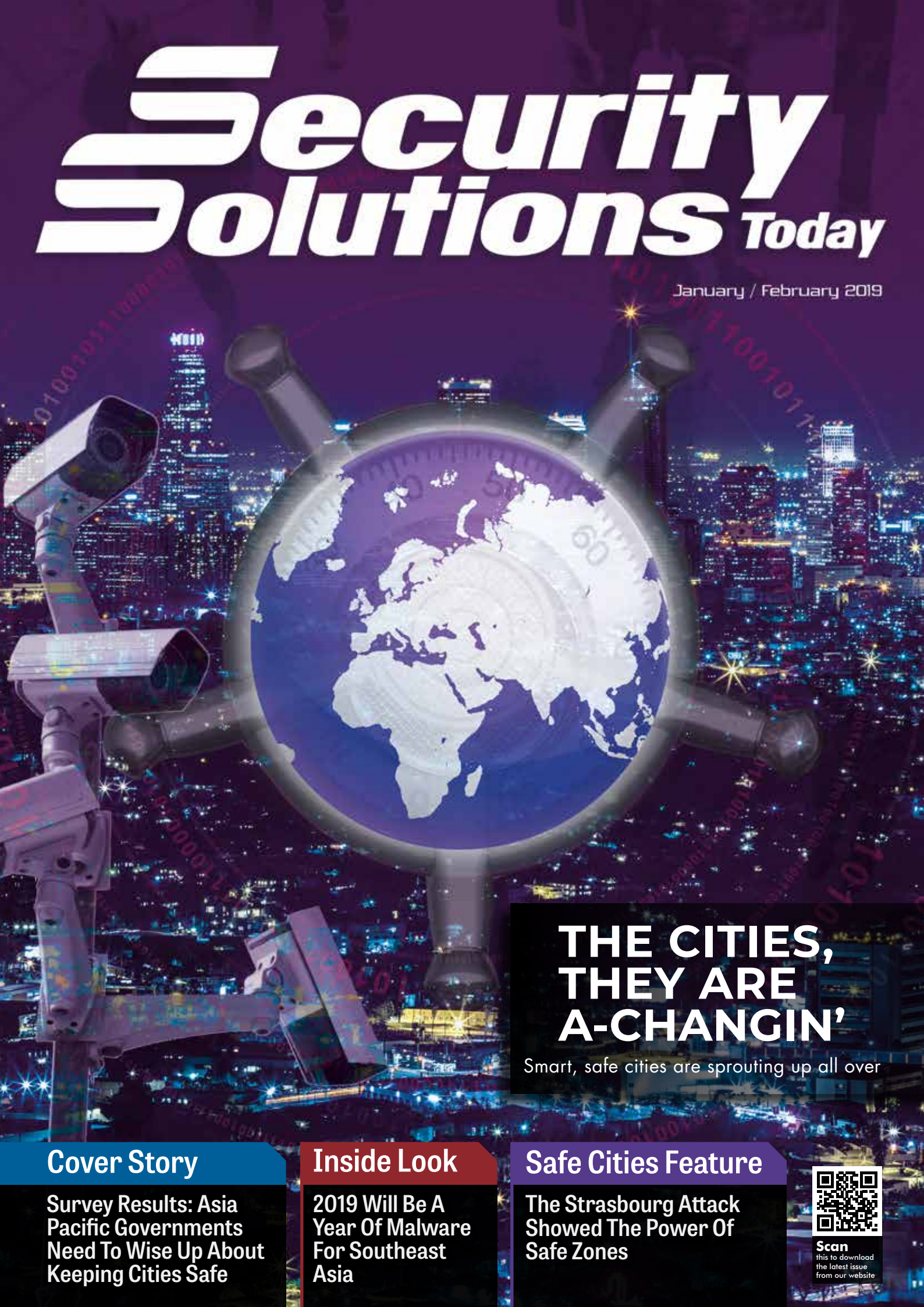
Security Solutions Today

January / February 2019



THE CITIES, THEY ARE A-CHANGIN'

Smart, safe cities are sprouting up all over

Cover Story

Survey Results: Asia Pacific Governments Need To Wise Up About Keeping Cities Safe

Inside Look

2019 Will Be A Year Of Malware For Southeast Asia

Safe Cities Feature

The Strasbourg Attack Showed The Power Of Safe Zones

Scan this to download the latest issue from our website

CE FC ISO 9001:2000

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

Smart City • Smart Living

600+ Exhibitors

32,000+ Buyers

Group Pavilions from Mainland China, Canada, India and Korea

See more:

Smart City Solutions

- Smart Economy
- Smart Government
- Smart Living
- Smart Mobility
- Smart People

Other Highlighted Zones

- Digitial Infrastructure
- Digitial Marketing & E-Commerce
- Enterprise Solutions
- Home-grown Innovations
- Retail Technologies
- Smart Devices & Accessories
- Startup

Daily Theme

- AIoT: Next-Gen Connectivity
- Data as Currency of the Future
- Reinventing Business with Smart Solutions
- Smart Living Powered by Technologies

Concurrent Events

15-16 / 4 / 2019
Internet Economy Summit

13-16 / 4 / 2019
HKTDC Hong Kong Electronics Fair (Spring Edition)

HKTDC
International ICT Expo

ufi Approved International Event

Fair Dates: 13-16 April 2019
Venue: Hong Kong Convention and Exhibition Centre

Register Now for FREE e-Badge

Web: ictexpo.hktdc.com/ex/09
Wap: hktdc.com/wap/ict/T119
App: HKTDC Marketplace

Admission: Free Admission for business visitors aged 18 or above only

Exclusive Travel Incentives for Overseas Business Visitors*

For query, please contact HKTDC Singapore office at: singapore.office@hktdc.org

IN THIS ISSUE

The Most Satisfying Phrase Heard after a Vehicle Attack...

"Defended by **DELTA**"

For advanced vehicle access control systems that stop terrorists dead, contact the company that started the industry. Worldwide security specialists depend upon Delta Scientific for crash-rated systems that include surface mounted and high security barricades, bollards, beams, portable barriers, sliding gates, guard booths and parking control systems. You can see our full product line by visiting our website at **www.deltascientific.com**. Get *"Defended by Delta"* today.

*You asked for it; we made it! The lighter weight, DC-operated, K4 certified Delta **DSC1500** portable beam barricade is available for purchase today.*

DELTA

Visit **www.deltascientific.com** for details and specifications.
GSA 47QSWA18D003B ▲ **1-661-575-1100** ▲ **info@deltascientific.com**

CONTACT

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

EDITOR
Michelle Lee
(sst@tradelinkmedia.com.sg)

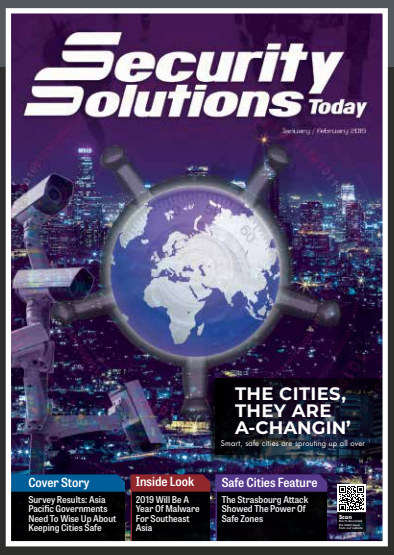
GROUP MARKETING MANAGER
Eric Ooi
(eric.ooi@tradelinkmedia.com.sg)

MARKETING MANAGER
Felix Ooi
(felix.ooi@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)



Images/Vectors Credit: Pixabay.com / Freepik.com

Designed by Siti Nur Aishah

SECURITY SOLUTIONS TODAY
is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
ISSN 2345-7104 (Print)

Printed in Singapore by Refine Printing Pte Ltd

ANNUAL SUBSCRIPTION:

Surface Mail:

Singapore	- S$45 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:

Malaysia/Brunei	- S$90
Asia	- S$140
Japan, Australia, New Zealand	- S$170
America/Europe	- S$170
Middle East	- S$170

ADVERTISING SALES OFFICES

Head Office:
Trade Link Media Pte Ltd *(Co. Reg. No: 199204277K)*
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 1523, 6846 8843, 6842 2581
Email (Mktg): info@tradelinkmedia.com.sg

China & Hong Kong
Iris Yuen
Room 1107G, Block A,
Galaxy Century Building
#3069 Cai Tian Road,
Futian District
Shenzhen
China
Tel : +86-138 0270 1367
sstchina86@gmail.com

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

THE PERFECT BRIDGE BETWEEN
PAST & PRESENT

UPDATING YOUR SURVEILLANCE SYSTEM DOESN'T MEAN YOU HAVE
TO PART WITH DATED COAX INFRASTRUCTURE...AND SING THE BLUES.
ALTRONIX EoC PRODUCTS ARE THE SIMPLE, COST-EFFECTIVE WAY TO UPGRADE TO IP.

NOW, THAT'S MUSIC TO EVERYONE'S EARS!

Altronix

eBridge™ PLUS

MADE IN THE U.S.A. ALTRONIX.COM LIFETIME WARRANTY

COMING SOON...

MARCH

IFSEC Southeast Asia 2019

Date: 19 - 21 March 2019
Venue: Malaysia International Trade And Exhibition Centre (MITEC), Kuala Lumpur, Malaysia
Organiser: UBM Malaysia
Telephone: +603 9771 2688
Website: www.ifsec.events/kl
Email: info-my@ubm.com

MARCH

IoT Asia 2019

Date: 27 - 28 March 2019
Venue: Hall 1, Singapore EXPO, Singapore
Organisers: Singex Exhibitions & Singapore Industrial Automation Association (SIAA)
Telephone: +65 6403 2100
Website: www.internetofthingsasia.com
Email: sales.iotasia@singex.com

APRIL

ISC West 2019

Date: 9 - 12 April 2019
Venue: Sands Expo, Las Vegas, NV, USA
Organiser: Reed Exhibitions
Telephone: (800) 840-5602
Website: www.iscwest.com
Email: inquiry@isc.reedexpo.com

MAY

Secutech 2019

Date: 8 - 10 May 2019
Venue: Taipei Nangang Exhibition Center, Taipei, Taiwan
Organiser: Messe Frankfurt New Era Business Media Ltd, Taiwan Branch
Telephone: +886 2 8729 1099
Website: www.secutech.com
Email: services@secutech.com

APRIL

International ICT Expo 2019

Date: 13 - 16 April 2019
Venue: Halls 3F-G, Hong Kong Convention and Exhibition Centre, Hong Kong
Organiser: HKTDC
Telephone: +852 1830 668
Website: www.hktdc.com
Email: smecentre@hktdc.org

JUNE

IFSEC Philippines 2019

Date: 13 - 15 June 2019
Venue: SMX Convention Centre, Pasay City, Metro Manila, Philippines
Organiser: UBM Exhibitions Philippines, Inc
Telephone: +63 2 551-7718 / 839-1306
Website: www.ifsecphilippines.com
Email: info-ph@ubm.com

JUNE

IFSEC International 2019

Date: 18 - 20 June 2019
Venue: ExCeL London, London, UK
Organiser: UBM plc
Telephone: +44 (0) 20 7921 5000
Website: www.ifsec.events/international/
Email: ifseccustomerservice@ubm.com

JUNE

BMAM Expo Asia 2019

Date: 27 - 29 June 2019
Venue: IMPACT Exhibition Center, Hall 6, Bangkok, Thailand
Organiser: IMPACT
Telephone: +66 8 6561 3344 / +66 2833 5111
Website: www.bmamexpoasia.com
Email: radcharinn@impact.co.th

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

xPortalNet HS

High Security System Software

- 20 Digits (Full DesFire 64-bit CSN and Card ID)
- DesFire Security Profile Configuration
- Alarm Monitoring & Lift Controller
- CCTV Integration
- Visitor Management System (VMS)
- Dynamic Floor Plan for Real-Time Monitoring
- Web Server Support

Projects


Commercial / Complex


Factory


Condominium


Plato DesFire Reader

500+ doors access & security system on SQL Server for factory and many more...

1300-88-3925 or enquiry@microengine.net

www.microengine.net


Our Office


Service Centre

REG No. 749921389

EDITOR'S NOTE

Dear esteemed reader,

The Smart City drive is one of the most important movements happening in the world today.

By making cities smarter, nations are also making their cities safer and better to live in. For example, authorities could install hotlines and panic buttons around the city that would allow law enforcement to respond quickly to an emergency. They could also use city-wide CCTV cameras to identify dangerous individuals before a crime is committed or nab them quickly once they've committed the crime.

Using modern day communication technologies to enhance operations or to innovate new services also makes cities more efficient, more connected and more cost-effective. As a rule, citizens in smart cities enjoy greater convenience and comfort and overall higher quality of life.

It is a movement that affects a huge number of people in the world. Already 55% of the world's population live in cities. This is expected to increase to 68% by 2050. The movement of people from rural to urban areas combined with population growth could add another 2.5 billion people to cities by 2050, with close to 90% of this increase taking place in Asia and Africa.

This translates to enormous opportunities for technology firms.

Smart cities are built upon technology. Smart cities means opportunities for companies in digital government services, efficient energy use and renewables, water and waste management, transportation, education, healthcare and more.

This movement is so powerful, we have devoted this issue to the different technological developments that make it possible for cities to create safer cities.

Lastly, from everyone at Security Solutions Today, a wholehearted thank you for your support in 2018. It has been a year of exciting developments and breakout news on the technological front and we enjoyed bringing all of that to you.

We look forward to delivering more insights, more news and more thought-provoking stories in the year ahead. See you in 2019!

Michelle Lee

Editor

secutech

8 – 10 May 2019, Taipei, Taiwan
www.secutech.com

Bringing Asia's security, IoT & AI ecosystem together under a single roof

7 Smart solution pavilions

- Smart Retail
- Smart Hotel
- Smart Factory
- Smart Parking
- Smart Healthcare
- Smart Community
- Smart Transportation

7 Thematic zones

1. AI+Software Zone
2. RFID Applications Zone
3. LPWAN Applications Pavilion
4. Smart Lock Pavilion
5. Cybersecurity Pavilion
6. Police Equipment Zone
7. Smart Factory & Industrial Safety

MOBILITY powered by Secutech

- Asia's leading fair for Intelligent Transport Systems
- Showcasing solutions that range from smart road, smart railway, smart parking to fleet management

SMART BIoT SOLUTION powered by Secutech

- Asia's first event for the 'Smart Building Internet of Things'
- Focusing on four major applications: residential & community, hospitality, nursing facility and commercial building

fire & safety powered by Secutech

- Highlighting a full range of solutions from natural disaster monitoring, safe city, industrial safety to personal safety
- Advanced smart disaster prevention applications

info security powered by Secutech

- Revealing the latest cybersecurity solution for the IoT

messe frankfurt

World's First 360-Degree Explosion-Proof Environment Camera

Oncam has released the only 360-degree single-sensor camera with an explosion protected housing.

The ExD Explosive Environment camera range is designed for use in potentially explosive atmospheres and harsh and hazardous environments. It is certified for demanding environments in markets such as oil and gas production and refineries, power and utilities, wastewater treatment, grain handling and storage and other hazardous materials facilities.

The camera housing is manufactured from stainless steel 316L. Its IP66, IP67 and IP68 ratings make it resistant to the harshest environment conditions. The housing also prevents water and dust ingress.

To provide the best possible protection for hazardous areas, cameras installed as part of a comprehensive security plan must guarantee the appropriate level of safety and adhere to stringent regulations. The Oncam ExD camera range ensures safety by containing electrical sparks that can ignite and potentially cause significant harm to both people and assets.

Designed to withstand the toughest conditions, the camera's flame-proof housing has obtained various certifications across the globe:

- IECEx — The International Electrotechnical Commission certifies the ExD camera range at a "high" protection level, with the housing protecting an inner explosion from spreading into the air surrounding it.
- ATEX — The ATEX certification approves the use of the ExD in applicable hazardous environments (excluding mining) within the European Union.

"The new ExD camera range is the perfect addition to our specialist

cameras, which are targeted toward markets that require robust equipment to provide video capture in extreme conditions," said Jon Marsh, VP Product, Oncam. "The expanding list of certifications for these cameras, along with Oncam's attention to the needs of these markets, allows us to provide high quality 360-degree coverage and intelligent video that increases situational awareness and protects critical assets from threats." SST

Market-Leading Intrusion Detection And Location Solution Gets An Upgrade

In 2017, Ava released the Aura Ai-2 fibre optic detection controller, which offers superior intrusion detection location accuracy together with extended range performance.

The market leader in the provision of risk management services and technologies has now upgraded the Aura Ai-2. With the upgrades, Aura Ai-2 easily outperforms its competitors in distance and accuracy.

The controller now offers monitoring of optical distances of 80km for perimeter fence detection or 110km for pipeline or covert buried detection.

Accuracy has also been enhanced. The system can now pinpoint an intrusion down to within +/- two metres on a fence-mounted application. The controller is also able to cover different applications simultaneously, for example fence mounted and covert buried detection. This essentially means you get two units in one, saving on both procurement and operational costs.

The Aura Ai-2 controller works by pulsing laser light along optical fibre cables connected to each of its two detection channels. Dependent on the application these cables are either laid adjacent to a pipeline, attached to a perimeter fence or buried along a perimeter boundary. Minute disturbances cause changes in the scattered light and the Aura Ai-2 controller automatically analyses this reflected light to detect, locate and report disturbances.

continued on page 12

Advanced optical signal processing algorithms, combined with artificial intelligence, accurately and reliably analyse the reflected light to discriminate between intrusions and other causes of disturbance. This significantly reduces nuisance alarms whilst arming operators with full awareness of any situation. When wired in a redundant loop configuration the two-channel controller provides cut resilience and continues to provide detection in the event of deliberate or accidental cable cut.

The Aura Ai-2 now has an industry-leading power budget of 13.5 dB. Optical power budget is the maximum allowable optical signal loss the system can tolerate while still maintaining proper operation. As it utilises the sensitivity of fibre optic technology, Aura Ai-2 is also perfect for monitoring fibre optic communications networks. The system can monitor for tapping and tampering by connecting spare (dark) fibres inside each network cable to Aura Ai-2. Network cable disturbances - including removal of protective layers, attempted tapping or cable movement - will be instantly detected and generate an alarm indicating the location.

Aura Ai-2 is the ideal protection solution for critical infrastructure such as high-risk oil and gas pipelines and chemical or water pipelines as they traverse often remote and inhospitable locations. It is also perfect for protecting long boundary perimeters alongside railway lines, airports and ports. SST

Magecart Attacks May Cost Online Shoppers, Card Companies US$500 Million A Month

Since the recent cyber attacks on Ticketmaster and retailer Newegg, international cybersecurity company CyberInt has identified an additional 32,000 smaller online retailers who have also been hit with similar tactics, techniques and procedures (TTP) exploiting vulnerabilities in the online commerce platform.

CyberInt provides holistic end-to-end protection to digital businesses in retail, ecommerce, gaming and financial industries.

The attack has been dubbed Magecart.

The new malware scrapes data from online stores and commerce pages and uses the data to "skim" shoppers' credit card details from legitimate online checkout pages. In all cases, retailers and their customers were not aware that anything untoward had occurred.

Based on the expected volume of stolen credit card details, it is safe to assume the organised criminal gangs concerned could be making as much as US$11.4 million a month out of these hacks alone, although the cost to their victims is many times more.

The average cost of a card stolen online for the customer and card issuer is almost US$1,100. In cases identified in one month alone by CyberInt, point-of-sale scraping of the 32,000 retailers recently hit could cost customers and card companies roughly US$500 million a month, with this figure likely to grow substantially as the shopping season starts in earnest.

Whilst there is no indication as to what those behind the attacks are doing with their huge haul of stolen payment card data, data is often resold and exchanged through a buoyant underground "carding" market.

Credit card details retail on the Dark Web for around US$25 each.

"In all the attacks we have monitored, the TTP used by the cyber criminals resemble those used by Russian organised criminal gangs," said CyberInt Lead Researcher, Jason Hill.

The reason for the concentration of organised criminal gangs inside Russia is that cyber crimes perpetrated on enterprises and individuals outside the country are not prosecuted inside Russia. This has given the gangs a free hand to develop and deploy sophisticated malware such as Magecart in the run-up to the 2018 shopping season.

