their applications and intelligent products, are integrated in the most beneficial way possible.

When it comes to restructuring, one of the most important points to look at first is the existing strategy. Can any existing components of this strategy be retained and savings made by doing so? Is the existing strategy actually compatible with planned business development? Answering these questions involves examining the existing security paradigm, determining the new risks, and reviewing the possible solutions from an economic perspective.

Organizational implications

Once the economic factors have been examined and the strategy for a mobile infrastructure has been defined, some of the most critical aspects come into play, involving areas such as mobility management, organizational security and risk management. A necessary first step is to set up internal guidelines for the use of these devices and modify existing guidelines to take account of any new aspects. In addition, all changes need be clarified with the relevant company bodies, such as the works council. It is also important to ensure that there is a clear assignment of tasks and responsibilities for any connected implementation or administration tasks.

Another critical aspect is employee awareness. The system can never be protected against its own users. Security achieved through implementing technical measures stands or falls with user awareness about security. It is important that users are made particularly aware of the need for greater personal responsibility and a more conscientious approach. Only when users come to realize that security measures are meaningful and necessary are they prepared to accept them more readily, even when they entail some restrictions in terms of use.

Technical implications

Additional software, such as a VPN client, is generally needed in order to be able to access company resources. This software must run on a wide variety of devices and be easy to install. Today's security requirements demand extensive measures on both the personnel and technical levels. A basic level of protection for the traditional IT infrastructure can be largely ensured through purely technical measures, through a firewall or proxy systems with the appropriate policies, for example. Over and above this, the use of mobile devices requires a rethink of existing security mechanisms. Switching from endpoint to access-based security solutions is absolutely essential. Endpoint security is based on the principle that a device is responsible for its own protection. Should a device actually be compromised, this means that the attacker has direct access to the company's data.

Access-based solutions give the attacker no direct access to company data in the event of a device being compromised. This approach is based on multi-stage protection. On the one hand, the device is protected against unauthorized access by third parties using a PIN or a similar mechanism.

On the other hand, access to company data is controlled by means of user authentication. A positive side-effect of such a portal or proxy system is that external devices have no direct data connections to the company's internal network.

And now?

Mobility is good for productivity but also represents a serious risk to information security. The key to comprehensive end-to-end security lies in a combination of device, network and data security. Measures that go beyond basic data protection and include user authentication, access control and policy enforcement are absolutely indispensable. The right technology partner can provide comprehensive support at all levels. This includes security solutions, optimisation and managed system administration and recovery that guarantee comprehensive security, compliance and integrity for the entire mobile infrastructure. The following points are of vital importance to the use of mobile devices within a company:

- The creation of guidelines for using and handling mobile devices and company data is essential.
- The IT Infrastructure has to be adapted to the new challenges and risks, taking account of both the existing infrastructure and the planned future development of the company
- Clear responsibilities must exist for the respective topics, with clearly defined scopes for company and employee
- Employees must be made aware of how the devices are to be treated
- Any known weaknesses or security risks, such as unregulated app downloads on devices, must be kept in check

Article courtesy of Siemens Enterprise
www.siemens-enterprise.com SST

Airport In South Korea Deploys IP Video Surveillance System To Beef Up Security

The Customer

Korea Airports Corporation (KAC), the country's leading public corporation, specializes in the efficient construction, management, and operation of airports. KAC manages a total of 14 airports throughout Korea including Gimpo, Gimhae, Jeju, and Daegu. More specifically, KAC manages and operates the movement of airplanes on runways, in mooring areas, and in passenger and cargo terminals, as well as various buildings, roads, and parking lots.

The Challenge

Gimpo airport is considered to be the gateway to Seoul, the Republic of Korea's largest city. The airport hosts up to 226 000 flights per year, the majority of which are domestic flights. In 2010 alone, Gimpo serviced over 17500 000 passengers, making it one of the busiest airports in South Korea.

An airport of this size requires an advanced security system that can manage numerous events and incidents simultaneously. The previous security system installed at Gimpo airport proved to be a poor fit and as a result, inefficient. For example, the parking lots at the airport lacked a high-resolution digital surveillance camera system; hence there was a high incidence of vehicle theft. It was also very difficult to identify the culprits of fender-benders; minor collisions were somewhat common during weekends and holidays when the number of vehicles in the parking lot would exceed capacity.

The ability of Gimpo Airport to identify who was at fault was hindered by the security system employed. In any airport, immediate action is important and necessary in the event of any accident or incident. To address these security weaknesses, Gimpo Airport saw that is was crucial to introduce a new video surveillance system to ensure the safety and well being of all the airport's clients and employees alike.

Gimpo International Airport's Security System Requirements

Gimpo Airport needed a network system that would increase the effectiveness of its day-to-day operations. The existing analog camera system at the airport was no longer suitable to manage the airport's numerous accidents and events. For example, the analog system encountered difficulties in playing and saving video images and produced low image quality and resolution. The airport required a more intricate sophisticated network solution that would streamline its security operations and management. The integration capability of the new security solution was an important criterion. It was projected that individual security solutions in diverse fields including iris and fingerprint recognition would at a certain point in the future, be integrated into the new network-based solution. The new system needed to be stable and fully integrated, with the possibility to install new components and to expand when necessary.

An airport of this size requires an advanced security system that can manage numerous events and incidents simultaneously. The previous security system installed at Gimpo airport proved to be a poor fit and as a result, inefficient. For example, the parking lots at the airport lacked a high-resolution digital surveillance camera system, and as a result, there was a high incidence of vehicle theft. It was also very difficult to identify the culprits of fender-benders; minor collisions were somewhat common during weekends and holidays when the number of vehicles in the parking lot would exceed capacity. The ability of Gimpo Airport to identify who was at fault was hindered by the security system employed. In any airport, immediate action is important and necessary in the event of any accident or incident. To address these security weaknesses, Gimpo Airport saw that is was crucial to introduce a new video surveillance system to ensure the safety and well being of all the airport's clients and employees alike.

The Solution

Omnicast, Genetec's video surveillance solution, is optimised for the management of digital video, audio and metadata over an IP network. Its distinguished scalability and flexibility enables users to add cameras, workstations, and other system components at any location on the network. Omnicast was chosen for its remarkable flexibility and integration capabilities and responded perfectly to the airport's security needs by combining access control and video monitoring that was previously employed as independent security solutions.

Gimpo Airport specifically selected Omnicast Enterprise, a feature-rich, scalable, and flexible IP video surveillance solution, to completely replace the existing system.

More than 20 high-definition cameras from Axis Communications, a global leader in network video products, were installed making Gimpo the first airport in Korea with HDTV quality network cameras. A combination of AXIS Dome and AXIS Network Cameras monitor 27 public areas including bus stops, taxi stands, and parking lots, covering an area of over 300,000 metres square and accommodating over 9,000 cars. Camera feeds are monitored in real time on two large 50-inch monitors, which are divided into nine and 16 sections, respectively.

The images are saved on two servers and kept for 30 days. Genetec's solution was used from installation to operation without the need for any extra development by Gimpo Airport.

Benefits

Gimpo Airport's main concern was the possibility of a network overload caused by the transfer of mass data from the high-definition Axis cameras. However, Insung Information reassured Gimpo Airport that the implementation would go smoothly, and reinforced this assertion by presenting an implementation success story. Orlando Sanford International Airport in the United States, one of the busiest airports in the state of Florida, achieved a major system upgrade by implementing Omnicast together with Axis network cameras. This notable upgrade consisted of converting 150 cameras from analog to digital and adding 80 new cameras to their system.

Insung also ensured that the system would be installed to meet the airport's specific requirements. "While it was a concern whether high-definition cameras would slow down the system, Genetec's Omnicast still performs remarkably well even several months after implementation. We are very satisfied with its performance. Moving forward, I believe we will continue to benefit from management and cost efficiency as well as the stability of the solution," said Yeon-seop Kim, manager of the Aeronautical Communications Team at Korea Airports Corporation.

In a real-time capacity, Omnicast has also been vastly useful as a traffic management tool. Road operators are able to view the entire road at once, making incident diagnosis and response immediate. The system has also allowed for quick evaluation of the effects an incident might have on traffic conditions several kilometres back. Orchestration of emergency vehicle arrival, monitoring of response time and surveying to ensure all needs are addressed can all be accomplished from one single location in the control centre.

Genetec's Omnicast solution makes it possible to automatically change monitoring targets with system events with alarm management and scheduling functions. For example, a surveillance camera can change targets to monitor the display devices of major facilities in the airport from midnight until dawn when there are not many passengers. Once the specific time period has ended, the camera can return to monitoring its original targets. This function significantly contributes to the safety and security of night workers at the airport.