Investigations into the TTP employed by this threat, such as analysis of the JavaScript payloads used to scrape and exfiltrate data, has allowed both the identification of further victims and the command and control infrastructure. The differences among these recent activities and those identified in other campaigns suggest multiple threat actors are conducting similar operations.

Given the apparent success of the attacks thus far, it is likely that more clusters of TTP and potential threat actor profiles will continue to evolve.

"Small retailers are particularly vulnerable as they are often a soft target for organised criminal gangs. We expect that the number of retailers targeted will continue to grow," said CyberInt CEO Amir Ofek.

Sophisticated detection and cyber analytics are now the only effective counter-measures for retailers to adopt. SST

IFSEC
PHILIPPINES

SECURITY • FIRE • SAFETY

13 - 15 JUNE 2019

SMX CONVENTION CENTRE
PASAY CITY, METRO MANILA

Organised By

UBM

THE LEADING
SECURITY, FIRE & SAFETY
EVENT IN THE PHILIPPINES

EMPOWERING THE PHILIPPINES TO BE THE SAFER NATION BY PROVIDING GLOBAL INNOVATION AND EXPERTISE TO THE EMERGING TRENDS AND SERVICES IN SECURITY, FIRE AND SAFETY MARKETS.

WWW.IFSECPHILIPPINES.COM

@IFSECPHILIPPINES #IFSECPHILIPPINES IFSECPHILIPPINES

Pelco 4K Video Camera Delivers In Challenging Environments

Pelco has released a 4K video camera that provides high-definition, crystal clear footages in challenging environments.

GFC Professional 4K camera delivers continuous 8 MP resolution details at 30 frames per second - amounting to four times the resolution of 1080mp – even with large, fast-moving crowds of people or vehicles and under difficult, unpredictable light conditions. This makes the camera particularly suited for sites like airports, seaports, casinos, stadiums and roadways.

The enhanced resolution gives operators highly accurate coverage of a large area as well as the ability to zoom in for a closer look at important details like a face or a license plate.

The GFC was developed with an eye towards versatility and flexibility. It is built to withstand vandalism, sabotage attempts and extreme temperatures. Due to its IR illuminator, it delivers detailed images even in total darkness, and tests show that it offers 5% to 9% higher Wide Dynamic Range than other 4K cameras.

It is also cost-effective: the H.265 video recording and Pelco smart compression keeps recording and storage costs low. SST

Altronix Is Now Lenel Factory Certified

Altronix Corp. has received Lenel factory certification and joined the Lenel OpenAccess Alliance Program (OAAP).

Altronix's LINQ technology interfaces with the OnGuard access control system and facilitates the remote monitoring and reporting of power diagnostics. These alerts minimise system downtime and eliminate unnecessary and costly service calls.

By integrating with the OnGuard access control platform, Altronix is now able to provide its customers with a seamless interface for their Altronix products and their OnGuard system.

"Altronix has completed required factory testing at Lenel to validate the functionality of its interface to OnGuard. This provides users with a single software platform to monitor power supply status, receive alert messages, and manage settings at multiple sites with ease," said John Marchioli, OAAP Product Management, Lenel.

LINQ enables users to monitor power/diagnostics and receive emails and alert messages while managing the settings of Altronix products with web-based management capabilities from OnGuard Alarm Monitoring stations or anywhere there's a network connection. Employing an intuitive user interface, LINQ Dashboard allows users to manage multiple sites with ease, regardless of the number of monitored devices. SST

IFSEC
SOUTHEAST ASIA
KUALA LUMPUR EDITION
SECURITY • FIRE • SAFETY

19 - 21 MARCH 2019

MALAYSIA INTERNATIONAL TRADE AND EXHIBITION CENTRE (MITEC), KL

Part of the Super 8 Series of Events

ASEAN SUPER 8

SECURITY IS **CRITICAL**

IFSEC IS ESSENTIAL

PRE-REGISTRATION IS NOW OPEN

Organised By

UBM

WWW.IFSEC.EVENTS/KL
WWW.SUPER8ASEAN.COM

@IFSECSEA #IFSECSEA

IFSEC Southeast Asia

Suprema ID Launches World's Slimmest Fingerprint Scanner

Suprema ID, a leading global provider of biometrics and ID solutions, has launched the world's slimmest fingerprint authentication scanner with FBI FAP30 certification.

The new FAP30 comes in a robust IP65-rated dust and waterproof structure with an ultra-slim optical sensor. It features proprietary advanced LFD (Live Fingerprint Detection) technology to prevent spoofing frauds.

The FAP30 fingerprint scanner maintains the highest FBI PIV/FIPS201 standards and mobile ID FAP30 certification, and enables users to capture high quality fingerprints in harsh environments and under direct sunlight of up to 100,000 LUX. It has been designed to provide the best reliable fingerprint authentication performance across dynamic environments, such as outdoor and mobile situations.

Suprema has a worldwide sales network in over 130 countries and is one of the world's top 50 security companies. SST

Counter UAS Sensors Integrated Into Light Armoured Vehicle

MyDefence Communication has integrated counter Unmanned Aerial System (UAS) technology into vehicle platforms for military forces. It is the first fully integrated counter UAS solution available for mobile platforms with support for third-party battle management systems.

With the integration, military operators can now effectively detect and defeat enemy drones used for reconnaissance or as weapon delivery systems.

MyDefence worked closely with General Dynamics Land Systems on the mission to arm the military with on-the-move capability to detect and defeat drones. MyDefence specialises in developing sensors and effectors for military customers to mitigate the threat of malicious drones.

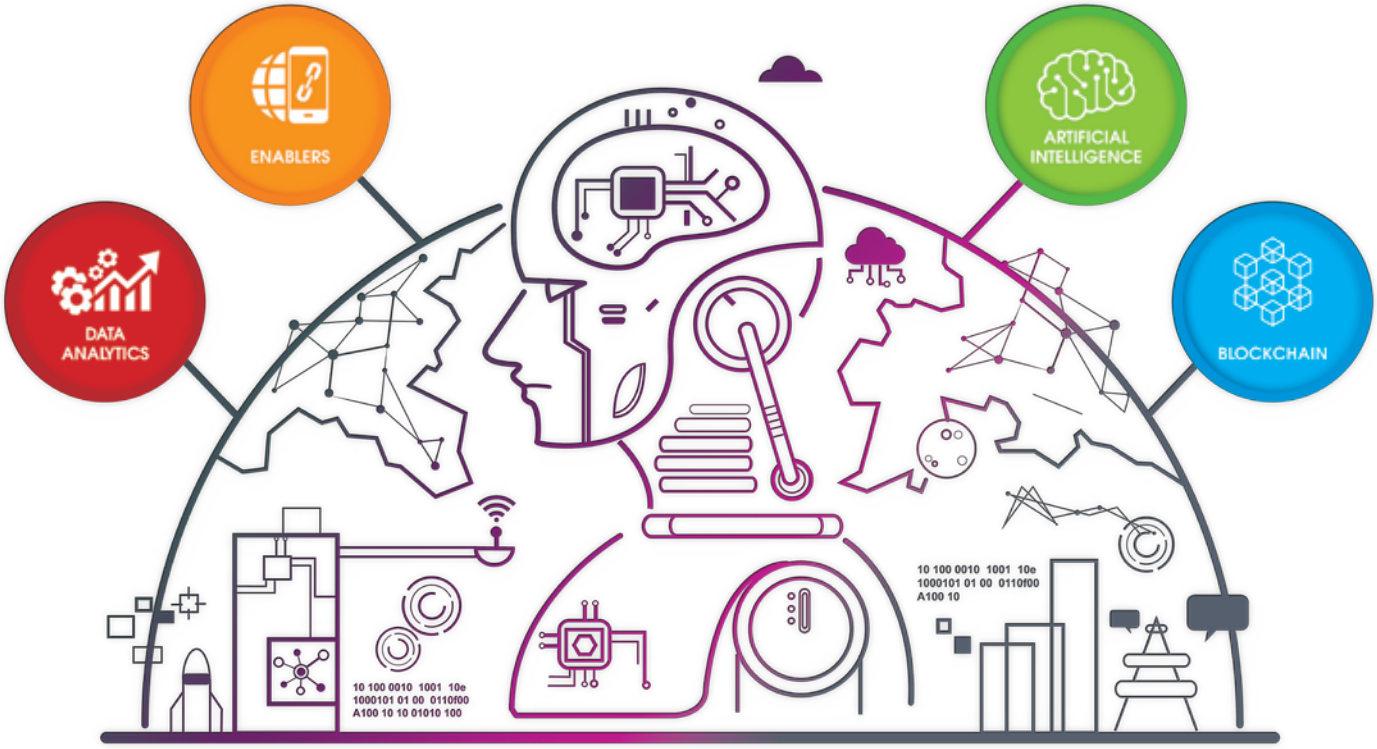
The platform can detect drones using RF technology and defeat threats using smart jamming. The solution can be effortlessly integrated with third-party battle management systems (BMS). Using a standard tactical link, the mobile platform can also communicate and provide feedback to any remote command and control system to impart greater situational awareness and enhance battlefield effectiveness.

Integration testing first began in 2017. The platform has since evolved and the Counter UAS solution can now be fully integrated into any vehicle platform, providing military operators with the flexibility and scalability they need. SST

IoT ASIA

27-28 March 2019
Hall 1, Singapore EXPO

INTERNATIONAL EXHIBITION & CONFERENCE ON THE INTERNET OF THINGS
TRANSFORMING BUSINESSES, GOVERNMENT AND SOCIETIES



Artificial Intelligence Blockchain Data Analytics Enablers Data Analytics Blockchain

BUILDING VALUE CHAINS

SMART CITIES // INDUSTRIAL IoT

Enablers Artificial Intelligence Data Analytics Blockchain Artificial Intelligence Data Analytics

ENABLERS Artificial Intelligence Data Analytics Blockchain Data Analytics Blockchain Artificial Intelligence Data Analytics Blockchain **ARTIFICIAL INTELLIGENCE**

Artificial Intelligence Data Analytics Enablers Blockchain Data Analytics Artificial Intelligence Data Analytics Enablers

DATA ANALYTICS Data Analytics Blockchain Artificial Intelligence Blockchain Artificial Intelligence Data Analytics Enablers **BLOCKCHAIN**

Artificial Intelligence Data Analytics Blockchain Data Analytics Artificial Intelligence
Blockchain Artificial Intelligence Data Analytics Enablers Data Analytics
Artificial Intelligence Data Analytics Blockchain Data Analytics

Gain key insights from best practices and case studies from Industry Leaders.

REGISTER NOW!

www.internetofthingsasia.com • #iotasia

Organised by

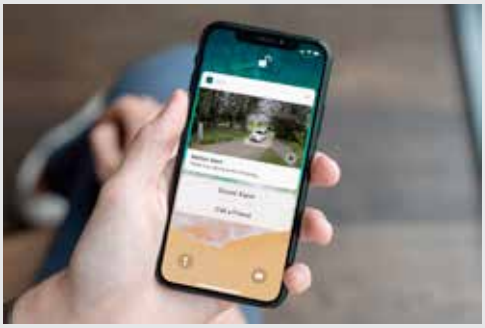
SiAA SingEx

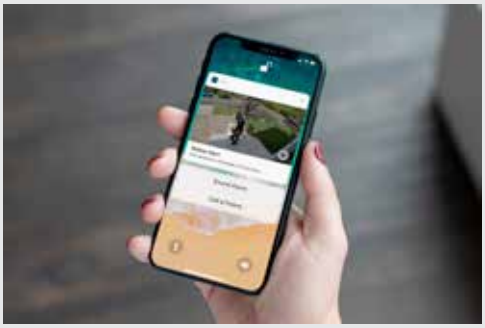
Industry Accolades

ufi Winner of the Marketing Award 2016

Arlo's Smart Video Surveillance Service Plans For Homes Now Available In Singapore

Arlo Technologies, Inc. has launched the Arlo Smart service plans for the Arlo family of smart cameras in Singapore.





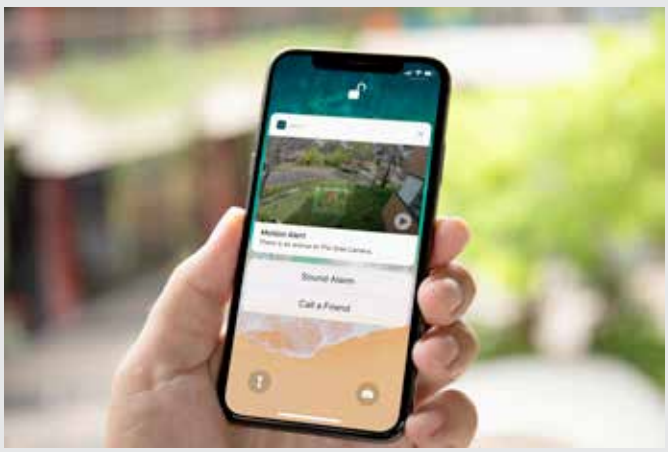
An award-winning market leader in connected cameras, Arlo offers new Arlo Smart subscription service plans that utilise intelligent algorithms and smart analytics to deliver advanced personalisation.

The plans provide users with the most responsive way to monitor their home. From intelligently learning about notification preferences to reducing 'false positive' alerts, the plans boast industry-first recognition features allowing users to differentiate new camera subjects such as animals, vehicles and packages, while suppressing unwanted alerts.

Using advanced algorithms, Arlo cameras can learn to understand what they see, reducing the number of false notifications from normal everyday movement. Smart features such as Person Detection and Cloud Activity Zones allow users to define motion zones and filter out false notifications like the neighbour's cat running along the fence or trees swaying in the wind. The Rich Notifications feature enables users to see what Arlo sees from the smartphone lock screen without having to launch the app to view videos.

With the help of new computer vision technology, Arlo Smart further informs users about what triggered their camera to begin recording. These insights on detected activity allow users to personalise alerts while filtering out false notifications. Arlo Smart users will be able to tailor notifications to their liking, ensuring they are notified when their Arlo camera, for example, sees a package being delivered, a vehicle passing by a specific area, or an animal wandering near the premises.

Arlo Smart service plans are available for purchase for every Arlo camera either through the Arlo web portal or Arlo app. The plans also extend the availability of cloud recordings up to 60 days. They start at just SG$3.99 per camera per month, or SG$11.99 per month for the Premier subscription for up to 10 cameras. Annual subscriptions are also available. Arlo is also offering new subscribers a one-month free trial of the Arlo Smart Premier plan. SST

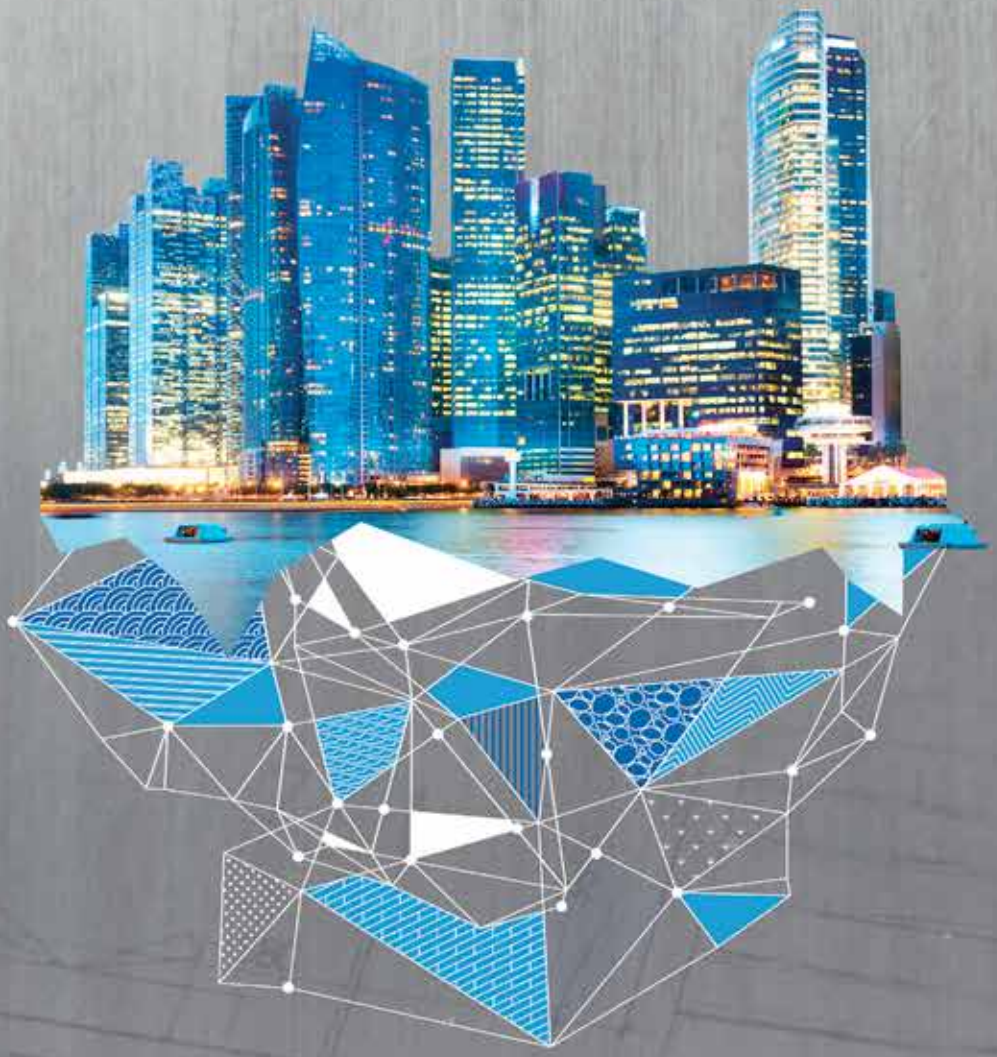


27-29 JUNE 19

IMPACT Exhibition Center, Hall 6, Bangkok, Thailand

BMAM EXPO ASIA 2019

THE BUILDING & FM EXPO



5,000 Sq.m.
Exhibition space

150
Exhibitors

4,000+
Qualified visitors

Book Your Stand
Now!

Contact: Ms. Radcharin Nuttayakul (Tucky)
M: +66 (0)8 6561-3344 T:+66 (0)2 833-5111 E: radcharinn@impact.co.th

Follow us on
BMAM Expo Asia

Organizer
IMPACT MUANG THONG THANI

Samsung Partners Telco Singtel To Secure Homes

Samsung Electronics Singapore is partnering Singapore telco Singtel to offer a new home monitoring video service called SmartCam.

The SmartCam service comes with the SmartThings Camera and 14 days of cloud storage.

With the High-Definition SmartThings Camera, homeowners enjoy detailed clarity for their monitoring and security needs throughout the day and night. The HD Wi-Fi enabled camera also provides homeowners with a live streaming service that they can access anywhere, anytime.

Advanced motion sensors will send homeowners alerts on unexpected activity in their homes.

Homeowners can also choose to turn on connected devices when motion is detected. Smart speakers can be set as siren alarms while smart lights will be turned on as an alert to any potential home intrusion. Consumers can also review these motion-triggered video clips easily on the Samsung SmartThings App to ensure that their homes are safely secured with the extensive cloud storage provided by the new SmartCam service.

Not only can consumers monitor their homes, but they can also have full control of their homes even on the go with the Samsung SmartThings Ecosystem. By connecting the SmartThings Camera with Samsung SmartThings Sensors, consumers will be able to easily check on guest arrival and open the door for visitors via the digital door lock even when they are not home.

"Consumers are living in a fast-paced society with busy schedules, leaving them with limited time to keep track of the happenings at home," said Lee Jui Siang, President, Samsung Electronics Singapore. "With the new SmartCam's real-time video home monitoring system, Samsung hopes to provide enhanced security and monitoring of the young and elderly at home. It allows consumers peace of mind while they attend to their busy schedules."

SmartCam is exclusively available at all Singtel Shop. Prices start from S$8.90 a month for a two-year contract. SST

Singapore Gives Financial Sector S$30 Million To Up Cybersecurity Capabilities

On December 3, the Monetary Authority of Singapore announced a new S$30 million Cybersecurity Capabilities Grant to strengthen the cyber resilience of Singapore's financial sector and help financial institutions develop local cybersecurity talent.

The grant will support the development of advanced cybersecurity functions in Singapore-based financial institutions. Examples of cybersecurity functions that could qualify for the grant are security operations, cyber threat surveillance and intelligence gathering, computer forensics, malware research and analysis and cyber threat hunting.