Maintenance was also an important criterion when choosing Omnicast. Surveillance systems. In facilities like airports where safety and security are critical, immediate action and repairs are required in the event of errors or failures. Omnicast's intuitive user interface, which is perfectly optimized in the Korean language, enables administrators and operators to easily control the system and quickly analyze the causes of these errors or failures.

In the event that the main server stops due to failure, the standby server automatically takes over operations. This important advantage of the Omnicast Enterprise Solution means that a failure can be resolved without interrupting system operations. The operators of Korea Airports Corporation in the CCTV Control Centre can now monitor video images and operate the system uninterrupted 24 hours a day, 365 days a year.

The Results

Omnicast was introduced to the Airport in August 2010 and since its installation has had a significant impact on the prevention and resolution of incidents. The system provides concrete evidence and clarifies where the responsibilities lie when events occur such as pedestrian accidents, minor automobile collisions, and thefts both within and exterior to the airport terminals.

"We can provide better service to our employees and passengers with this new solution. Omnicast's advanced features help us manage the surveillance for our parking lots and help us prevent accidents that can lead to casualties," commented Kim. "The biggest advantages of Omnicast are the systems scalability and flexibility. All the other regional airports along with International Line building at Gimpo Airport are planning to add new security systems. Omnicast will definitely be considered for these future projects." SST

Healthcare Facility Near Mexico City Uses Five-Megapixel Cameras To Monitor Perimeter Zone

The Customer

Merck is the second-largest healthcare company in the world and a global leader in consumer products and animal care. Over the years, Merck researchers have created ways to treat and prevent a range of illnesses, from the discovery of vitamin B1, to the first measles vaccine, to cold remedies and antacids, and the first statin drugs used to treat high cholesterol. The large pharmaceutical company has constructed corporate laboratories in Naucalpan de Juárez, Mexico, a municipality just northwest of Mexico City.

The Challenge

Merck was looking for video technology to provide day and night surveillance of the perimeter zone at the corporate laboratories in Mexico. The company needed

high resolution and sharp images to enable identification of faces and license plates, but analog technology fell short of meeting their needs.

The Solution

To provide high-quality videos for surveillance of the perimeter zone at Merck's newly constructed laboratories, Ariel Maldujano, head of Management And Technology services, turned to Alarmas Universales, an integrator company with 38 years of experience in the market. Marco A. Godina of Alarmas Universales designed and installed the new system at the Merck facility in Mexico. When looking for technology to provide higher-quality video imaging, Godina learned about Arecont Vision through a manufacturer's representative.

Arecont Vision's five Megapixel day/night cameras were the perfect choice to provide the resolution required for the application at Merck in Mexico, and Alarmas Universales installed five Arecont Vision cameras along the perimeter zone.

The quality of Arecont Vision megapixel cameras is a huge selling point, and Godina of Alarmas Universales said, "We never forgot that Arecont Vision pioneered Megapixel technology." The quality of the Megapixel image was most important, and another benefit noted by the integrator is Arecont Vision's digital zoom capabilities. The sharper images have enabled the customer to identify faces and license plates. The system has performed well to-date, and Arecont Vision has been responsive to the needs of the integrator and the end-user.

Arecont Vision Megapixel IP cameras provide better overall coverage with higher resolution for superior picture quality and better results. These cameras also provide broader coverage with fewer cameras. The system produces superior images in both daytime and evening lighting environments. In addition to greater image clarity, the Megapixel cameras' ability to cover more area using fewer cameras versus conventional standard-resolution IP cameras helps to lower the total cost of ownership of the system. The Megapixel IP cameras allow operators to zoom in on specific areas of live or archived video to see important details such as a license plate number. The cameras combine image quality with smaller image files and improved video streaming using H.264 compression. Smaller file sizes reduce storage requirements. SST

CAM SECURITY & FIRE 2013

CAMBODIA'S No.1 INTERNATIONAL SECURITY & FIRE PROTECTION SHOW

CAMBODIA'S No.1 INTERNATIONAL SECURITY & FIRE PROTECTION SHOW

Co-located with :

CAMBUILD'13

CAMBODIA INTERNATIONAL BUILDING & CONSTRUCTION INDUSTRY SHOW

10-12 SEPT 2013 • DIECC, PHNOM PENH, CAMBODIA

10-12 SEPTEMBER 2013

DIECC, PHNOM PENH, CAMBODIA

Organised & Managed by :

AMB EVENTS

AMB EVENTS (CAMBODIA) PTE LTD
#240, street 101, Sangkat Beoung Trabek,
Khan Chamkarmorn, Phnom Penh.
Tel : +(855)23 210 806 Fax :+(855) 23 217 290
Email : support@ambexpo.com

To Book Your Booth at the Expo, contact Mr. Veasna at veasna@ambexpo.com

To Visit the Expo, save USD5 on Expo Entrance Ticket.

www.expocambodia.com/camsecurity13

Police Department In Australia Adopts Video Surveillance System To Increase City-Wide Safety And Fight Crime

Background

Located just five kilometres west of Melbourne, Australia, Footscray is a small suburb, which is home to a diverse and multicultural population of over 75,000. As part of the City of Maribyrnong, Central Footscray is bustling with a myriad of shops and restaurants, and its easy transportation via bus or train to Melbourne continues to spur growth in the area. Footscray's convenient location has also attracted many new businesses and recently, local government initiated plans for a $500 million high-density commercial and residential development project.

The Challenge

Like most developing suburbs, Footscray was seeing an increase in street-level crime such as gang activity, drug trafficking, assaults, theft and vandalism. Although the Footscray Police Department was working around the clock to apprehend suspects and deter criminal activities, lack of technology, specifically video surveillance, forced them to be more reactive than proactive when responding to critical events.

According to Brendan O'Mahoney, detective acting sergeant at Footscray Crime Investigation Unit, "We ran a number of operations over the years where we would install covert cameras; so we would put them up and then take them down, but this became very costly in terms of money, time and resources." detective O'Mahoney knew Footscray needed to get Maribyrnong City Council on board to help fund the implementation of a more permanent video surveillance system. He recruited his team and brought forth the case to City Council representatives who recognised the value the surveillance system would offer; not only in terms of increasing safety and deterring crime, but in encouraging more local development and business in the areas.

End-User Needs

It was at this point in time that the Footscray PD compiled and sent out a Request for Proposal (RFP) detailing their high-level requirements for the solution. They offered four main criteria as guidance: 1) the general areas where video surveillance coverage was required; 2) the solution had to able to grow and accommodate the very latest security technologies; 3) the system had to offer 99.9 percent reliability where video would always be available; and 4) the video platform needed to be user-friendly so new officers with little experience on video surveillance could be trained quickly. "We wanted to leave it to the market to propose the best solution that could also keep up with the latest technology," explained detective O'Mahoney. "We prioritized certain requirements and areas of town which needed surveillance coverage and let the integrators suggest both the design and solution."

The Solution

It took SNP and OPS about three months to get Footscray's new stand-alone video surveillance system up and running; a truly impressive feat for a brand new city-wide surveillance system comprising the latest security innovations.

Today, Omnicast manages video feeds from over 35 pole-mounted Axis network cameras spread out across 16 different locations in the suburb. The network cameras connect back to the police station network wirelessly via a Firetide wireless infrastructure mesh network which was chosen for its flexibility and its ability to deliver real-time video at approximately one tenth the cost of a wired system.

Video feeds are then cabled down to an off-the-shelf Dell storage array offering 24TB of storage, and

finally sent to the Omnicast client application, which is installed on two workstations; one in the police station control room and another in the duty room. Omnicast's Failover Directory provides a hot standby to Footscray PD's client connections and security system policies in case of an interrupted connection. Omnicast's Failover Archiving was also incorporated to preserve the communication with the cameras in case of failure and Auxiliary Archiving was used to further strengthen system availability by recording video with different quality and retention time. SNP and Footscray even went one step further to incorporate a revolutionary concept called Video Trickling, made possible by both Axis IP network cameras and Omnicast. Then, Omnicast's Video Trickling feature would ensure that video created is retained in memory, in case the units were offline. When the connection comes back, Omnicast's Auxiliary Archiver resumes recording and the system automatically starts transferring the video of the units that were affected by the connection failure.

Benefits

To date, Footscray PD and Maribyrnong City Council have achieved much more than they expected from their new citywide surveillance system. According to detective O'Mahoney, "Robberies and street offences have drastically decreased since implementing the system".

With one control room primarily being used for after-the-fact investigations and the other for 24/7 manned monitoring; Footscray is able to both actively and passively monitor their surroundings.