The grant will co-fund up to 50% of qualifying expenses, capped at S$3 million. The grant can be used by financial institutions to establish their global or regional cybersecurity centres of excellence in Singapore; and by financial institutions with key global or regional cybersecurity functions and operations in Singapore to expand and deepen their cybersecurity capabilities locally.

The grant will also encourage Singapore-based financial institutions to upskill their local workforce through cybersecurity-related training programmes. This will help attract more cybersecurity professionals and expand the local talent pool in the financial sector.

"The Singapore financial sector has made significant progress in recent years in building up cyber resilience and managing cyber risk. But the cyber threat landscape continues to evolve and we have to constantly strengthen our cyber capabilities," said Tan Yeow Seng, Chief Cyber Security Officer at MAS.

Applications for the grant are now open. SST

4K Wire-Free Security Camera With Widest Viewing Angles

Arlo Ultra delivers next-generation level of protection with 4K Ultra HD resolution and one of the widest viewing angles in the market.

Among the features of Arlo Ultra: 4K Ultra HD resolution with high dynamic range (HDR), integrated spotlight with colour night vision, 180-degree viewing angle, dual, noise-cancelling microphones and advanced image processing.

With a new 4K image sensor with HDR image processing, Arlo Ultra is capable of capturing and outputting 4K video quality from the lens to the user. This feature not only adds additional detail and clarity to videos but also allows users to zoom in on video clips to uncover critical information such as license plates, clothing or other telling details in suspicious activities.

Meanwhile its expansive panoramic 180-degree diagonal field of view offers one of the widest viewing angles in the wire-free security camera industry, handing users more flexibility in the placement of their camera for property, home or business monitoring.

In addition, Arlo Ultra includes an integrated spotlight that can illuminate the night with a powerful LED light, giving users the ability to see colour in the dark rather than the common black and white night vision.

Arlo Ultra also takes audio quality to the next level with clearer and more natural recorded conversations. Designed with dual microphones, Arlo Ultra produces two-way audio with advanced noise cancellation that can minimise background noise and accentuate foreground audio such as voices.

Leading network connected camera maker Arlo fashioned Arlo Ultra as a sleek, compact device for both outdoor and indoor use. With a fast and easy wire-free setup and weather-resistant design, Arlo Ultra cameras can be installed nearly anywhere outdoors or indoors. The newly designed magnetic mount allows users to conveniently mount their camera from ceilings, walls and eaves or place on tables and counter surfaces.

Arlo Ultra also includes a one-year subscription to Arlo Smart Premier, giving users an intelligent smart home security experience powered by Arlo's AI and computer vision technologies.

Arlo Ultra represents major advancements in video, audio, software, AI and computer vision capabilities, said Brad Little, Vice President and Managing Director, Arlo Technologies, APAC.

Arlo Ultra is slated to be available in Singapore in the first quarter of 2019. SST

Singapore-Listed Companies Among The Least Exposed To Cyber Threats Globally

According to the latest Cyber Exposure Index by Cyber Intelligence House, 70% of Singapore-listed companies have little or no exposure to cyber threats.

This compares favourably with the 45% global average clocked across stock market indices by 11 countries.

With 481 out of 677 Singapore-listed companies showing no identified exposure risks between October 2017 and October 2018, and only 28 companies (4%) deemed to be in the high risk category, Singapore ranks third in low average exposure score, after Indonesia and Hong Kong.

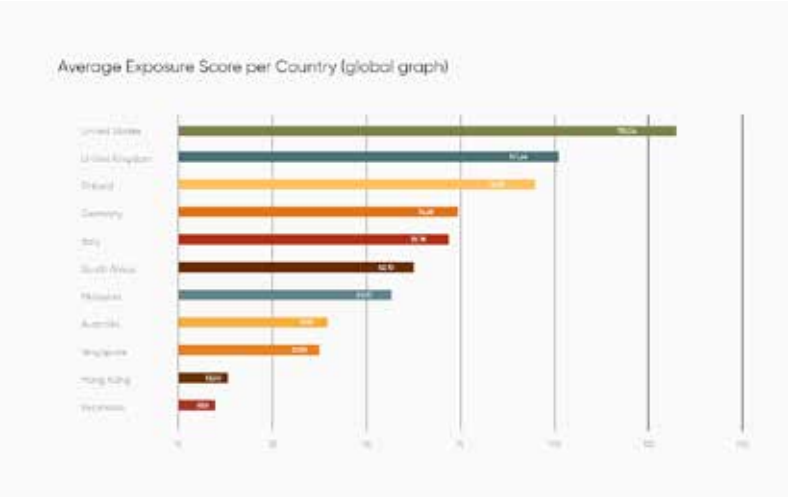
Cyber Exposure Index is the world's first proprietary global scoring system that evaluates exposure of listed companies according to signs of disclosure of sensitive information, leaked credentials and hacker group activity.

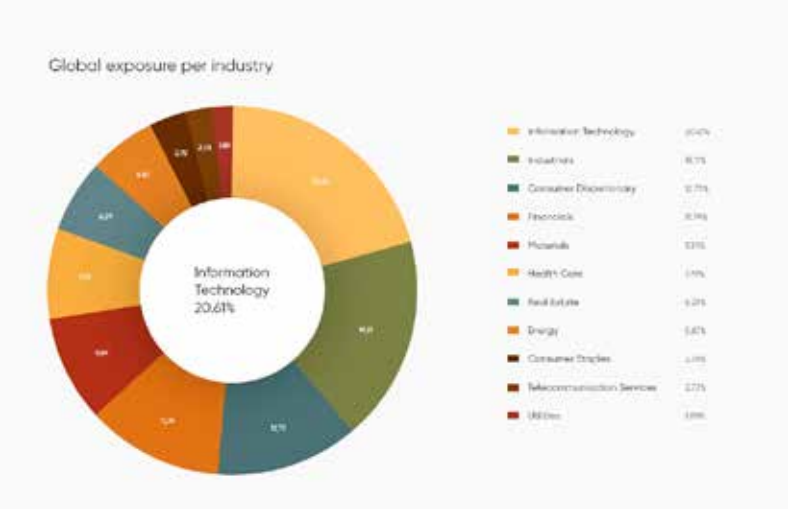
The index aggregates data on more than 6,000 listed companies collected from publicly available sources in the Dark and Deep Web and from data breaches, and ranks them according to the number of findings and the risk that the findings represent, divided by the number of employees. Scores range from 0 for companies with no exposure over the past 12 months to 300+ which represent the top 10% most exposed companies globally.

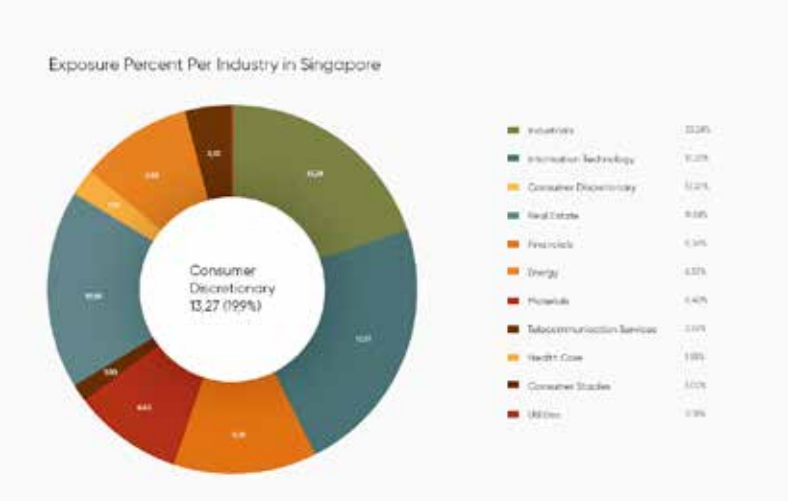
On the other end of the spectrum, countries that were found to have the highest risk of cyber exposure were the United States, United Kingdom and Finland. Other markets also covered in the study include Australia, Germany, Italy, Malaysia and South Africa.

Cyber exposure – the extent of a company's data already revealed by or to hackers – is the best predictor of the likelihood and intensity of cyber crime against that company in the near to mid-term.

"Any level of cyber exposure, even if it if poses no immediate danger, can be damaging as it sows the seeds of sabotage. The growing interconnectivity of companies and complex dependency networks is creating expanded attack surfaces and endless virtual entry points that not only increases the







threat of data breaches exponentially, but also the magnitude of the impact. It is therefore imperative for companies to know how cyber exposed they are," said Mikko Niemela, CEO of Cyber Intelligence House.

With the accelerating pace of digital transformation across the world, Cyber Intelligence House expects to see a dramatic increase in the exposure levels of companies across most industries.

"Mitigating data breaches begins with understanding where critical information is stored, from where is it leaking and how it is exposed. The Cyber Exposure Index is the first step in this remediation and mitigation process by identifying existing threats and making them transparent to help companies who want to employ a proactive approach to identifying these loopholes within their organisation. It also helps investors compare the risk level between companies to make more informed decisions," said Niemela. SST

Dahua Technology Ranked #2 On a&s Security 50

Dahua Technology jumped up to the number two spot on the 2018 a&s Security 50, moving one position higher than last year. This is the fifth consecutive climb up the list for Dahua Technology since 2014.

An influential ranking, Security 50 ranks global manufacturers by product sales revenue, gross profit, profit margin and net profit in their 2017 public financial reports.

Dahua Technology scaled up the list in 2018 by achieving gross revenue of RMB18.84 billion (US$2.88 billion). This is a 41.38% year-on-year increase.

The company has been investing heavily in R&D since 2014. Since 2016, Dahua AI algorithms has been sweeping the top position in a number of KITTI, ICDAR and MOT international challenges.

In 2018, Dahua Technology launched a series of AI products and solutions that enable perimeter protection, face recognition and people counting.

The same year, Dahua Technology launched Heart of City, a smart city development engine to realise the 1 platform, 2 centres, N applications (1+2+N) new smart city framework for application at the city, industry and commercial level.

Dahua Technology also opened its European Supply Centre to offer its European markets enhanced customer service and faster delivery using local assembling and centralised logistics services. SST

SURVEY RESULTS:
ASIA PACIFIC GOVERNMENTS NEED TO WISE UP ABOUT KEEPING CITIES SAFE

Designed by freepik

Asia Pacific has some of the world's smartest cities; there will be at least 88 smart cities worldwide by 2025 and Asia Pacific will account for 32 of them, ahead of Europe and the Americas, predicts IHS Markit.

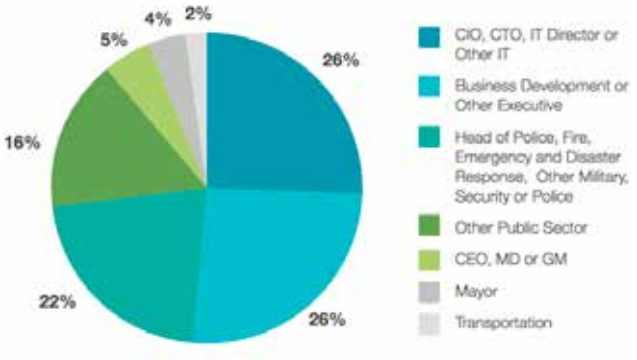
Smart cities are cities that use data and technology in powerful ways to improve safety and to deliver services that improve the well-being of citizens. They typically feature a network of connectivity across systems, devices and objects (the Internet of Things, or IoT). A report estimates that smart cities accounted for more than 1.1 billion IoT items in 2015, rising to 9.7 billion by 2020.

But are governments in Asia Pacific doing all they can to make their cities safer and smarter?

A 2018 Safe Cities survey by Hitachi Data Systems (now known as Hitachi Vantara) suggests not.

Hitachi carried out the survey on delegates at the Safe Cities Asia conference in Singapore, which was attended by city government representatives, agencies and key municipal leaders from Asia Pacific. Over a quarter of the respondents had a technology background of some kind, with the rest ranging from city mayors and corporate CEOs to military, emergency services, and providers of infrastructure such as transportation and logistics (see Figure 1).

Figure 1: Survey respondents by job title



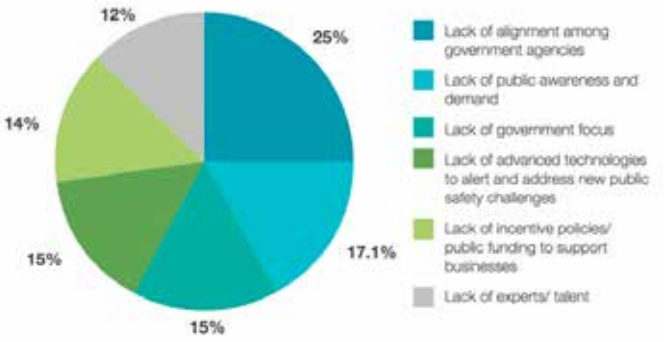
Source: Hitachi Vantara

The survey offers up enlightening insights into the plans and progress of public safety initiatives across Asia Pacific, and suggests that integration is key to success.

Lack Of Government Focus Holding Back Public Safety Projects

The survey revealed a lack of government focus to be the major stumbling block to adoption of smart city initiatives that promote public safety (see Figure 3).

Figure 3: What are the top three factors you think hinder the implementation of public safety projects?



Source: Hitachi Vantara

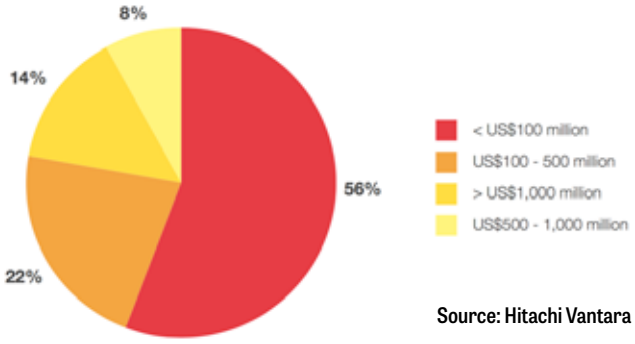
The main barrier seems to be the failure to adopt an integrated approach to safety initiatives; a quarter of survey respondents felt a lack of alignment between government agencies was actually holding back the implementation of public safety projects.

Ideally, as many stakeholders as possible should be involved in the planning process for implementations that would go further in making the city smarter and as safe as possible.

The Good News: Serious Money Is Earmarked For Safer Cities

Nearly half (44%) of the respondents estimated that their countries would invest more than US$100 million in public safety projects during the next two years. Some 22% of them predicted that the investment would be higher, at between US$100-US$500 million, while nearly 14% anticipated spending over US$1 billion (see Figure 2).

Figure 2: How much do you expect your country will invest in public safety projects over the next two years?



Source: Hitachi Vantara

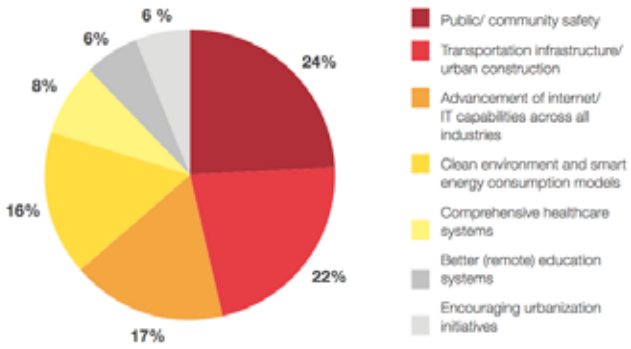
Almost all surveyed (about 90%) said that either they or their organisations had already been involved in a safety project. Moreover 69% of respondents are planning to invest in public safety projects in their countries over the next two years.

More Infrastructure, More Technology Needed To Tackle Crime

What needs to be done to achieve a smart city? Get the infrastructure up, said 22% of the respondents.

They suggested what is needed is physical development initiatives such as urban construction projects and enhancing or expanding transportation infrastructure. Ramping up Internet and IT capabilities was also high on the list, with a 17% response rate (see Figure 4).

Figure 4: As governments are encourged to build up "Smart Cities and Nations" in the region, what area(s) do you think need(s) to be addressed to realise the "Smart City and Nation" goal?



Source: Hitachi Vantara

Surveillance Is Top Priority

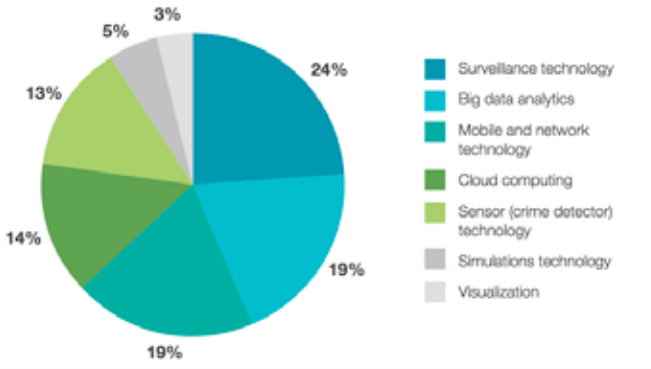
One of the key priorities in realising a smart city is public safety. And crime is a problem that technology can address. Integrating new IT platforms with city resources can dramatically driving down crime rates and enhance public safety.

Take the experience of the Dubai government. An increase in government investment of 29% in the form of the Smart Dubai initiative resulted in an increase in the overall safety result of 8% and helped ensure citizens are safer from individual risk and property risk by 3% and 31%, respectively, according to the IHS Markit report The Benefits Of Safe Cities.

Sophisticated technology is key in monitoring and preventing crime by identifying criminal acts, or potential criminal acts, in advance. For example, advanced analytics tools are able to crunch data from a variety of sources, such as video cameras on trains, in department stores and throughout the city, as well as other data on social platforms such as Twitter to extract vital insights that can identify crime hotspots.

An overwhelming 95% of respondents rated the role of technology in ensuring public safety as Important or Very Important. And the public safety technology that most plan to invest in over the next two years is surveillance, followed by big data analytics, and mobile and network technology (see Figure 5). The convergence of all three means there is great scope for lifting safety and security in modern cities.

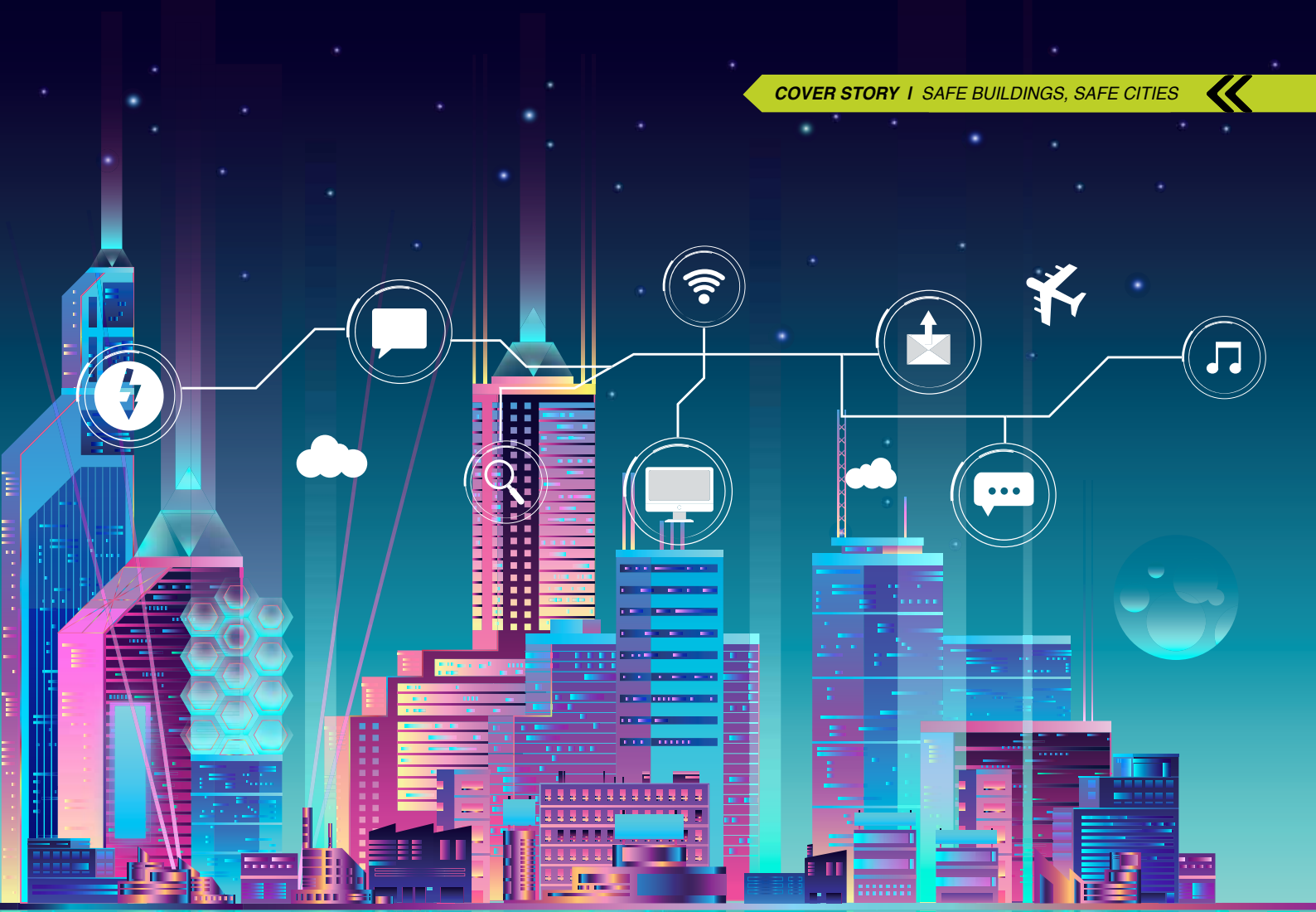
Figure 5: In the next two years what are the top three technologies you will invest in?



Source: Hitachi Vantara

A Smart City Is First And Foremost A Safe City

The ultimate goal for any smart city is to create an environment where people can live without fear. This can be done by holistically managing all the various parts of city administration, whether that component be securing critical utilities, enhancing transportation and emergency services, or reducing crime. SST



Designed by pikisuperstar / Freepik

LOOK TO SMART BUILDINGS FOR TOMORROW'S SAFE CITIES

Want to know what safe cities would look like tomorrow? Take a close look at the latest building innovations around the world.

The building blocks of tomorrow's smart cities can be glimpsed in today's smart buildings, where modern buildings are proving to be testbeds that allow city builders and solution providers to identify and implement the technology that will shape the future of cities.

We showcase two building solutions that are transforming buildings into safe, secure, proactive systems.

ThermEye: For People-Counting Smart Buildings That Can Save Lives

ULIS, a designer and manufacturer of a wide range of innovative thermal image sensors, recently launched ThermEye Building, a thermal sensor line that detects and counts people for connected buildings.

One of the key features of ThermEye Building is the ability to detect potential fire hotspots and manage people flow during a fire.

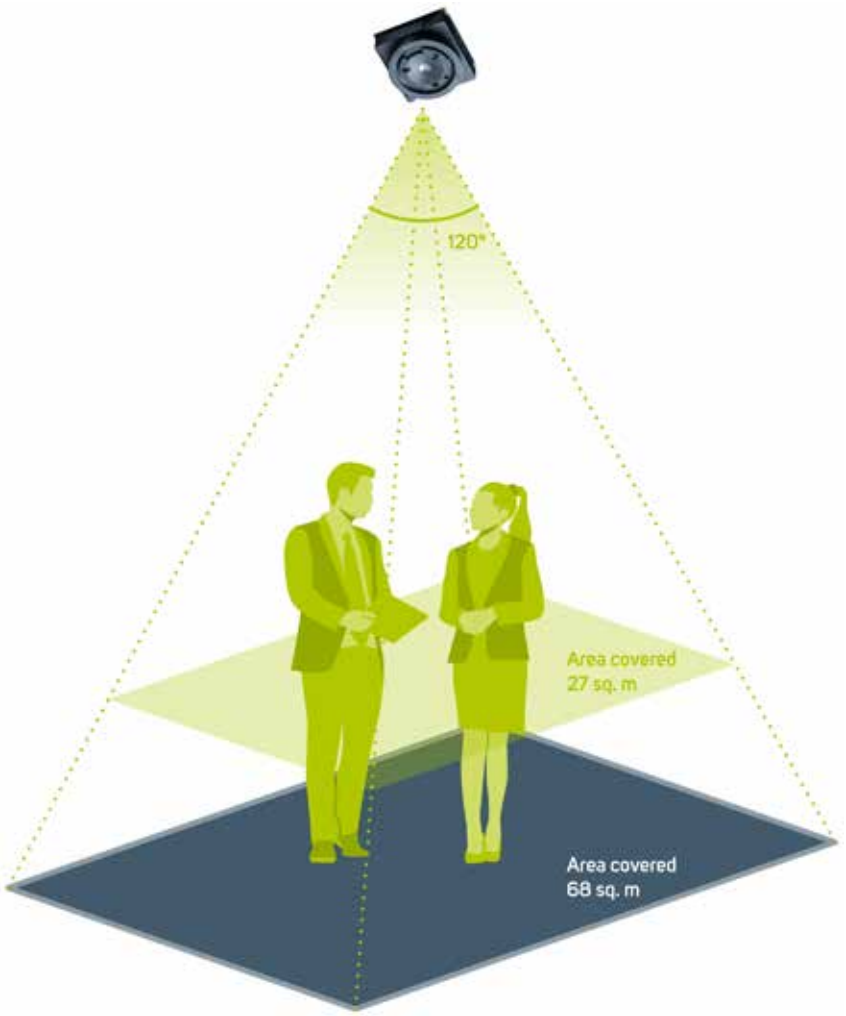
The ThermEye Building range includes two products: ThermEye-b90 and ThermEye-b120. Both models boost 80x80 thermal sensors that provide system integrators with advanced functionalities to detect presence (even people who are not moving) and localise and count people. These functions improve capability to analyse human activity and communicate with relevant smart building applications.

Coupled with a 90° or 120° field of view lens, a single ThermEye Building sensor can cover a zone of 30m², equivalent to a meeting room accommodating eight to 10 people.

The product range is configured with a conventional video channel (50 images per second) and features an intermittent mode that is compatible with low-power consumption applications.

Just one AA battery is needed to run a ThermEye Building sensor when transmitting an image at two-minute intervals. The advantage of running entirely on batteries is that end-users can deploy the systems in both new and existing buildings.

The solutions developed for the ThermEye Building product line guarantee occupant anonymity and privacy, as there is no facial recognition. This is a plus for integrators wishing to use data to develop other future solutions for smart building applications that improve how facilities optimise space usage and energy management, detect potential fire hotspots and manage people flow during a fire.



"We have extensive expertise and experience in designing reliable high-resolution thermal image sensors. We are now applying this know-how and industrial rigour to our mass market sensors," said Cyrille Trouilleau, smart buildings manager at ULIS.

Established in 2002, ULIS has grown to become the world's second largest producer of thermal image sensors (microbolometers), exporting 97% of its products to camera makers across Europe, Asia and North America.

Metasys 10.0: Bringing Occupant Comfort, Safety, Security And Productivity To New Levels

In December, Johnson Controls launched *Metasys* 10.0, a building automation system that redefines modern building management.

Johnson Controls is a global diversified technology leader that creates intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems to deliver on the promise of smart cities and communities.

With this latest version of *Metasys*, Johnson Controls introduced significant enhancements and powerful integrations for safer and smarter building operations. It provides facility personnel with smarter building automation, faster responses to critical alarms and new integrations with fire detection, security and lighting systems – all with visibility from a single common interface.

Metasys 10.0 introduces a new and improved set of integrations. These include new integrations with C·CURE 9000 Access Control and victor Video Management Systems, and simpler integrations with SIMPLEX® Fire Systems and with lighting systems from leading lighting providers.

A new *Metasys* Application Programming Interface (API) enables data to be securely extracted from *Metasys* 10.0 and integrated with Johnson Controls or third-party data visualisation tools for robust data analysis and reporting.

"Johnson Controls is committed to helping build smarter, safer cities and this latest *Metasys* release supports that commitment," said Chris Eichmann, vice president and general manager, Global Controls Products, Johnson Controls. "With new and innovative integrations, users can now leverage data from access control and video management systems to better automate building conditions. For example, users can lock or unlock doors and verify badge scans from within the intuitive Metasys interface, which helps create more secure environments for city employees and residents."

Several new hardware devices were also added to *Metasys* 10.0, including:

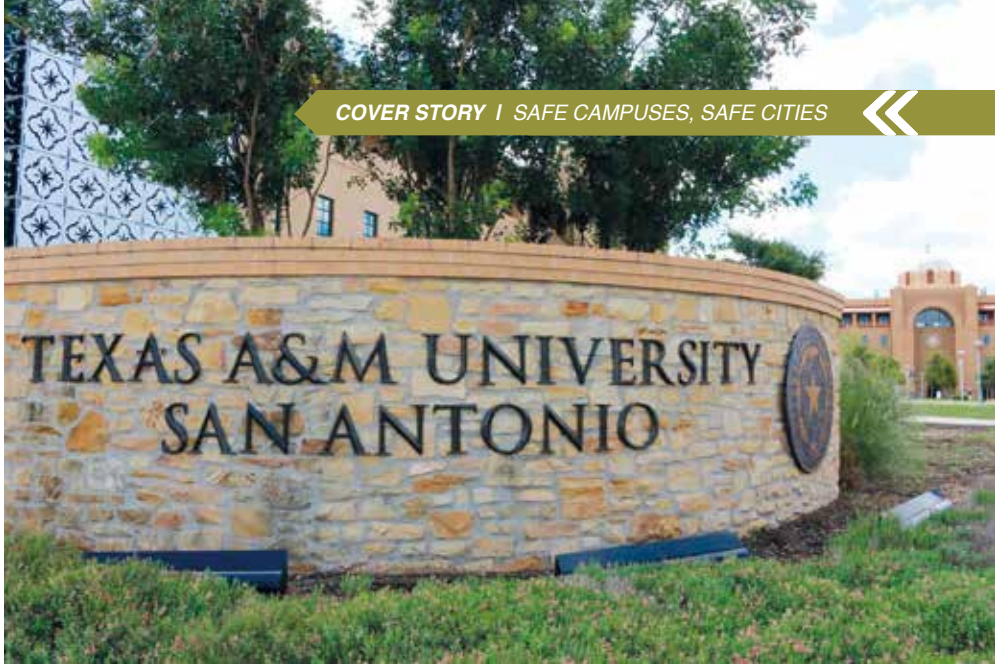
- Two new equipment controllers with removable screw terminal blocks for easy installation, high capacity memory and fast processing
- A new 4-in-1 network sensor series with the ability to sense temperature, humidity, CO_2 and occupancy – all with one sensor
- A new TEC3000 thermostat controller with colour touchscreen

Another innovative feature is Ethernet ring topology support for *Metasys* IP equipment controllers. Delivered as part of Johnson Controls' collaboration with Cisco, it allows controllers to be configured in a ring network, improving system reliability and resiliency.

Metasys 10.0'S benefits include:

- Operational savings through extended building management capabilities and enhanced productivity
- Energy savings through coordinated control, precise data and peak equipment performance
- IT and platform security through best-practice processes
- Faster troubleshooting and response through advanced diagnostics
- Greater occupant comfort, security and satisfaction SST

SAFE CAMPUSES MAKE FOR SAFE CITIES



School security is a growing concern around the world, particularly in the United States, where a string of deadly mass shootings has chillingly brought home the vulnerability of the campus to devastating violence.

Gun attacks are not the only security issue schools have to deal with. Institutes of learning must not only protect students from violence, they must safeguard students from weapons, thefts, bullying, intimidation and drug trafficking on school grounds. Achieving this is a complex undertaking. Schools see an enormous flow of visitors, both pedestrians and cars, comprising groups such as students, teachers, parents, school staff, vendors, suppliers and irregular visitors. Schools have to manage the access of this wide range of people to different areas and facilities.

To establish a safe campus, schools must detect threats fast, communicate effectively with staff, students, parents and security forces in an emergency and deliver a secure learning environment where students and staff feel safeguarded.

Two solutions address these imperatives.

In December, Texas A&M University-San Antonio (A&M-SA) became the first university in the world to deploy the SafeZone Indoor Positioning Solution across its entire campus to secure the university.

SafeZone is provided by global technology innovator CriticalArc.

First launched in 2014, SafeZone is a distributed command and control solution that provides response teams with complete operational awareness, to enhance the protection of dispersed people, facilities and assets while delivering efficiency savings. Accessed by users through an intuitive app, SafeZone enables users to call for help in seconds, when and where they need it, while providing security teams with features for targeted mass notifications and management of lone worker presence. Delivering situational awareness across large geographic areas, SafeZone supports a rapid and coordinated response to incidents by distributing information to first responders and allowing them to collaborate as events unfold.

Another solution is the newly introduced Intelligent Campus Solution by Huawei and YITU. Launched in October 2018, Intelligent Campus empowers a flexible, secure, and reliable intelligent security system to help institutions improve campus management.

Turning A School Zone Into A SafeZone

SafeZone is revolutionising the way institutions manage day-to-day safety and security on campuses.

The indoor positioning solution by CriticalArc provides campus police with an unprecedented three-dimensional view of multi-story buildings. For example, instead of sending an alert about an incident somewhere in the student union building, SafeZone provides pinpoint specifics such as “it’s on the fourth floor, west wing, outside room 410”.

Among other capabilities, SafeZone allows users to get help within the shortest possible time simply by activating an alert using an app or a wearable duress alarm. As soon as the alert is triggered, the location and details of the user are streamed to the monitoring team, allowing officers to coordinate a smarter, more targeted response. By enabling responders to visualise the precise location of an incident, anywhere on campus, SafeZone is much more powerful than traditional fixed panic alarms and blue light telephones, which are more expensive to install and less accurate in operation.

Texas A&M University-San Antonio’s Chief of Police Ron Davidson wanted the full-coverage system because the campus was expanding and now boasts a newly completed residence hall. This means having students around the clock for the first time in the university’s history.

In addition, Chief Davidson was in search of a common operating view that would provide his Emergency Operations Center and all officers on patrol a real-time location of all available officers and volunteers, as well as show the location of

all incidents essential for coordinating first responders and the Campus Community Emergency Response Team.

"SafeZone is essential technology to position your organisation on the cutting edge of campus law enforcement. The real-time common operating view both enhances officer safety and acts as a force multiplier. Plus, the entire police department benefits from advanced features such as heat mapping and incident playback to optimise performance," Davidson said.

SafeZone was easy to deliver with no disruption to the campus. It was deployed in a matter of weeks during the summer break. The process to get the SafeZone indoor positioning solution deployed is a simple one, as it's a wireless installation and easy to maintain. In addition, organisations can introduce wireless, wearable duress alarms able to pinpoint anyone anywhere on campus as an alternative to fixed, expensive, wired panic alarms.

SafeZone is currently operational in more than 80 countries worldwide, and commercially available worldwide for a range of university, hospital, enterprise and finance applications.

Intelligent Campus: Proactively Safeguarding Campuses

Jointly developed by Huawei and YITU Technology, Intelligent Campus empowers a flexible, secure and reliable intelligent security system to improve campus management.

By leveraging emerging ICT technologies including cloud computing, the Internet of Things, big data and artificial intelligence, Intelligent Campus addresses challenges to traditional campuses such as low management efficiency, weak comprehensive security and high operational costs.

The solution is based on YITU's Smart Park Management Platform and Huawei's Atlas Intelligent Computing Platform.

Smart Park Management Platform is a latest-generation facial recognition and integrated campus management software. It allows institutions to use video-based facial recognition to control access to buildings and sites, to conduct proactive safeguarding and to analyse how different areas are used.

The video-analytics system can be deployed in different configurations depending on the size of the implementation. AI servers can scale to meet the needs of a large enterprise campus or edge servers can support smaller campuses.

Meanwhile the freshly unveiled Huawei Atlas Intelligent Computing Platform uses the ground-breaking Ascend 310 AI processor developed by Huawei to deliver 16-channel HD video real-time analysis. This platform is compatible with various terminals and supports diverse applications to integrate data, visualise the campus status, manage all services and control events. It also integrates different forms of hardware for better adaptability. It includes the Atlas 500 AI edge station for small-scale campuses, and AI servers fitted with the Atlas 300 AI accelerator card for mid- and large-scale scenarios.

Huawei is a global mainstream IT vendor with a broad spectrum of servers and a full line-up of IT products. So far, 211 of the Fortune Global 500 and 48 of the Top 100 enterprises have selected Huawei as their partner for digital transformation. YITU Technology is a pioneer in artificial intelligence research and innovation. SST

INTELLIGENT SOFTWARE HELPS REDUCE VEHICLE ACCIDENTS BY 19%

A cloud-based system for enterprise safety, quality, reporting and incident management has helped a major transportation company reduce vehicle accidents by 19%.

RATP Dev USA operates and maintains urban transportation systems in 14 countries on four continents (Algeria, China, France, India, Italy, Morocco, Qatar, Saudi Arabia, South Africa, South Korea, Switzerland, the Philippines, the United States of America and United Kingdom). More than 1.5 billion passengers travel on its networks every year. In the United States alone, it transports more than 78 million passengers across the country via various transportation offerings such as bus, urban and intercity rail lines (streetcar) and shuttle services.

The solution, Coruson, is used by RATP Dev USA to manage safety, risk and operational performance across all its bus, paratransit and rail services.

Coruson was developed by Ideagen, a UK-based global software firm that provides software and services to organisations operating within highly regulated industries such as aviation, banking, finance, life science, healthcare and manufacturing.

Coruson is currently used by some of the largest and most prominent transport organisations in the world including the International Airlines Group – the umbrella organisation for British Airways, Iberia, Vueling and Aer Lingus – Haeco Group, Ryanair, ADAC and HNZ Global.

RATP Dev USA adopted Coruson in December 2017 as part of its drive2zero Safety Management System.

The drive2zero framework has four components: Safety Policy, Risk Management, Safety Assurance and Safety Promotion. The framework was adopted to continuously improve transit operations and support RATP Dev USA's commitment to an unparalleled safety record for customers and employees.

Mike Anderson, VP of Safety and Security for RATP Dev USA, said, "To date, we've implemented Safety Management System in eight of our subsidiaries out of around 35, so we still have a lot of work to do. But our initial results are very promising – we've seen an overall reduction year-to-date of 19% in vehicle accidents alone."

As part of the same framework, SmartDrive Systems, a leader in video-based safety and transportation intelligence, provides RATP Dev USA's fleets, drivers and management with driving performance insight and analysis, which is helping the company save fuel, expenses and lives.

"Where in the past we have seen companies report positive results in nine to 12 months, we're now seeing results in six to seven months," described Patrick Manley, Director of Safety for RATP Dev USA. "That's due to an increase in hazard reports as we now have people telling us where risk is in our organisation and a comprehensive way of managing that risk."

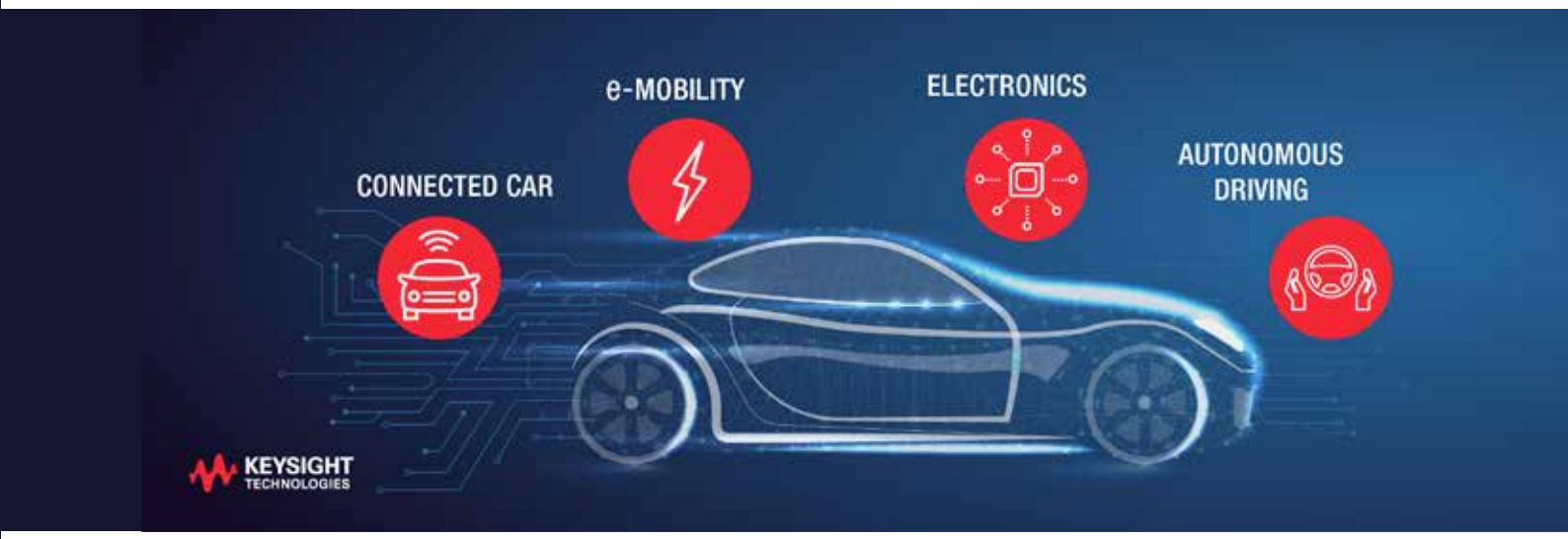
Said Gordon McKeown, Head of Product at Ideagen, "We are absolutely delighted that our Coruson software has played such a crucial part in helping to reduce vehicle accidents across eight RATP Dev USA subsidiaries and we are confident of seeing even more success across the wider network as the project progresses."