Footscray authorities have also been able to apprehend warranted suspects without physical addresses by catching them on cameras and regularly using video footage as supporting evidence in court. This has been facilitated by Omnicast's Bookmark feature where operators are now required to bookmark every event, and write a really brief description of what was going on, along with the unit code that handled the dispute. detective O'Mahoney added, "Later on, we can use the search tool to easily find what we are looking for." SST

A City In Italy Turns To An IP-Based Video Surveillance System To Safeguard Its Artistic Heritage And Ensure Residents Safety

Background

The city of Maddaloni in Italy, also called "the city of twenty cupolas," is renowned for its rich artistic and cultural heritage that goes back to the time of the Normans. Located in the heart of Campania in the province of Caserta, Maddaloni is home to around 40,000 inhabitants.

The city of Maddaloni is committed to ensuring efficient security services for its residents. It required a video surveillance system that would allow the local police to monitor urban traffic, public buildings and historic sites, while respecting the privacy of residents. A solution for monitoring the territory would also serve as a deterrent to illegal activities.

The Solution

The municipal administration of Maddaloni turned to C.E.D.I. Informatica, which was already the city's technical partner. The Caserta-based systems integrator designed and developed an IP-based video surveillance system using network

cameras and video encoders from Axis Communications. The installation includes two video encoders and 11 network cameras located in various areas considered to be at risk.

The Results

The results were positive. The solution fully met the requirements of the customer, as evidenced by their intention to expand the area under surveillance in the future.

Safeguarding historic sites, providing security for residents and managing urban highways

The project designed for the city of Maddaloni aims to safeguard the artistic heritage, protect residents against vandalism and crime, and also improve urban road conditions. It consists of 11 Axis network cameras located outdoors and connected by wireless technology. There are five AXIS Cameras around the area, positioned to give a complete view of the city squares being monitored.

In addition, two AXIS Video Servers/Encoders are located in different buildings. This is the best solution for integrating the six analog cameras already located around the city of Maddaloni into the new IP video surveillance system. The purpose of the video servers/encoders is to facilitate the migration from analog systems to IP systems ideal for video surveillance and remote monitoring. These video encoders receive four analog channels and transmit them using IP.

All buildings are connected by five GHz Wi-Fi bridges, to increase security and reduce interference. The project also includes a hub that serves as a control room and data collection centre, located at the Municipal Police Headquarters, where images are sent by wireless connection and the recordings are archived.

To ensure full compliance with privacy laws, the access to and inspection of the collected data is restricted to officers of the local and state police. The recorded images are stored for three days. The application uses Linux based software, customized by C.E.D.I. Informatica to meet the needs of the customer.

Objectives achieved

The implementation of the video surveillance project has proven to be beneficial to the city of Maddaloni. In addition to detecting serious threats, the cameras installed in public areas serve as a deterrent against assault, theft and vandalism. As well as integrating the existing analog cameras into the new system, the flexibility of the Axis solution will allow future expansion and the implementation of new applications.

"The objective of C.E.D.I. Informatica has always been to satisfy the needs of our customers in every respect. Today, thanks to our strong experience in this sector and the use of reliable and cutting-edge products from Axis, we can say we've accomplished our mission better than ever, and we believe the city of Maddaloni could be the shining example in our book of case studies," said Piero Molinari - C.E.D.I. Informatica. SST

24th YEAR
CPSE - CHINA PUBLIC SECURITY EXPO

ufi Approved Event

THE WORLD'S BIGGEST SECURITY TRADESHOW 115,000m² 1,800 Exhibitors 200,000 Visitors 5,500 Booths

THE 14TH CHINA PUBLIC SECURITY EXPO

Oct 29 - Nov 1, 2013 | SHENZHEN CHINA

www.cpse.com.cn

The CPSE Golden Excellence Award 2013

CPS Forum 2013 - The 10th China Public Security Forum

The Public Security Academic Forum

October
29
SHENZHEN CHINA

Exhibitior partial list

AIRONIX AXIS BOSCH Canon CHANGHONG CSST COSHIP CNB alhua EverFocus FERMAX FUJICA GE Security HIKVISION
Honeywell H3C HUAWEI Infinova Ingersoll Rand JinPeng JSST JC LG Panasonic Phenix Relong SANYO safer SAMSUNG
SONY SIEMENS Skyworth SECOM Shidean Tiandy Tech TAMRON TSINGHUA TONGFANG tyco Fire & Security TCL VIDEOTREC WAPA WRT YAAN ZTE NetView

University In Melbourne Implements A More Flexible Access Control System To Better Suit Its Fluid University Environment

The Customer

The main campus of La Trobe University in Melbourne (Bundoora) is situated in spacious parkland and includes a Wildlife Reserve. This metropolitan campus also houses the main research and teaching facilities of the University, including the Research and Development Park, a world-renowned library, multi-media facilities and a medical centre.