Meanwhile across the US, the Public Transportation Agency Safety Plan (PTASP) Final Rule requires operators of public transportation systems to develop safety plans that include processes and procedures necessary for implementing safety management systems from July 2019 on.

Mike added, "Any of our subsidiaries or locations that adopt drive2zero will now automatically meet the requirements of the PTASP rule." SST

AUTONOMOUS CARS ARE COMING: RIGOROUS TESTING WILL MAKE THEM SAFE

►► **By Michael Reser,** Business Development Director, Keysight Technologies, Inc.



It is no secret that the development of the autonomous vehicle is evolving fast.

After years of work on enabling technologies, everything is starting to come together - the disparate systems in cars, road infrastructure and traffic management centres.

Currently communications standards such as 5G and Wireless Access for Vehicular Environments (WAVE) are under development, and cities are undergoing pilots to test and analyse the performance of these vehicles.

It is likely that sometime soon autonomous vehicles will be ubiquitous on streets, ferrying people and goods from Point A to Point B with little or no human interactions.

Before that happens, however, some work still need to be done to ensure autonomous vehicles are safe, secure and convenient.

The key to having roads filled with driverless cars is connectivity and getting these disparate technologies to work together in concert. And to achieve that, extensive testing and the development of robust standards are needed.

The Need For Rigorous Testing

Autonomous vehicles will only work if they can reliably and securely communicate with other vehicles and infrastructure. They need to make lightning quick decisions to avoid hazards, stay in their lane or simply navigate city streets. Plus automobiles are more complex than ever.

So basically you have multiple high-speed communication systems that need to communicate with each other. This means having fast automotive wireless and wired communications systems that can handle all that data.

Given these complexities, multiple digital systems must be extensively tested. Radar, Lidar and other sensor technologies collect enormous amounts of data from the environment while driving, and disseminate the data to pertinent automotive systems. Those systems need to be able to take the data in, weed out redundant or irrelevant information, process the data, and make quick and flawless decisions. Finally, they all need to seamlessly work together without failure. Each component of every system needs to be tested and validated from an electrical as well as communication protocol point of view.

It is also important to remember that autonomous vehicles are basically moving data centres cruising down the road at highway speeds. Automotive Ethernet systems tie all these systems together, acting as the data backbone for these computer networks on wheels.

Rigorous Testing That Never Stops

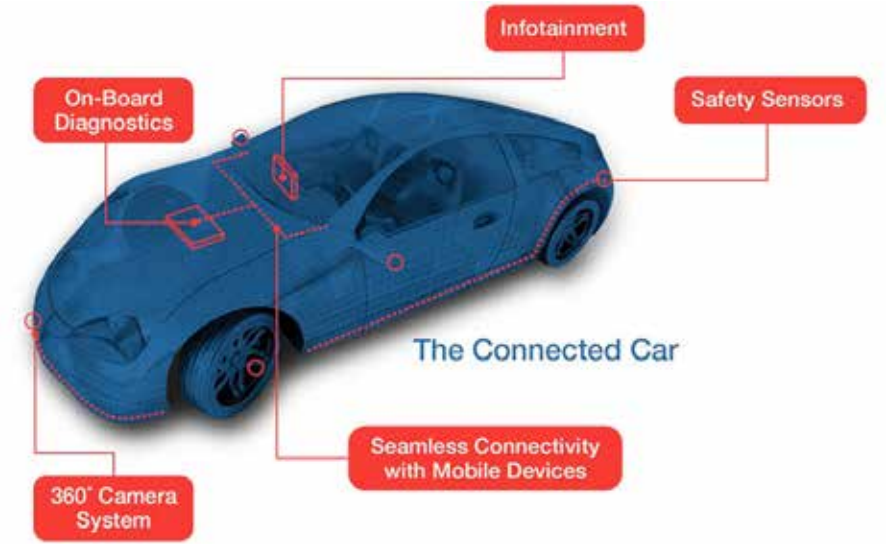
Rigorous testing of new autonomous vehicle technologies using a variety of testing tools can validate components from the physical layer (including electrical and timing for example) to the application layer. For example, testing to make sure an optical image can be extracted off a camera and converted into actionable data; whether firmware can be debugged separately from the electrical system, or whether a Lidar sensor can capture incoming data without error.

Specialised equipment can test whether two end points are communicating effectively through an automotive Ethernet link, tracking data as it moves along a digital bus. Also, engineers are using oscilloscopes to understand how legacy automotive standards, such as Controller Area Network (CAN), Local Interconnect Network (LIN) and FlexRay are interacting with modern automotive Ethernet protocols. Test engineers are also looking to the future by making sure automotive systems can handle forward-looking technologies and protocols as we move to 5G.

Testers can simulate and emulate power failures, data corruption, security breaches, even false signals or alerts, to ensure that autonomous vehicles are error proof before they go on the market.

Consider Power Too

It is not just autonomous driving technology that is undergoing test right now. New power sources have the capability to change the way we move from Point A to Point B. Engineers are also testing batteries, electrical components, electric vehicle charging stations and supply equipment.



Tests are being conducted to identify whether power is flowing from a charging station to a vehicle's battery and to debug any conflicts. Powerful analytics software can monitor various control signals such as charge conditions, temperatures and voltage, monitoring for unexpected behaviour before running diagnostics to troubleshoot the issue.

In addition, the batteries themselves are undergoing rigorous testing. From characterising cells, modules and packs, manufacturers can collect valuable data that allows them to design higher quality devices and optimise parameters such as long-distance driving (drive duration, endurance and longevity) as well as driving profiles, which impacts the distance a battery can be used with one charge.

Due to the higher content of electronics within hybrid and/or electrical vehicles, Electromagnetic Compatibility (EMC) considerations are critical, as interferences between systems can be a significant safety concern requiring extraordinary care during product development and final testing.

Autonomous vehicle development has been supercharged over the past several years, making it critical to test every component in every vehicle to ensure it performs properly. Testing those components and systems are not optional because it is not just about performance and availability. Autonomous vehicles make thousands of critical safety decisions every second. Even one failure can mean serious injury or the loss of life. Engineers understand the consequences and take every possible step to eliminate risks and safety issues. They know the public's trust is in their hands. SST

Photo by Goh Rhy Yan on Unsplash

SAFE SKIES FOR SAFE CITIES

Terrorism by unmanned aircraft is a growing threat, with unmanned aircraft system (UAS) technology getting easier to acquire by the general public and ill-intentioned groups.

Drones have been modified to carry all manner of potentially harmful payloads, from grenade-sized bombs to drugs and other contraband. What's worrying is that most current security systems set up in critical infrastructures are not designed to protect against drone incursions.

Electro Optical Industries offers answers to this threat in the shape of its most powerful 360° Thermal imaging sensors SPYNEL-X and SPYNEL-S.

The Infrared Search & Track System With The Highest Definition In The World

Spynel-X is the Infrared Search & Track (IRST) system with the best image resolution and the longest detection range on the market. It captures full 360° images in real time with unparalleled resolution of 120 Mpix.

The camera displays the highest performance in its category: one single IR sensor can provide 24/7 early human intrusion detection over a 16km-diameter area. One 360° thermal sensor can thus replace up to 90 HD MWIR cameras.

Meanwhile the SPYNEL-S features a cooled Mid-Wave InfraRed (MWIR) focal plane array for high performance, especially in warm and humid regions. Rotating continuously at up to one revolution/sec for total 360° azimuth coverage, it captures real-time images with an impressive resolution of up to 30 Mpix. As it produces high-resolution images, any type of target, of any size, will be automatically detected and recognised, making it far more sensitive and convenient than radar. Monitoring 360 degrees every second, it can catch multiple intrusions coming from multiple directions, unlike PTZ cameras which are blind outside their limited field of view.

Most of the time, UAVs' small size and low electromagnetic signature go unregistered by traditional detection measures. With SPYNEL's thermal imaging technology, it is impossible for a drone to go unnoticed: any object, hot or cold, will be

detected by the 360° thermal sensor, day and night.

Both model are unlike all other systems on the market, which must use separate sensors to get similar functions: one sensor for detection and another sensor for identification, such as a PanTiltZoom camera.

Xavier Elbaz, Sales Manager at Electro Optical Industries explains: "With separate systems, it is hardly possible to ensure a real 360° coverage for detection and identification because of blind sectors created by the mechanical supports. Moreover, separate sensors must be integrated and calibrated to properly operate together. SPYNEL and its V-LRF option ensure no blind sector for a real 360° coverage in all surveillance phases: detection and identification."

SPYNEL V-LRF and its automatic detection and tracking software CYCLOPE are easy to deploy and to use, and the system is easily interfaceable for multi-sensor protection of critical infrastructure like prisons. Data is smoothly merged with other sensors' data like radars, AIS, and fence vibration sensors and displayed on the same interface unlike separate sensors, which must be integrated and calibrated to operate properly together. SST

VEHICLES ARE GETTING SMARTER AT KEEPING DRIVERS SAFE

Singapore's Nanyang Technological University (NTU) is working with industry partners to make vehicles smarter with the goal of improving drivers' safety on the road.

The university is currently exploring several vehicle-to-everything (V2X) technologies. These include dedicated short-range communication V2X, existing 4.5G mobile network and the upcoming 5G mobile network, which will improve the data transmission speed and radio coverage distance for communication between vehicles to infrastructure, paving the way for faster notifications and warnings.

Starting 2019, NTU will work with industry partners to study how these technologies can synergistically complement each other and be applied in autonomous vehicle prototypes, traffic infrastructure and unmanned aircraft systems. These vehicular communications will be used to relay real-time navigation traffic and hazard information to vehicles.

"Employing cellular communication and integrating them into existing V2X technologies for mobility can help to reduce travelling time, minimise the risk of serious accidents and optimise road usage for a densely populated urban city like Singapore," said NTU Vice President (Research) Professor Lam Khin Yong. "Emerging technologies researched today may soon become the norm in our everyday lives, contributing to Singapore's vision to be a Smart Nation."

Already some research projects have delivered promising results.

Early Warning System For Vehicles

One of them is an early warning system for vehicles. NTU and NXP scientists demonstrated how tapping into the car's electronic systems through the on-board diagnostics port allows on-board diagnostics port data to be collected and interpreted in a way that could help make roads safer for all users.

The V2X system provides advance warning to drivers about road hazards such as a car stopping unexpectedly or a passenger suddenly opening a vehicle door.

In a 20-minute live demonstration conducted on NTU campus, the vehicle successfully notified fast-approaching vehicles that its doors were being opened and that it was disabled along an expressway. It also informed the driver that another car was coming out of a side road.

Nearby vehicles would receive the same warnings too wirelessly in real time via the smart on-board unit, giving drivers of these vehicles more time to react and avoid collision.

Another function shown was a combined Green Wave and Green Light Optimised Speed Advisory system. This system allows a vehicle to receive data from upcoming traffic lights. Using the data, the vehicle is able to tell the driver how fast or slow he must drive in order for him to catch the green wave – where all traffic lights on his route are green.

Anti-Collision Alerts For PMDs

NTU also showed off a communication system that helps prevent collision between cars and personal mobility devices (PMDs) like e-scooters or e-bikes.

The system is meant to minimise the peril of collision between vehicles and PMDs, a peril that is growing with the rise in PMDs on roads.

Image source: NTU

The project saw automotive parts giants Continental and Schaeffer working with NTU scientists to integrate a V2X smart unit into PMDs to allow vehicle drivers and PMD users to detect one another. With the unit, vehicle drivers and PMD riders can be alerted when a PMD is in the blind spot of a reversing vehicle. Such an early warning system elevates the awareness level of all road users and lowers the risk of an accident in situations where visibility is low or blocked.

System That Overcomes GPS Black Spots

A novel positioning system developed by Cohda Wireless uses the V2X radio signal to determine a vehicle's location in spots where GPS satellite signals cannot be received. GPS black spots are commonly found in areas with tall buildings or areas that are underground or under sheltered car parks.

Using the on-board unit in the vehicle to communicate with roadside units installed in car parks, the V2X-locate system uses the known locations of the roadside units and the V2X radio signal to pinpoint the vehicle's location down to one metre accuracy 95% of the time, in the same way that a GPS navigator uses GPS satellite signals.

Cars Of The Future Will Enjoy Ultrafast Video And Data Communication

Panasonic has developed a futuristic 60GHz V2X system that can download extremely large files in split seconds. Conventional V2X systems use a slower 5.9GHz frequency to communicate.

This allows for ultra-fast real-time high definition video streaming and file downloads in future intelligent transportation systems such as autonomous vehicles. Downloads can happen when the moving vehicle is within range of the 60GHz base stations installed on lamp posts or bus stops.

World Leader In Smart Mobility Solutions

A world leader in smart mobility solutions, NTU has partnered top companies like Volvo, BMW Group, Blue Solutions, ST Engineering and mobilityX to develop innovative technologies for autonomous vehicles, electric vehicles and multi-modal mobility solutions.

Besides cellular communication technologies for vehicles on land, NTU is also working on the development of drone air traffic management via 4.5G mobile networks. This will endow drones with better localisation and positioning capability and ensure a smoother stream for high definition video footage. SST

CITIES GOT SMARTER AND SAFER IN 2018

Cities around the world got a little smarter and safer in 2018.

According to the Worldwide Semiannual Smart Cities Spending Guide, smart city initiatives attracted investments of more than US$81 billion globally in 2018.

The Spending Guide provides insights into the rapidly growing smart cities market and how the market will develop over a five-year forecast period. It gives a detailed look at the technology investments associated with a range of smart cities priorities, programmes and use cases. It is compiled by International Data Corporation, a global provider of market intelligence, advisory services and events for the information technology, telecommunications and consumer technology markets.

What Cities Are Investing In

Three areas attracted nearly one-quarter of global smart cities investment spending in 2018. They are fixed visual surveillance, advanced public transit and smart outdoor lighting.

"Intelligent transportation and data-driven public safety remain the largest investment areas, but we are also finding significant pockets of spending and growth in back office and platform-related use cases, which are less often publicised but increasingly happening behind the scenes in cities around the world," said Serena Da Rold, programme manager in IDC's Customer Insights & Analysis Group.

On a geographic basis, the Asia Pacific region, including China and Japan, accounted for nearly 42% of global spending in 2018, followed by the Americas (33%), and Europe, the Middle East and Africa (25%).

The United States is the single largest country market for smart city spending (over US$23 billion in 2018), followed by China.

The current three largest areas of spending appear among the top five in terms of spending across all regions, but apart from these three, other top spend areas include mobile video capture and recording in the United States and Latin America, and digital permitting, licensing and inspection in the Middle East and Africa region.

And Spending Will Grow

Spending is set to grow to US$158 billion in 2022, according to the Spending Guide.

By 2022, intelligent traffic management spending will oust smart outdoor lighting in third position, and the current top three spend areas (fixed visual surveillance, advanced public transit and smart outdoor lighting) will only account for one-fifth of total spending, as smaller and fast-growing application areas emerge and reach critical mass.

They include the categories of officer wearables and vehicle to everything (V2X) connectivity. These two areas will see the fastest investment growth though they currently are at a low base in most regions.

Spending by the 53 cities that are currently sized in IDC's database accounts for around 15% of global smart city spending, with Singapore, Tokyo, New York City, London and Shanghai leading the way in terms of 2018 investments.

"IDC expects to see strong, continued investment by the private and public sector in urban areas and in Smart Cities and Communities programmes and projects," said Ruthbea Yesner, vice president of IDC's Smart Cities and Communities programmes. "This also means that it is a more competitive market." SST

SMARTER, SAFER CITIES WITH AI

►► **By Chuah Seng Heng,** General Manager, Developed Asia and Japan, Motorola Solutions

Imagine this scenario: A crime has been committed in a busy crowded mall and the suspect is on the run. His movement is tracked via CCTV cameras. Meanwhile backend systems crunch through masses of data even as they run facial recognition software. The offender's identity is matched with a criminal records database within seconds and the information is shared with the police instantly. The offender is quickly identified and safely apprehended by the police.

This may sound futuristic but technologies exist today that are already helping police departments around the world keep people and communities safe. And these technologies are all powered by artificial intelligence.

AI's Impact On Business And Public Safety

Artificial intelligence is polarising public opinion, with technology leaders such as Mark Zuckerberg and Bill Gates on opposite sides of the debate. Will artificial

Photo Credit: Pixabay.com

intelligence make our world a better place, or will it ultimately replace all humans? Whichever side of the debate you are on, it is undeniable that artificial intelligence is already delivering tremendous benefits in the public safety domain.

In the realm of public safety, artificial intelligence is a growing, diverse and powerful new tool to help emergency services deal with today's evolving threat landscape.

For instance, chatbots are helping first responders to work in a way that enables them to keep their heads up and their hands free. These chatbots do much more than what we have experienced as consumers from chatbots like Alexa and Siri. These "virtual partner" chatbots are trained to understand and respond to the context and nuance of language used by first responders in daily operations and at critical events.

There are also many technologies, either existing or in development, that help commercial and public safety organisations find crucial pieces of data within large volumes of video footage for safety and security missions.

Artificial intelligence technologies are vital in IoT cloud computing systems because they make sense of raw data and provide actionable intelligence for decision makers. With video technology becoming increasingly commonplace, the vast amounts of video data being recorded on a daily basis is too immense for people to view and manage alone. That's an important place for artificial intelligence to come in, helping to process and to identify unusual patterns in video data, such as pinpointing a dangerous offender within a large crowd.

Artificial intelligence helps to transform raw, high-resolution video into rich and structured data that helps users to detect and track exactly what they are looking for. This includes unusual patterns and movements of objects and people, with inbuilt alarms to alert system operators to potential anomalies and hazards.

Artificial intelligence is also changing the way business is done today.

The business value artificial intelligence brings to enterprise and public safety organisations is amplified when organisations use it alongside their existing technologies such as two-way radio networks.

Take theme parks and casinos, which are among the businesses that take a big hit from any operational disruption. By adopting intelligent video analytics and letting artificial intelligence take care of the heavy lifting, the businesses spend less time on monitoring video feeds. This frees up their staff to respond to incidents more quickly and safely while reliable and continuous radio communications ensure they receive real-time information as incidents unfold.

Artificial Intelligence And IoT In A Digital Era

The Asia Pacific region is one of the fastest growing regions for IoT technology investment. IoT investment in this region is expected to reach US$500 billion by 2021 according to a report by DBS Group Research. That means almost half of the world's IoT investment will be in this region.

Singapore, with its thriving digital ecosystems, mature infrastructure and policy, is fast becoming an artificial intelligence and IoT hotspot for experimentation and innovation. In 2017, the Government announced that as much as 22% of the nation's technology budget would be set aside for security including artificial intelligence and analytics.

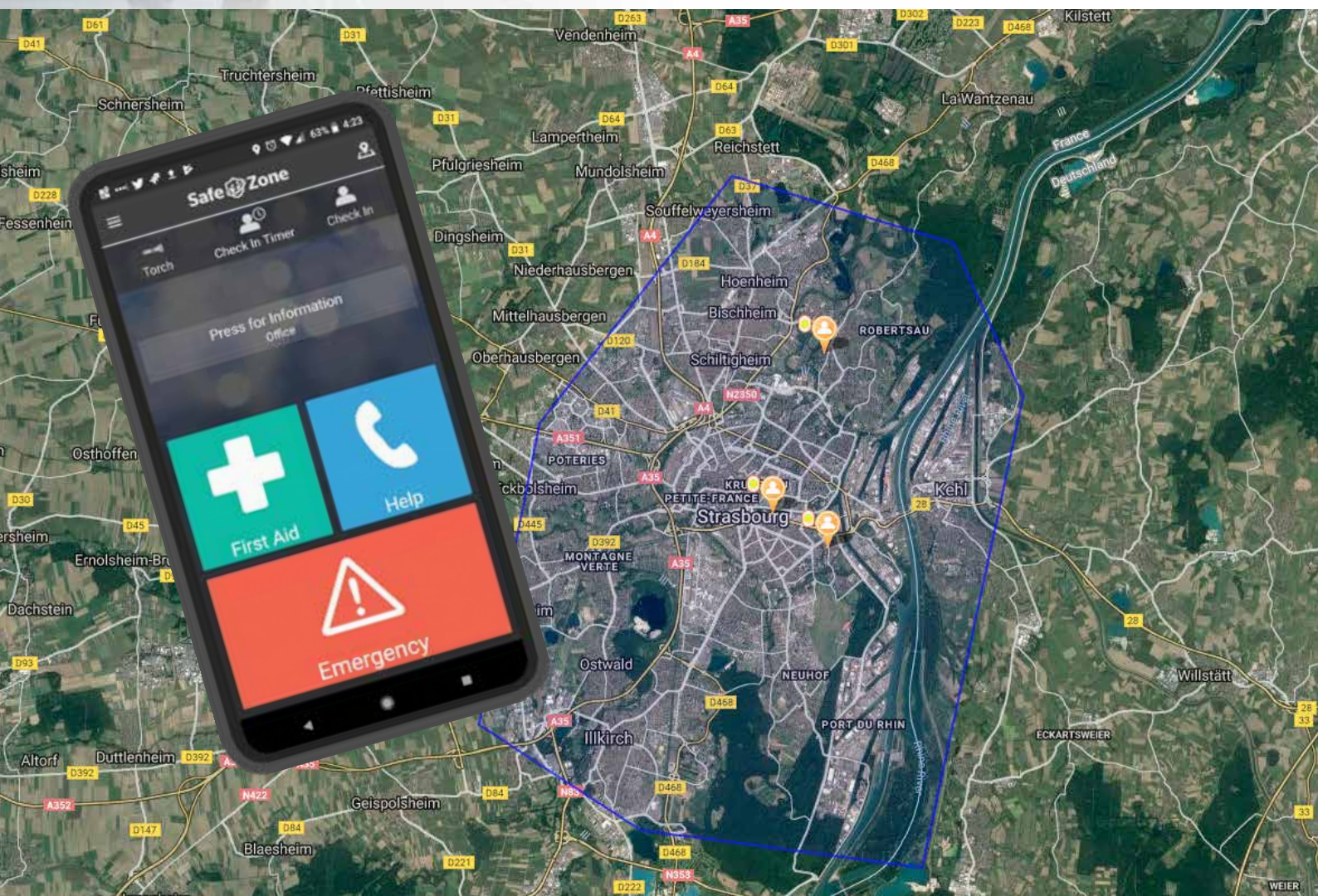
While rapid advances in artificial intelligence can be a polarising issue for consumers, here in Singapore consumers embrace artificial intelligence and are positive about the increasing adoption of artificial intelligence. According to a 2017 Accenture survey, Singapore consumers believe artificial intelligence will have a positive impact on their everyday lives and they are increasingly ready to embrace it.

The Equation Is Straightforward: Smarter Data Can Keep Cities Safe And Secure

The market for artificial intelligence has been spurred by the huge masses of affordable data available in our world today, the rapid development of cloud computing and the increasing realisation that smarter cities can make life better for all of us. Nevertheless many of us do not realise or actively think about how artificial intelligence can affect and improve everyday life in terms of keeping our cities safe and secure.

Granted, any technology used in this environment must be reliable, robust and support first responders to work more safely and efficiently. While the idea of intelligent computers taking over human tasks continues to be the topic of popular debate, one fact is undeniable: Artificial intelligence is already changing and improving the lives of citizens living in a city. SST

SECURITY CONTROL ROOMS EMPOWERED BY A MISSION TO PROTECT



Security control rooms around the world are seeing an uplift in their capabilities and their importance.

They are using the latest geo-location and visualisation tools to increase their command and control capabilities without the expense and complexity of traditional PSIM architecture that effectively just monitors systems, not people.

The actions of one security team last month during the deadly terrorist rampage in Strasbourg city in France illustrate how these new tools have the potential to make a very real difference.

On 11 December 2018, suspected Islamic extremist Chérif Chekatt attacked civilians in the city's busy Christmas market with a revolver and a knife, killing five and wounding 11 before fleeing in a taxi.

Three students from Edinburgh's Heriot-Watt University who were on university placement in Strasbourg discovered just how powerful security technology can be during the event.

Shortly after 8pm that day they received a notification on their SafeZone app warning them to keep off the streets and to stay in their current secure location.

That warning and subsequent updates were sent to them by the university's SafeGuarding team almost 900 miles away, where the team was monitoring breaking news of the shooting incident. Checking their SafeZone system, the officers on duty had quickly discovered that three of the university's students were within a mile of the incident locus.

From the moment when the news first broke, to the moment when all the students had been located and advised to remain in their secured buildings, only 30 minutes had elapsed. All this while, a full scale security operation was underway: the European Parliament building was going into lockdown and the police were using Twitter to relay information to the public.

The technology they're all using is developed by CriticalArc and it is now deployed in over 80 countries.

Creating Safe Zones In 80 Countries

The technology works by letting control room operators pinpoint the precise locations of individuals: staff, students, service users, in fact any user who is 'checked-in' using a simple app on his smartphone.

This service makes it easy for users to communicate directly with security operators. Users can use the mobile app to call for help, ask for advice and report suspicious activity.

The solution also allows security teams to send out alerts and safety instructions to groups or individuals. The teams can also monitor activity patterns and coordinate resources. For example, using the solution, teams are able to keep track of where registered first aiders are and see exactly how team members are deployed, minute by minute.

The technology operates globally and in many ways universities and hospitals are the ideal proving ground for it because of their diverse operations and nature of their challenges.

For example, students and teaching staff frequently travel to study and work. With the solution, they can be 'geo-fenced' - protected and communicated with - wherever they go, anywhere around the world where they can get a signal on their phone.

SafeZone users have reported good results. There are many reports of how it has helped security officers deal with medical emergencies, how it reduced criminality, how it protected during terrorist incidents, how it improved customer service and how it resolved problems halfway around the world.

A student caught up in flooding in southern India was successfully evacuated to safety through the app. An employee was reached by first aiders moments after suffering a heart attack. A user was given advice and reassurance in South America when she missed her flight. A sexual assault was prevented by timely intervention.

Empowering Security Teams

In particular, SafeZone empowers security teams to intervene more effectively and provide first response services. This has implications for the way organisations think about security control operations.

In this new world, a combination of more powerful technology, higher skills and a new understanding of risk is transforming the way security departments work, said Darren Chalmers-Stevens, CriticalArc's Managing Director EMEA and APAC.

Darren Chalmers-Stevens, CriticalArc

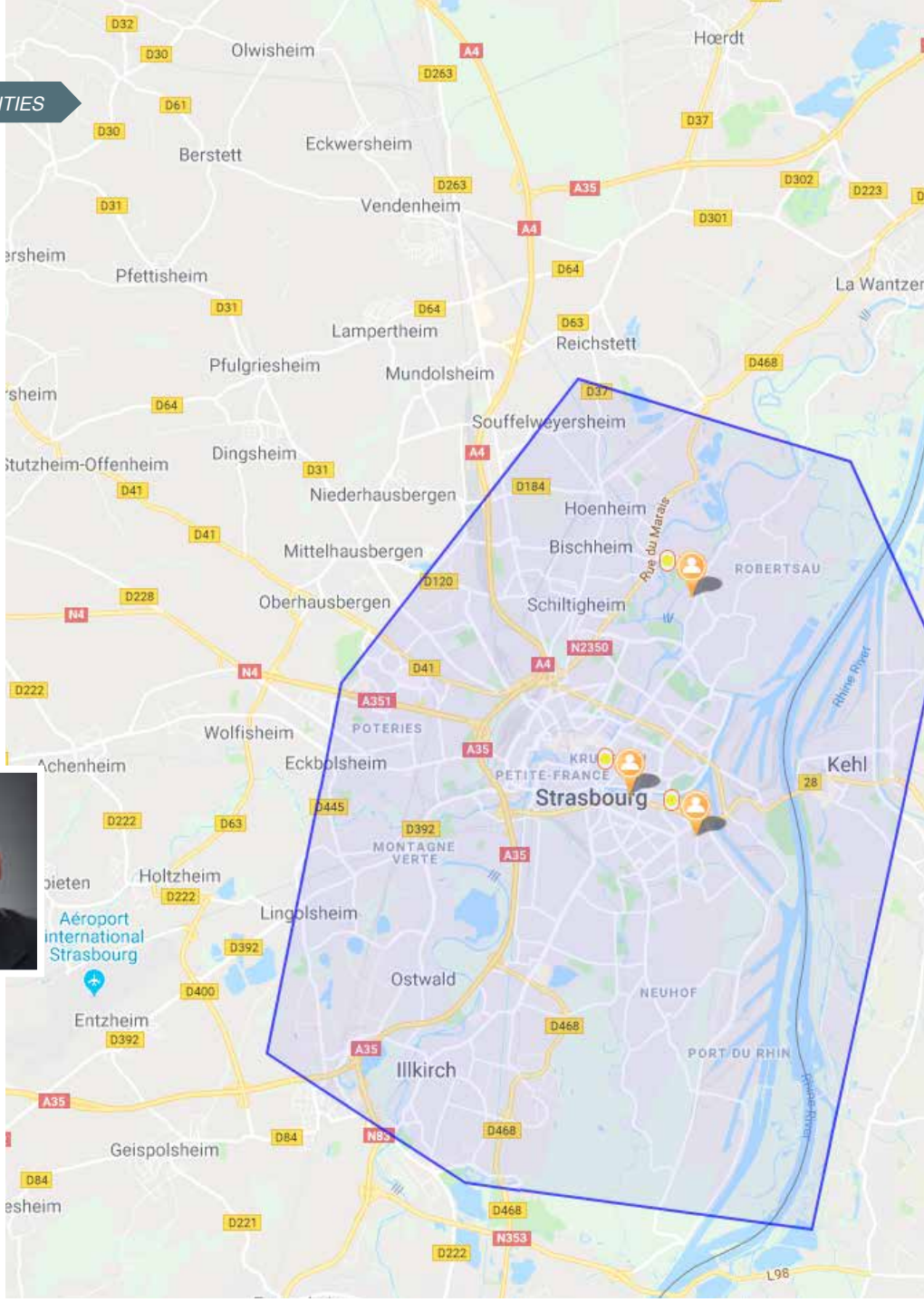
"Security staff have renewed importance as first responders, providers of customer care and ambassadors for the brand."

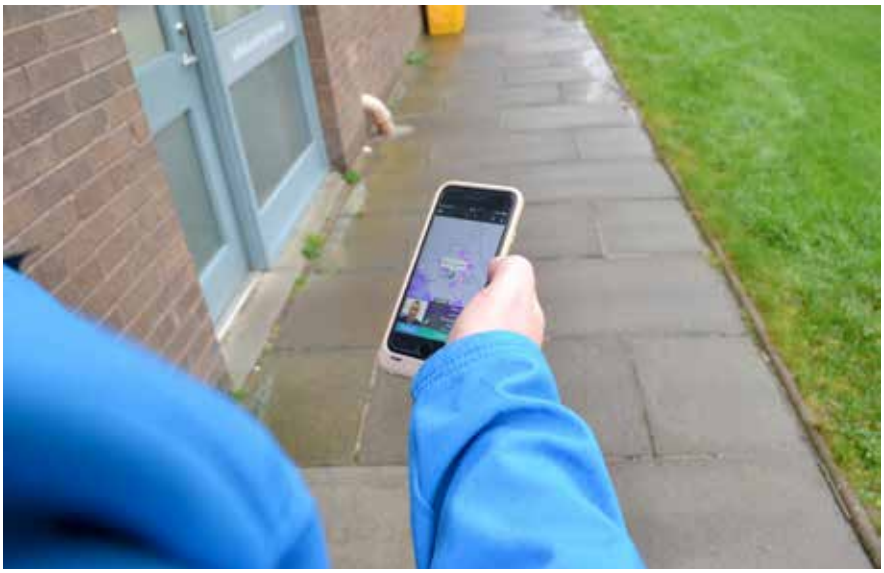
Currently security technology is valued for its ability to replace people and cut costs, as remotely monitored systems means smaller guarding teams and lower wage bills. Now a new generation of more highly skilled and motivated security officers are taking the lead, and they are spending less time patrolling empty buildings and more time interacting with people.

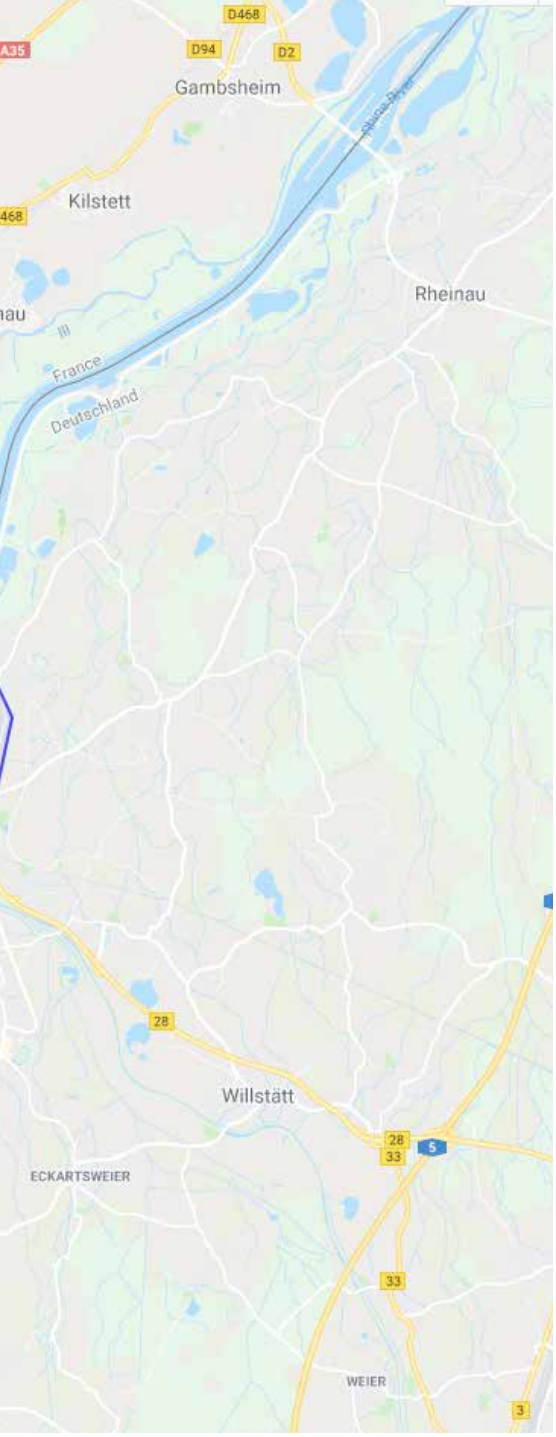
"Security teams are finding that their new ability to communicate directly with individual service users is giving them a new, more important role to play," said Chalmers-Stevens.

What's so different about SafeZone is that it's not just the technology that's transformative, but the way people are using it, argued Chalmers-Stevens,

"Each time we put this in the hands of a safety or security manager, new







applications and benefits become apparent. It's letting them be more forward-looking. So with each system that goes live, we recognise additional applications for the technology."

A Network Of Safe Zones

CriticalArc envisions a global community made up of SafeZone users working closely together, linking their systems in a shared service model for on-the-ground support for each other's users.

It's already happening at city level in different countries, with campuses, hospitals and local care agencies cooperating to extend protection for service users citywide and even state-wide.

With police and ambulance crews often over-stretched, this model has the potential to allow skilled security officers to fill the void in the first vital minutes of an emergency incident.

If somebody has particular medical needs for example, and he is moved from one protected zone to another, information of his medical needs will be automatically shared with the first-responding security team that is closest (subject to the user's consent), allowing the right help to be dispensed more quickly.

The same model is also being developed internationally, with SafeZone operators collaborating across borders to provide support for service users who are travelling abroad.

In February 2019, over 100 senior executives and security leaders from around the world will gather in the UK for a landmark user conference. These men and women are responsible for thousands of protected locations - including campuses and city centre sites – each location with thousands of registered users and each facing similar challenges, ranging from handling routine calls for assistance to planning for major emergencies. SST

2019 Will Be A Year Of Malware For Southeast Asia

▸▸ **Jeff Hurmuses,** Area Vice President and Managing Director, Asia Pacific, Malwarebytes

Here is our prediction for the Asia Pacific region in 2019: It's going to be a rough year.

Southeast Asia, in particular, is today a prime target for cyberattacks as the region becomes more closely intertwined in terms of trade, capital flows and technology, making it more susceptible to complex cyberattacks. What makes the region attractive to cyber criminals is also the fact that many users in the region use outdated operating systems and browsers, making them easy targets.

In 2019, there will be more malware activity in the Asia Pacific region than ever before, especially malicious cryptomining. Cryptomining is where hackers take over a host computer's resources and use them to mine cryptocurrencies without the user's consent.

The writing is already on the wall; in the past quarter 65% of total cryptomining malware detected occurred in Asia Pacific.

Here are my other security predictions for 2019 for the Asia Pacific region:

- **Under-the-radar malware will be the biggest threat**

Recently, there has been a noticeable shift in malware development methodology. Threat actors are awakening to the fact that the longer they hold an infected endpoint, the more their profit increased. As long as they survived attempts at remediation, they could turn the money taps back on.

The 2017 Cost of a Data Breach study by the Ponemon Institute and IBM revealed that the mean time taken to identify an organisational breach was 197 days, while the time to contain that breach was 69 days. That is 266 days to remediate an attack. How much critical information could be siphoned in 266 days? How much data was lost in the 69 days between the detection and containment?

Persistence — established by not only lengthening the time to detection, but also keeping a tentacle in the compromised device to later regrow the malware after detection — has now become as important to malware writers as avoiding detection.

A new class of malware has recently emerged: under-the-radar malware. Built around the dual purposes of avoiding detection and sustaining persistence, these difficult-to-remediate threats are a cause for concern for businesses today and in the future as they grow more sophisticated and pop up more frequently.

So while ransomware made the headlines last year, in 2019 we will see more attacks designed to avoid detection and maintain persistence.

It's already been on the increase this year, with Philippines being one of the most targeted countries in the region. Take for example Emotet, a banking trojan malware programme that uses the same vulnerabilities that WannaCry and NotPetya exploited; Philippines is the most infected country with nearly 60,000 instances of Emotet infections detected by Malwarebytes.

In terms of volume, most of these attacks take the form of fileless attacks and compromises.

These have had success in attacking businesses because the majority of past and present security solutions are designed to detect file-based malware. Those traditional security solutions, deployed at almost every business in the connected world, are simply not built to detect and remove malware that resides in memory rather than on the disk.

This growing gap in protection has led to a tremendous increase in attacks, compromises and resulting data theft from fileless attacks.

> ***In 2019, there will be more malware activity in the Asia Pacific region than ever before, especially malicious cryptomining. Cryptomining is where hackers take over a host computer's resources and use them to mine cryptocurrencies without the user's consent.***

In fact, fileless malware attacks are estimated to account for 35% of all attacks in 2018, and they're almost 10 times more likely to succeed than file-based attacks, according to a recent Ponemon Institute report.

Fileless malware is just one example among many attack methodologies currently evading traditional security defences and maintaining persistence of compromise. From a single missed fragment of the exploiting code, the attacker can rebuild the infection and maintain the compromise.
|
This class of difficult-to-remove malware requires a new approach if businesses are to stop the threats before they create damage. The security providers of today need to be able to pivot based on the newest threat vector and quickly develop the tools to combat it, because the future is not full of easy-to-detect junkware, but sophisticated and dangerous malware programmes that are difficult to detect and difficult to remediate.