The University covers a vast 330 hectares and incorporates 60 buildings across several campuses in regional Victoria – in Bendigo, Albury-Wodonga, Shepparton, Mildura and Beechworth.

The Challenge

La Trobe University has a particularly strong commitment to international students and collaboration with other education institutions. It leads the International Network of Universities which is a consortium of universities specifically designed to promote student mobility. Currently the University has links with some 250 institutions in more than 40 countries.

This University prides itself on forward thinking to accommodate the needs of staff and students now and in the future and security considerations are no exception. Security on site is comprised of guards, an extensive CCTV camera system and a Gallagher access control with integrated intruder alarm system upon which they rely heavily. The Gallagher system was installed in 1998 and originally controlled six doors in the Eastern lecture theatre.

The Solution

Since then Gallagher system has been installed throughout many of the University's buildings and campuses and a steady technology migration to the latest Gallagher Command Centre software platform has taken place. The University now has 1012 doors across its campuses. Wayne Aldous, security manager – Infrastructure and Operations Division, Security and Traffic Unit - has weighed up the leading access control systems on the market and is confident in their choice. "With on-going software releases and system enhancements the Gallagher access system is proving to be the right product for the University".

The Gallagher system now protects a wide range of facilities including the Physical and Health Sciences precincts, Law and Management buildings, Administration, Computer science labs, and Student Accommodation. The Gallagher system provides a full audit trail of events for reference in the event of criminal activity and OH&S matters.

The Results

"We find the reports powerful and look forward to future developments in this area," Wayne commented. La Trobe University creates reports from the Gallagher system and includes these, plus time stamped video footage as part of incident reports for police as required.

Currently the University has 22 operators with workstation licenses – these operators manage day-to-day cardholder access requirements in their respected departments. The Computer Sciences and Library for instance, manage access control of their own areas independently. The introduction of the latest version of Gallagher's Command Centre software provides La Trobe University staff with significant flexibility and independence in terms of cardholder management and access control. Different areas of the university, for example student accommodation, can independently manage access outside their relevant divisions based on the cardholder's needs.

"One of the most beneficial features

regarding the Gallagher access system is the access group time and date expiry. It means that access can be granted and denied to specific areas in advance of when it is required. We can check whether the access status of students to different areas is enabled, pending, or expired. The ability to provide temporary access means staff do not have to manage access requirements in real time. It has proven very useful," Wayne said.

La Trobe University will also be implementing Gallagher's UltraSec access system to protect and monitor areas where high consequence substances are stored. UltraSec is a high security variant of Gallagher's access system. It achieves superior security through very high levels of system data encryption and monitored communications, using encryption key lengths of 128 bits and 168 bits. UltraSec meets high security requirements determined by the Australian Radiation Protection and Nuclear Safety Agency (a Federal Government agency charged with responsibility for protecting the health and safety of people, and the environment, from the harmful effects of ionizing and non-ionizing radiation).

Interfaces between a range of third party systems and the Gallagher system have been established including to their Digital Video Recording system and to the University's energy management system. La Trobe University has its own power generation capacity and it on-sells the excess energy it generates to the grid. The University is looking to upgrade their CCTV camera system to one that incorporates artificial intelligence in drawing attention to suspicious activity.

There is opportunity to integrate the University's Syllabus Plus resource scheduling system to the Gallagher system via the Syllabus Plus Interface. This will facilitate cost savings and improve efficiencies in resource management.

Wayne added, "The segregation of fundamental components of security is no longer. Today security systems are integrated. You have intrusion detection, door latch monitoring, key position monitoring – the list goes on. Gallagher's access system is proving an ideal integration platform." La Trobe University uses Mifare smartcards providing the ability to implement cashless car parking, and student photocopier and print services in the future. SST

Australian Customs And Border Protection Service Implements Asset Tracking System To Ensure National Security

Background

The Australian Customs and Border Protection Service are responsible for the protection of the Australian community, while supporting legitimate trade and travel. At a time of unprecedented threat levels – illicit drug trafficking, terrorism, people smuggling – Customs and Border Protection manages the security and integrity of Australia's borders, working closely with other government and international agencies, to detect and deter unlawful movement of goods and people across the border.