- **New, high-profile breaches will push the security industry to finally solve the username/password problem**

The ineffective username/password conundrum has been a big concern in Asia Pacific this year, and specially in Singapore where extremely weak numeric password systems have contributed to three of the biggest data breaches to date in the nation: the SingHealth cyber attack, the Iranian hacking syndicate that penetrated four Singapore universities, as well as the alleged attack on Singapore Airlines' KrisFlyer frequent flyer programme. There are many solutions out there—asymmetric cryptography, biometrics, blockchain, hardware solutions and more - but so far, the security industry has not been able to settle on a standard to fix the problem. In 2019, we will see a more concerted effort to replace the password solution once and for all.

- **Threat actors will turn their efforts to businesses and networks with thousands of endpoints, to generate a greater ROI**

It looks like threat actors are searching for more bang for their buck, and business targets are returning more value for their efforts. Infecting a network of endpoints is more lucrative than infecting individual laptops. Criptominers, Banking Trojans and ransomware, traditionally aimed at both businesses and consumers, will be leaning more towards business targets.

- **Cyber criminals will turn more and more to artificial intelligence to create malicious executables**

While the idea of having malicious artificial intelligence running on a victim's system is pure science fiction at least for the next 10 years, malware that is modified by, created by and communicating with an AI is a very dangerous reality. With an artificial intelligence attacker, you can have the manual, dynamic benefits of a real person behind the keyboard, while also having the attack completely automated. AI controllers will enable malware to modify its own code to avoid being detected on the system, regardless of the security tool deployed.

- **Digital skimming will increase in frequency and sophistication**

Cyber criminals are going after websites that process payments with the goal of compromising the checkout page directly. Whether you are purchasing roller skates or concert tickets, when you enter your information on the checkout page, if the shopping cart software is faulty, information is sent in clear text, allowing attackers to intercept in real time. Security companies saw evidence of this with the British Airways hack. SST

Cybersecurity Experts Predict 2019

What do cybersecurity experts from different fields think will go down in 2019? Here are some of their predictions.

Apathy Will Set In

"We are about to enter an era of mass complacency. While in the past, headlines on data breaches caught attention and left readers shocked and concerned, today they are increasingly becoming the norm. No longer are data breaches isolated events; we are now seeing cases of individuals having their personal data compromised for the second or third time and companies being attacked again and again. All of this will contribute to an apathetic mindset in 2019 – a the-worst-has-already-happened mentality that is extremely dangerous.

Research by ISACA in 2017 found that only 50% of CIOs and IT leaders took any meaningful action towards improving security following the WannaCry ransomware attack. Many are using their security budgets to meet compliance requirements and avoid fines, when they should be striving to turn the situation around.

At the same time, 2019 will herald in a raft of laws aimed at alleviating the situation. 2018 has been a significant year from a regulatory perspective. GDPR came into effect and certain countries have begun bolstering security requirements around critical infrastructure. California has introduced a Privacy Act similar in nature to the GDPR, and has upped the ante by being the first state in the US with an Internet of Things cybersecurity law.

The proliferation of such laws is needed not only because new technologies necessitate guidance around their lawful use but also to compel organisations to meet certain minimum requirements.

Perhaps the largest surprise from a regulatory perspective throughout 2018 relates to mandatory disclosure laws. These laws, which require organisations to disclose details of data breaches, have been blatantly ignored by those who'd prefer to keep such attacks out of the public eye. Knowingly violating the law is a practice that we can only hope will decline as social pressure to announce such breaches ramps up."

Tony Jarvis, *Chief Technology Officer, AMA, Check Point Software Technologies*

IoT-Based Events Will Move Beyond Massive DDoS Assaults To New, More Dangerous Forms of Attack

"In recent years, massive botnet-powered distributed denial of service (DDoS) attacks have exploited tens of thousands of infected IoT devices to send crippling volumes of traffic to victims' websites. Such attacks have not received much media attention of late, but they continue to occur and will remain threats in coming years. At the same time, we can expect to see poorly secured IoT devices targeted for other harmful purposes. Among the most troubling will be attacks against IoT devices that bridge the digital and physical worlds. Some of these IoT enabled objects are kinetic, such as cars and other vehicles, while others control critical systems. We expect to see growing numbers of attacks against IoT devices that control critical infrastructure such as power distribution and communications networks. And as home-based IoT devices become more ubiquitous, there will likely be future attempts to weaponise them."

Hugh Thompson, *Chief Technology Officer, and* **Steve Trilling,** *Senior Vice President and General Manager, Security Analytics and Research, at Symantec*

Security By Design And Standards

"Currently software is still largely written without formal standards and processes behind it. Unlikely building bridges, software development is not a standardised repeatable job. That said, open source has been on the rise for a long time and is now commonplace.

I believe trust will grow in common building blocks based on open source software. Moreover, vertical software development standards will emerge more strongly. More effort will be placed on standards, audibility and accountability as seen in safety critical systems such as cars and aircrafts, where lives depend on correct software execution. These standards might evolve from the bottom up or they may be government regulated. Potential new verticals on the rise for this are financial services, solutions built around blockchain and security based on mobility solutions.

In 2019, we might see a rise of consortia within verticals to establish more security standards that are domain specific and that improve trust and interchangeability. Much of this might be built on open source components."

Dr. Ralf Huuck, *Senior Technologist, Synopsys*

Security Of Process Plants Will Be In The Spotlight

"Due to developments in recent years, the security of process plants will be in the focus in the coming year. Stress will be laid on three main points: First, basic protection of existing facilities which means properly applying state-of-the-art technology. Second, the identification and elimination of vulnerabilities. Third, the understanding and implementation of organisational and normative requirements. Other important trends of the future are open architectures, modular engineering and integrated diagnostic concepts."

Dr. Alexander Horch, *VP R&D and Product Management, HIMA*

Security Teams Will Need More Development And Engineering Skills

"Security teams used to focus on firewalls and endpoints and many security professionals cut their teeth as system and network administrators. Nowadays infrastructure is defined by code, breaches are increasingly caused by weak applications and automation is essential for under-staffed teams. This is changing the skillset required by security pros. We now also need to have a deep understanding of applications and an ability to build automation into our tools and processes."

Ross McKerchar, *Chief Information Security Officer at Sophos*

IoT Cyber Attacks Will Surge

"IoT attacks will remain an issue in the year to come. In Asia Pacific, many countries are moving forward with Smart City and Smart Nation initiatives. This opens the opportunities for a new wave of IoT cyber attacks.

In the healthcare and retail industries, we'll be seeing many more attacks. The reason is that the value of the data these industries are collecting is increasing. Investments must be made to protect the data within these industries and beyond.

In 2019, industrial control systems (ICS) and operational technology (OT) organisations will begin waking up to the changes taking place in the cyber landscape. I predict that we'll see more security investments occurring in this space. At the same time, security testing of OT (embedded) systems will grow considerably.

Security training is imperative. Attacks could be approached from a data poisoning perspective in which faulty information is intended to influence organisational decision making through the sensors deployed within the target city or nationwide. We'll also see the same old issues persist: hardcoded credentials and unpatched components, not very well designed OTA updates and continuous update policies."

Olli Jarva, *Managing Consultant, Synopsys*

Attackers Will Increasingly Capture Data in Transit

"We are likely to see attackers exploit home-based Wi-Fi routers and other poorly secured consumer IoT devices in new ways. One exploit already occurring is marshalling IoT devices to launch massive cryptojacking efforts to mine cryptocurrencies. In 2019 and beyond, we can expect increasing attempts to gain access to home routers and other IoT hubs to capture some of the data passing through them. Malware inserted into such a router could, for example, steal banking credentials, capture credit card numbers or display spoofed, malicious web pages to the user to compromise confidential information. Such sensitive data tends to be better secured when it is at rest today. For example, eCommerce merchants do not store credit card CVV numbers, making it more difficult for attackers to steal credit cards from eCommerce databases. Attackers will undoubtedly continue to evolve their techniques to steal consumer data when it is in transit."

Hugh Thompson, *Chief Technology Officer, and* **Steve Trilling,** *Senior Vice President and General Manager, Security Analytics and Research, at Symantec*

Many Jobs Will Be Taken Over By AI

"Many more business jobs will be staffed by bots in the year to come. Many people will learn that artificial intelligence (AI) and machine learning (ML) are already all around them, often making decisions that affect their lives, their families, their health and their jobs. If you think the average person is average, wait until you find yourself yelling at a bot over the phone."

Sammy Migues, *Principal Scientist, Synopsys*

A Lot More Phishing, A Lot Fewer Ransomware Attacks

"Phishing attacks will increase exponentially. The days of poorly worded messages filled with grammatical errors and cut-and-pasted logos are over. Messages are now more succinct and do a much better job of masquerading as legitimate correspondence. This will increase the success rate of phishing attacks. In fact, spear-phishing (phishing designed to target specific individuals or roles in a company) will become the norm. Since the cost and risk of mounting phishing attacks to plant malware or to steal credentials are so disappointingly low, phishing will continue to be one of the most prevalent attack vectors used by malicious individuals.

Meanwhile ransomware attacks will decrease. However basic malware will become commonplace. Once the holy grail of hackers (and feared by corporate security professionals), ransomware has decreased over the last year or so and that downward trend will continue into 2019. This is because fewer companies paid ransoms to recover data than expected, while malware/ransomware defences have improved. Ransomware will, however, remain in the hacker's toolkit, but will be used mostly as a distraction, to divert attention to files locked by ransomware, while a data harvesting attack is silently occurring elsewhere in the network. Whether delivered via email or visits to malicious websites, basic malware (keylogging, data mining and so on) will also increase as an attack vector of choice because of its simplicity and effectiveness."

Gene Scriven, *Chief Information Security Officer (Senior VP of Global Information Security) at ACI Worldwide*

More Corporate Adoption Of Behavioural Biometrics, More Industrial IoT Disruptions

"In Asia, we are far more accepting of using physical attributes like facial recognition or fingerprints to authenticate credentials. While passwords may change, physical biometrics are genetic and specific to each person, making it even more lucrative for hackers to exploit the serious vulnerabilities present in biometrics authentication. In 2019, we will see companies add behavioural biometrics with strong authentication, either based on advanced technology like FaceID or 2FA to provide a continuous authentication by incorporating a person's physical actions which will be very hard to mimic.

Also, IoT devices are gaining in popularity in Southeast Asia, from consumer homes to industrial IoT to initiatives like lampposts in Singapore's Smart Nation project. While attacks on consumer IoT are prevalent, the possibility of disruptions in manufacturing and similar industries raises the severity of the threat. In industrial IoT, attackers will target the underlying cloud infrastructure as millions of devices are connecting to the cloud for updates and maintenance. The access to these multi-tenanted and multi-customer environments will help attackers launch widespread attacks that will reap them much bigger rewards."

William Tam, *Director of Sales Engineering, Asia Pacific, Forcepoint*

Luxembourg City Tram Provides Safe Commute Again After 50 Years

After being shut down for 50 years, the Luxembourg city tram is up and running again. And it is now both safe and future-ready.

Between 1875 and 1964, trams transported passengers in the capital of the small country of Luxembourg before they were shut down. They remained shut for over half a decade.
However with experts estimating that the number of commuters in Luxembourg will double by 2030, the authorities decided to reactivate the tram lines to cope with this projected hike.

Modern Safety Technology

Luxtram awarded the French rail specialist Mobility the project and set Mobility the target of deploying signalling system that meets the highest safety requirements of SIL4. The plan was also to significantly increase the frequency of the trams in order to boost the number of transported passengers and to ensure the tram's viability for the future.

Instead of a system with conventional N.S1 relays, plans called for a space-saving solution with programmable logic controllers (PLCs).

The experts from Mobility worked closely together with the French HIMA branch on the design of the safety technology. HIMA is the world's leading independent manufacturer of safety systems. The goal was to develop a signalling solution that complies with SIL4 safety level according to CENELEC and install it directly on the tracks. Mobility took the opportunity to deploy a new concept based on technology from HIMA. The solution: modern COTS safety controllers from HIMA.

The signal systems along the route were renewed by Mobility and equipped with the powerful safety controls from HIMA. The HIMA controls make Luxembourg's tram traffic safer. They also make the tram faster; the high performance of the controls enables the time intervals between two trains to be shortened. This allows the operator to significantly increase train frequency and thus the passenger carrying capacity of the tram. At the same time, the open, modular COTS components help reduce lifecycle costs.

On 10 December 2017, operator Luxtram inaugurated the first leg. On a 3.5 km stretch between Luxexpo and Pont Rouge, eight stops were put into operation, including two transfer platforms. Six tram cars with a capacity of up to 420 people currently operate on this first leg.

By 2021, the route length is slated to be expanded to 16 kilometres with 24 stops and nine transfer centres, leading to the final stops at Findel Airport and Cloche d'Or. Once completed, 32 rail vehicles will travel on the tram route. The project will cost 565 million euros.

Space Savings

Luxtram's and Mobility's decision is in line with the trend towards standardised, open safety systems. More and more system integrators and railway operators worldwide rely on standardised, open safety systems to meet the requirements of urban transport with increasing volume of passengers, increasing connectivity, limited installation space and digitalisation.

By using the HIMA technology, Luxtram was able to save substantial space in the track area: the new control cabinets were able to be optimally integrated into the architecture of the stops and transfer platforms. At the LuxExpo stop, the installation of the HIMA safety controller solution in compact control cabinet directly on the track saved costs and removed the need to build a technical room. Used in traditional relay solutions, technical rooms are not only a major challenge for planners due to the lack of space in urban trams, they are also an additional cost factor when they need to be laid underground near the tracks in a densely built-up area.

The Technical Details - PLC instead of relay

- Three CENELEC SIL4 certified safety controllers type HIMatrix
- Long-term availability of at least 20 years in terms of spare parts and retrofit
- The entire tram route can be monitored centrally
- The Luxtram project was the first tram project with HIMatrix controllers
- More than 50 axle counters and 150 induction loops were installed on the leg

The Benefits - COTS solutions increase safety and reduce lifecycle costs

- **Maximum safety:** The safety controllers are certified according to SIL 4 CENELEC.
- **Space savings:** HIMA controllers can be installed in compact control cabinets directly at the tracks. As a result, space-consuming technology rooms are a thing of the past.
- **Flexibility:** The deployed signalling solutions based on the scalable, open HIMA systems can be optimally adapted to Luxtram's needs.
- **Future-proof:** Compared to conventional relays, the modern safety controllers are significantly easier to install and updates ensure they are kept in sync with the latest technology.
- **Time savings:** The operator completed the project six months ahead of schedule.
- **Increased capacity:** Thanks to increased computing power, Luxtram was able to significantly increase the operating frequency of the tram. According to the Luxembourg Ministry of Sustainable Development and Infrastructure, the average number of tram passengers on weekdays during the first two months of operation was 17,000 – more than double the forecasted number. SST

Consumer Video Surveillance Market Topped US$1 Billion In 2018

Acceptance of home video surveillance has grown. Sales revenue from Arlo, Nest and other standalone network video surveillance cameras will have reached US$1.1 billion in 2018, according to IHS Markit, a leader in critical information, analytics and solutions. In comparison, sales revenue was US$966 million globally in 2017.

The United States was by far the largest country for these camera types, representing about 48% of unit shipments in 2017.

The expanding sale is due to the growing acceptance of video surveillance for the home.

"Acceptance has grown in part because people now have more control over their surveillance systems," said Blake Kozak, principal analyst, smart home and security technology, IHS Markit. "Users of network systems can log in and view footage using their smartphones, share clips via social media or speak to their families through two-way audio-enabled cameras. Cameras are becoming a gateway into the home, expanding their use beyond just security."

Consumer video cameras are rapidly evolving. Some of the biggest trends in consumer video cameras today include improvements in camera resolution and the transition to 4K, analytics and battery-powered cameras.

Impact Of 4K

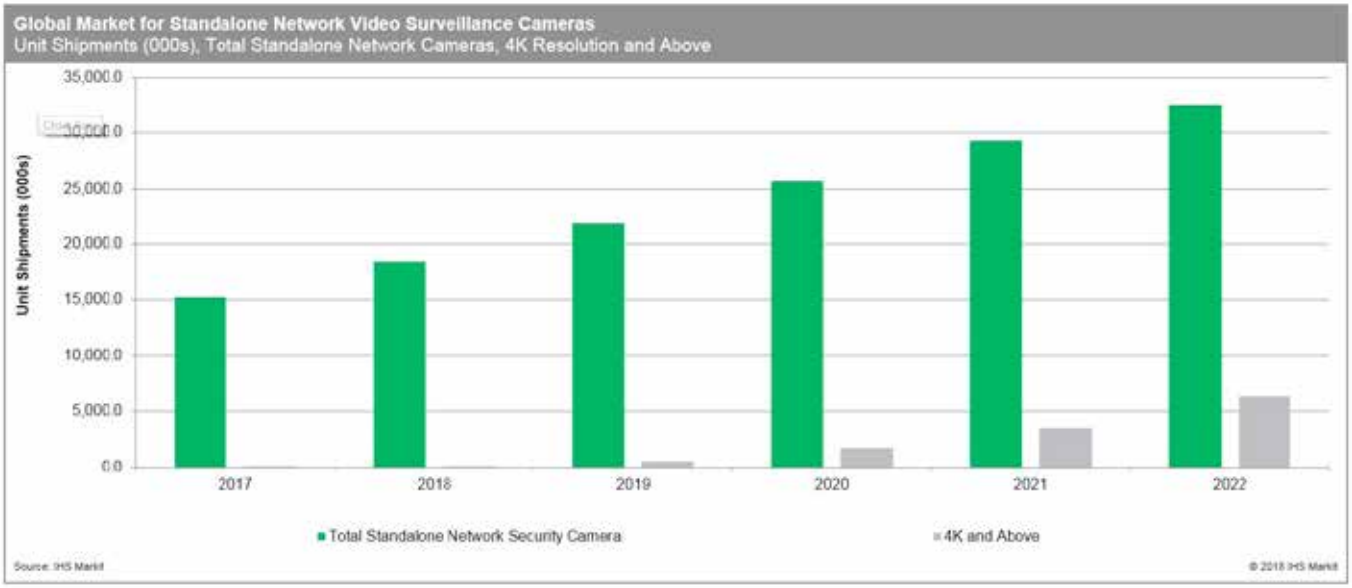
In 2017, under 1% of standalone network cameras across the globe were 4K resolution or above. However by 2022, about 20% will be 4K.

For 2018, 720 pixels or lower was the most popular resolution choice, with about 48% of cameras sold featuring this resolution.

Most vendors now promote 4K as a solution for wide-area surveillance, claiming fewer cameras can be used to cover the same area. In fact, a digitally zoomed image from a 4K camera is still a 2-megapixel image. However this resolution provides a much more usable degradation of resolution quality than high-definition (HD) footage, where digital zooming quickly reduces the image quality below video graphics array (VGA) resolution. Higher-quality footage also allows for more advanced and reliable analytics to be developed.

"Camera resolution remains one of the most important measures that vendors use to convey the quality of their products to end users," Kozak said. "It is a feature consumers understand and are familiar with, due to past experiences purchasing televisions, personal computer monitors, smartphones and other consumer devices."

Two of the biggest barriers to adoption of 4K standalone security cameras are storage capacity and bandwidth. Storage capacities required for 4K footage can be quadrupled compared to storing HD footage.



4K cameras, which have roughly four times the resolution of HD cameras, also require four times the bandwidth, which means recording and management servers and software could also require upgrading to cope with the demands of managing multiple 4K streams.

Both storage and bandwidth requirements raise the cost of 4K cameras.

Deep Learning Analytics Is Still In The Future

Deep learning is one of the fastest growing fields in artificial intelligence. It allows computers to interpret large amounts of data in the form of images, sound and text. Deep learning analytics has yet to have a presence in the consumer market but it is an emerging trend in the professional security market. IHS Markit expects that as the adoption of cloud-based software services in the consumer industry develops and evolves, the market's adoption of deep learning analytics will be the natural next step.

In the past the only way to deliver analytics to consumers in the video surveillance industry was by developing rule-based algorithms. Rule-based analytics relies on a structure of "if-this-then-that" commands designed by developers to help the camera decide outcomes. These rules are fairly rigid by design and, as a result, these types of camera analytics are unable to solve problems they are not already programmed to encounter. However, rule-based analytics remains an excellent method for completing relatively simple tasks quickly and efficiently.