"Customs and Border Protection plays a vital role in national security, derived from its broader responsibilities at the border and the extensive powers, expertise and technology it brings to bear," said Michael Carmody, chief executive officer, of Australian Customs and Border Protection Service. "Modernization of customs organizations will remain imperative, with the Australian Customs and Border Protection Service motivated by continuing pressure for more sophisticated and integrated processes."

The Challenge

Border protection responsibility lies in the hands of over 5500 Customs and Border Protection employees in over 50 locations around Australia and overseas, and is managed from the Central Office in Canberra.

Protecting the Australian community demands sophisticated intelligence, targeting high-risk aircraft, vessels, cargo, postal items and travellers. It also requires sophisticated tools, including thousands of items of weaponry, protective gear, specialised equipment and vehicles. Effective deployment and management of these tools is vital to assure the safety and security of Customs and Border Protection's officers, and the 22.6 million Australian citizens they serve and protect.

Prior to 2011, Customs and Border Protection maintained a system of separate spreadsheets to track and manage this considerable arsenal. More importantly, the view from Central Office in Canberra lacked immediacy. Lags in reporting times could lead to delays in repairing or replacing critical equipment, or in identifying missing or stolen weapons.

What Customs and Border Protection sought was a fast and easy way to correlate information about the location and status of arms and bulletproof vests with the officers to which they had been assigned. As staff across different locations kept their own spread sheets, Customs and Border Protection needed a solution that could easily deliver accurate and up to date views to Central Office

The Solution

Under Michael Carmody's imperative for more efficient, integrated processes, the Australian Customs and Border Protection Service issued a global tender for an asset tracking system. They discovered that a partnership between Relegen and HID Global best fit their needs.

Relegen specialises in the development and delivery of asset intelligence solutions. The Australian Defence Force has employed Relegen's technology – assetDNA™ – to manage critical assets for over a decade. The similarities between the ADF's and Customs and Border Protection's asset management needs, combined with the flexibility of the assetDNA solution, made Relegen the clear choice around which to build Customs and Border Protection's new system.

The Relegen solution is enhanced by their assetDNA software technology, which enables users to assign

a globally unique identity to each asset. In this case, Customs and Border Protection have opted to use the assets' serial number. This identifier is then carried by Relegen's proprietary assetDNA tagging solution. A third layer of security is added through DataTraceDNA®, a covert security technology from DataDot Technology Ltd. This means that even in the event that the assetDNA tag is removed or destroyed, Customs and Border Protection can still identify the asset as one of their own.

The ability of assetDNA to track each asset uniquely, and in real-time, is made possible by radio frequency identification technology from HID Global. A world leader in the development and production of innovative identification tags and readers, HID provides innovative asset tags and technical support vital to the Customs and Border Protection solution.

HID manufactures asset tags that adhere and function under extreme conditions, resisting impact and vibration, and exposure to harmful elements such as saltwater and chemicals.

Benefits

Relegen and HID are working together to help implement the sophisticated asset tracking system across all Customs and Border Protection locations. This includes the tagging of each of the armaments and critical assets in each agency, as well as training for all Customs and Border Protection personnel.

The result will be a comprehensive system that gives Customs and Border Protection a real-time view of

all assets deployed and in inventory, empowering the Central Office to make critical decisions based on the latest information at-hand. It will also mean greater safety and security for Customs and Border Protection officers. Officers can perform their duties, confident they have been issued the correct equipment, and be assured that it is in proper working order. In addition, the new system minimizes the risk that weapons may be stolen or remanufactured.

The new system will also enable optimization of asset use. Customs and Border Protection can now identify each asset's progress through its lifecycle, and identify specific assets in need of immediate repair or replacement.

Customs and Border Protection will recognise significant productivity enhancements in staff time spent mustering their formidable arsenal.

Going forward, the Customs and Border Protection asset-tracking system provides a model for any organization managing operation-critical assets, in routine or emergency response situations.

Worldwide, police forces, fire departments, emergency medical teams, hospitals, and other organizations are employing solutions from Relegen and HID Global to respond quickly and comprehensively in emergencies, provide better safety for their employees, and drive the performance of their mission critical assets more effectively. SST