Increasing Adoption Of Battery-Powered Cameras

In 2017, battery-powered cameras represented about 24% of standalone network cameras globally. This is expected to reach 28% in 2022.

Battery-powered cameras have changed the face of the consumer video surveillance industry dramatically over the past five years, explained Kozak. Their flexibility and ease of installation has led to wider adoption of security cameras in the residential sector.

"The success of these products has also raised general consumer awareness of home surveillance systems. Battery life remains a key end user concern, which is why suppliers are now offering swappable battery pack accessories. When the camera's battery life is running low, the user can simply detach the spent battery pack and immediately replace it with a fully charged replacement. This solution provides consumers with a clear and simplified battery management process." SST

How Intelligent Can Retail Security Get?

Photo by Fancycrave.com from Pexels

Intelligent retail is the buzz word of the moment.

The retail sector is increasingly adopting innovative solutions from the fields of AI, robotics and big data analytics to reduce retail costs, drive sales, boost profitability and build customer satisfaction.

Intelligent retail also means smarter retail security, where electronic security solutions are applied to prevent losses, protect assets and investigate criminal behaviour.

One of the latest intelligent retail solutions on the market is Surveon POS Solution.

Offered by Surveon Technology, the end-to-end video surveillance solutions provider, Surveon POS Solution is able to extract transactional data from point-of-sale (POS) systems and pair the data with video from the time of the transaction.

This assists investigation into criminal activities such as stealing of cash and product shrinkage.

Product shrinkage is when a retailer has fewer items in stock than on the inventory list due to clerical error or goods being damaged, lost or stolen between the point of manufacture (or purchase from a supplier) and the point of sale.

Surveon POS Solution also records shipments and tracks parcels to boost security for retailers.

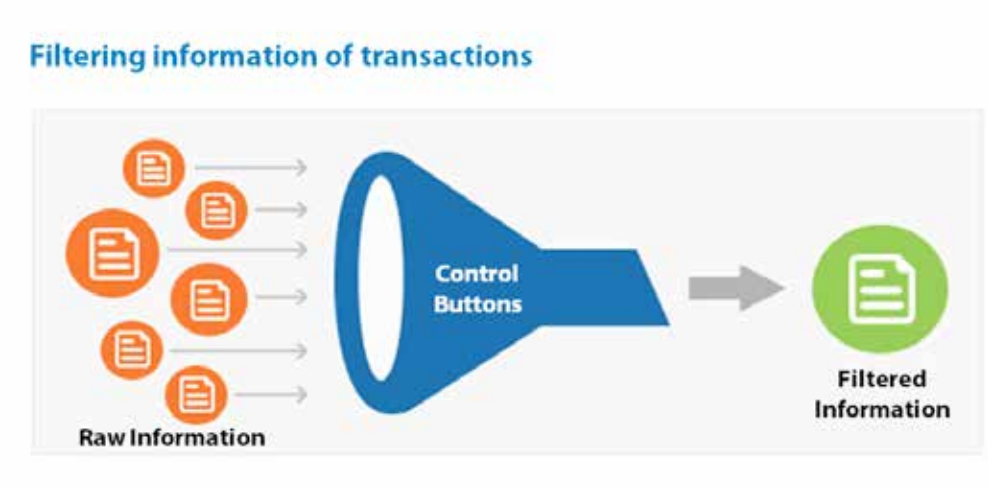
Easy Clarification For Transaction Errors

Surveon POS Solution provides transaction data with surveillance video to pinpoint where the responsibility for

the error lies when transaction errors happen. It supports 1/2/4/6 transactions live view and 1/2/4 transactions playback on the same screen.

Quick Monitoring With Multiple Filters

Finding the useful information from thousands of transaction data wastes time, especially for chain stores. Surveon POS Solution allows retailers to set filters through control buttons to get only valuable information on their transactions, enhancing efficiency.

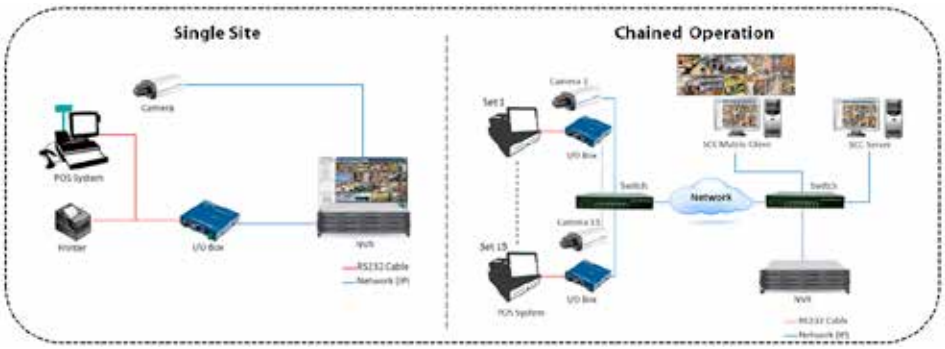


Saving Time With Log Search

To hunt down a specific transaction among thousands of data, Surveon POS Solution provides log search function. Just enter the time, camera and keyword in VMS, the system will find the transaction and its corresponding video, helping retailers save time.

Flexible Management With Multiple Architectures

Surveon POS Solution supports multiple architectures and local/remote monitoring for single store or retail chain operation, providing retailers with a flexible and scalable option to manage their system. In addition the Surveon product line, including camera, NVR and VMS, is compatible with major third-party POS systems, reducing the amount of time and effort needed to integrate the system. SST



ANPR Camera Market To Grow 16.4% Through 2022

Global market revenue from sales of intelligent automatic number plate recognition (ANPR) devices will reach US$800 million by 2022 and increase at a compound annual growth rate of 16.4%, says global information provider IHS Markit.

This is because the types of ANPR applications have increased and so has the range of offered functionalities.

Greater Accuracy, More Functions

Advances in video analytics and the processing power used in modern ANPR devices are reshaping the market, said IHS Markit analyst Anna Sliwon.

IHS Markit analyst Anna Sliwon.

Advances in video analytics have had a big impact on modern ANPR solutions, which has led to increasing adoption in access control and parking applications, including at hotels, hospitals and airports. These advances allow hotel chains, for example, to offer free parking to their guests at all associated hotels, not just the one where the guest is booked for his stay.

ANPR devices are now more likely to deploy analytics. They do not require back-office processing software to perform their functions, which reduces the overall system set-up costs and lowers adoption barriers across many industries.

Processing power improvements have also allowed ANPR devices to become much more compact, further simplifying installation.

Advanced algorithms now allow for real-time accurate object detection. This means, for example, that speed enforcement devices can offer more functions than ever before, such as seatbelt detection in vehicles and helmet detection for motorcyclists. The more advanced algorithms used in these devices rely on machine learning and deep-learning techniques to analyse recorded images for seatbelt or helmet presence.

This recognition process is very complex, because the ANPR camera needs, for example, to make out the image of the seatbelt from an image that contains a lot of background noise, such as light reflections from the car windshield and shading and obstructed views caused by a driver using a sun visor.

Helmet detection and seatbelt detection have helped to transform speed enforcement devices into multi-function devices that improve the efficiency of law enforcement agencies. Detection of dangerous driving, for example detecting whether a car is tailgating an emergency vehicle or whether it is driving between two lanes of traffic, is another

important add-on feature enabled by analytics powered with artificial intelligence (AI).

Red light enforcement is yet another key ANPR application that has benefitted greatly from advances in analytics. Traditionally two separate devices must be deployed in one location – one to read the licence plate of the car and another to record the red light. Modern devices with improved analytics are able to perform both tasks using a single device. This lowers system cost and speeds up ticket processing for violations.

More Data, More Privacy Concerns

Despite the great promise of advanced analytics, there are barriers to broader adoption of ANPR systems, reports Anna Sliwon.

Concerns over privacy is one hurdle. As ANPR systems gather more data across industries, and additional devices are deployed in more locations than ever, concern is growing over the privacy rights of vehicle drivers. The public is questioning why ANPR images are being recorded, as well as where they are stored and how secure they are. These concerns will have to be proactively addressed by manufacturers and installers alike, to prevent a public backlash against these technologies.

System cost is one of the biggest barriers to adoption. In countries where the cost of labour is quite low and the concepts of smart cities are not very well developed, the law enforcement agencies may prefer to continue conducting manual checks. Private businesses might not be willing to invest in training their staff in how to operate ANPR devices.

What's next for ANPR? Advanced analytics are transforming ANPR devices into multi-purpose detection systems, which fit very well with the concept of safe cities and smart cities, despite many other competitive technologies at the core of these systems.

According to Anna Sliwon, the next stage for ANPR systems is to integrate facial recognition with number-plate recognition. While these two functions have already been combined in some access control applications, the detection is still performed by two separate cameras, mostly due to installation angles and other practical factors. Ahead, improvements in camera features and analytical algorithms could open the door to these two features combined into one single system, which would greatly improve the investigative capabilities of these devices. SST

Nine Out Of 10 Consumers In Asia Pacific Don't Trust IoT Security

According to the latest survey by The Internet Society, consumers in Asia Pacific like IoT devices. They just don't trust that these devices are secure.

The Internet Society is a global non-profit organisation dedicated to ensuring the open development, evolution and use of the Internet. The findings is from the fifth installment of its Asia Pacific survey on policy issues. Internet of Things (IoT) is the rapidly expanding network of devices, physical objects, services and applications that communicate over the Internet.

The 2018 survey found that IoT devices are rapidly gaining traction in the region: the majority of respondents indicated they already own IoT devices and have plans to purchase more. Seven in 10 respondents own at least one IoT device and close to half already own three or more devices. Furthermore, close to three-quarters of the respondents plan to purchase an IoT device in the next 12 months.

The most popular IoT devices were: Internet connected appliances like smart TVs and fridges, connected wearables, fitness monitors, voice command systems like Google Home and virtual reality headsets.

However consumers in the region have deep-seated concerns about the security of their IoT devices.

Asia Pacific consumers clearly lack confidence in manufacturers. The vast majority – 90% of respondents – said they do not trust IoT manufacturers and service providers to secure their device.

Two out of three respondents said that security is one of the key factors that would influence their decision to purchase an IoT device. The other top factors in the purchase decision include device features, pricing and device brand. Internet users in Asia Pacific want security and privacy guarantees for their IoT devices.

> *"The most popular IoT devices were: Internet connected appliances like smart TVs and fridges, connected wearables, fitness monitors, voice command systems like Google Home and virtual reality headsets."*

The majority of respondents (60%) who do not own an IoT device stated they are unlikely to use an IoT device if there is no guarantee that the personal information collected will be fully protected.

Respondents were also concerned about:

- their personal information being leaked (81%)
- hackers taking control of their devices and using them to commit crimes (73%)
- hackers gaining access to their personal information (72%)
- being monitored without their knowledge or consent (71%)

Despite their overwhelming concern about security and privacy, consumers in APAC feel they do not have the ability to protect themselves or have already failed to do so.

Only half of those who own an IoT device have changed default passwords, and only a third have read the privacy and policy terms and conditions of their device. Notably, of those who did not change device passwords: 30% decided not to, 10% did not know how to and close to 50% claimed their device did not have one. SST

Vulnerabilities Found In Market-Leading Drone Platform

Drones, especially those with high-definition cameras, are now commonly used by enthusiasts and professionals alike. While there are worries about drones invading the privacy of others when in the wrong hands, drone users themselves may be at risk, especially if their data and personal information lives in the cloud.

This was demonstrated in November when Check Point Software Technologies Ltd found vulnerabilities in market-leading drone maker DJI. DJI is a leader in civilian drones and aerial imaging technology.

The vulnerability resides in the user identification process within DJI Forum, a DJI-sponsored online forum about DJI products. Check Point's researchers discovered that DJI's platforms used a token to identify registered users across different aspects of the customer experience, making it a target for hackers looking for ways to access accounts.

The report submitted to DJI, in accordance with DJI's Bug Bounty Program, describes how DJI consumer users who had synced their flight records, including photos, videos and flight logs, to DJI's cloud servers, and DJI corporate users who used DJI FlightHub software, which includes a live camera, audio and map view, could have become vulnerable. An attacker could have potentially gained access to a user's account through the vulnerability. This vulnerability has since been patched and there is no evidence it was ever exploited.

The bug bounty programme allows the drone maker to fix any vulnerabilities detected.

"We applaud the expertise Check Point researchers demonstrated through the responsible disclosure of a potentially critical vulnerability," said Mario Rebello, Vice President and Country Manager, North America at DJI. "This is exactly the reason DJI established its Bug Bounty Program in the first place. All technology companies understand that bolstering cyber security is a continual process that never ends. Protecting the integrity of our users' information is a top priority for DJI, and we are committed to continued collaboration with responsible security researchers such as Check Point."

Given the popularity of DJI drones, it is important that potentially critical vulnerabilities like this are addressed quickly and effectively, said Check Point. SST

CallMe App Allows Homeowners To Screen And Admit Home Visitors From Anywhere

For new-build apartment blocks, IPercom by Urmet is a cost-effective solution to the problem of how to admit visitors when you are not home. Urmet specialises in the support and delivery of 2-wire and IP door entry systems for small, medium and high-volume multi-dwelling apartment developments.

With Urmet's CallMe app, homeowners are able to receive video entry calls on their smartphone or tablet as well as on the traditional fixed station in their apartment. Homeowners can view who is at their door using their mobile device and grant access even when they are out of the apartment, whether they are in in a coffee shop, at work or on holiday.

The set-up is straightforward. Homeowners download the CallMe app and follow the easy set-up guide to create an account. Their username is then updated on the Max touchscreen inside the apartment and calls set to 'remote' so that they can be received on both the apartment station and the CallMe app via WiFi or 3G/4G.

Only one Internet connection is required for the whole building, meaning that an entire block of apartments can enjoy the benefits of call forwarding from the landlord's single Internet connection. There is also no licence required, which further reduces the cost, and no gateway, so that no additional equipment needs to be installed.

The solution also conforms to Secured by Design requirements, under which a fixed apartment station is compulsory so that residents can use the video entry security system and answer the call even if they do not have the app.

The app is free to download and available for both Android and iOS. SST

For new-build apartment blocks, IPercom by Urmet offers a cost-effective solution to the problem of how to admit guests when you are not home.

Forging Safer Cities With Intelligence Sharing

▸▸ **By Jagdish Mahapatra,**
Managing Director, Asia
CrowdStrike

Cyber attacks on cities and critical infrastructure are increasing with the adoption of technology causing them to be more vulnerable. While technology has brought about greater connectedness and socio-economic benefits, a lack of cybersecurity preparedness can have serious consequences in the form of security vulnerabilities. Security breaches may see the leaking of sensitive citizen information, and in more serious cases, even cause physical damage and disruption of essential services.

Governments in Asia are increasingly finding themselves the target of e-criminals and nation states that engage in a sophisticated array of tactics in their cyber attacks. These attacks have the potential to drain millions of dollars from national economies and disrupt infrastructures and essential services. These attacks are perpetrated not only by opportunistic hackers working alone, but also by organised criminal gangs, activist collectives and even nation states.

As threat actors become better organised and more sophisticated in their methods, traditional defence methods and tools are proving less effective.

For effective containment of these threats, a security posture supported by intelligence can make a big difference.

Vulnerability Of Vital Networks

Today, businesses rely heavily on network to store everything from the digital records of customer information to corporate strategy and sensitive product information. These networks are prime targets for adversaries and are complex to secure as they often consist of hundreds of thousands of endpoints, with every desktop, laptop, smartphone, server and router serving as a potential entry point for a hacker.

Cybersecurity, including protecting critical infrastructure, is now widely recognised as a national security issue by governments worldwide.

In June 2018 in Singapore, adversaries infiltrated the databases of SingHealth, the nation's largest healthcare institution group, to steal the data of 1.5 million patients. Government entities in Taiwan, Malaysia and the Philippines were also the target of threat actors aiming to steal data, disrupt operations or destroy infrastructure.

The ability to share tactical and strategic threat intelligence will enable both governments and private organisations to sound the alarm on new attacks and evolving adversary tactics, thereby safeguarding the community collectively.

A Case For Intelligence Sharing

A recent report by CrowdStrike highlights that actors are using a variety of novel tactics to target specific sectors. These actors demonstrate exceptional creativity and perseverance in defence-evasion and living-off-the-land techniques. Since threats and attacks are often targeted at sectors such as technology, finance, banking and retail, collaboration between peers can help improve the relevance and quality of the shared intelligence. The ability to work closely together in a more collaborative way ensures that industry leaders can better understand the threat landscape and gain insights into practices deployed by others in the industry to safeguard their own organisation.

There are two factors that may hinder the open sharing of threat information. Companies may be afraid of leaking sensitive customer information, while government bodies have strict regulations when it comes to the information they can share.

However, the number of new threats uncovered on a daily basis are accelerating cooperation and intelligence sharing among vendors. It is becoming increasingly clear that the tactics hackers employ today are growing in sophistication, at a level far beyond what many enterprises are currently prepared to defend against.

Paving The Way For Sharing

Government-led initiatives can pave the way for businesses to join the threat information sharing movement. Asia is beginning to take steps to bolster cybersecurity for the region, with the Asean Ministerial Conference on Cybersecurity set up in 2016 for leaders from ASEAN member states to discuss the coordination of regional cybersecurity efforts.

In Singapore, the Cyber Security Agency of Singapore and the Financial Services Information Sharing and Analysis Centre recently signed a Memorandum of Understanding for both parties to collaborate on sharing security threat intelligence. It also paves the way for joint exercises designed to protect the financial services sector, a sector where Singapore is a regional leader.

This comes after Singapore introduced a holistic cybersecurity strategy in which a key goal is to step up protection of the nation's essential cybersecurity services in key sectors such as banking and finance.

Threat intelligence is important in providing context and understanding of cyber adversaries and their motivations, and better hone organisational defences in the context of the threat landscape. The success of e-criminals in orchestrating major data breaches over the world can be attributed to the open sharing of knowledge and tools for a long time. The community needs to follow suit and begin to work together on the global, regional and country levels in terms of information sharing to stay ahead of cyber crime.

Different types of intelligence can be used to harden defences. Tactical intelligence, for example, is information that can immediately improve defences against known vulnerabilities and attacks. This includes IPs or URLs, malware signatures and suspicious patterns, or other indicators that can be added to your preventative tools.

Meanwhile strategic intelligence refers to high-level activities that an organisation can take to properly calibrate its security posture. Examples include information about new attack methods, shifts in targeting behaviour by threat actors, or political or economic events that are likely to inspire a shift in threat actor activity.

Strategic intelligence is not as simple for an organisation to leverage as tactical intelligence but it may ultimately prove to be more valuable because it can inform both security and business decisions.

What is clear is that governments across the region have a central role to play in the sharing of threat intelligence to forge safer cities for all. SST

Smart Thermal Cameras Keep Art Treasures Safe At The Louvre Abu Dhabi

Art treasures at the Louvre Abu Dhabi museum located alongside Abu Dhabi's coast are being safeguarded by SightLogix's SightSensor smart thermal cameras. The smart intruder detection system has been providing waterside security for this innovative architectural facility since it opened in 2017.

The security demands of the Louvre Abu Dhabi go well beyond most other cultural sites.

Stakes are high. Many of France's most famous institutions have lent art to the high-profile museum. Aside from the valuable collections, any security breach at the site would significantly damage the security reputation of the UAE itself.

Hence the deployed system must perform at extremely high levels of reliability, while minimising disruption to visitor experience and the operations of the museum.

Located between sand and sea, the Louvre Abu Dhabi on Saadiyat Island also presents a difficult security challenge. Security systems must cover the surrounding body of water, detecting the presence of all watercrafts approaching the facility.

> *They detect intruders with great accuracy, even in the presence of reflections and water movement that would normally trigger a high number of nuisance alerts for smart camera analytics.*

SightSensor smart thermal cameras proved to be up to the task. At the Louvre Abu Dhabi, SightSensor cameras create a wide buffer zone of security over the surrounding body of water, detecting the presence of all watercrafts, including jet skis or rubber dinghies, approaching the facility or crossing the bay at up to 600 metres away.

The cameras provide volumetric coverage over water and do not require fences or clearly defined perimeters. They detect intruders with great accuracy, even in the presence of reflections and water movement that would normally trigger a high number of nuisance alerts for smart camera analytics.

The SightSensor's precision video processing automatically analyses the scene to determine security threats and communicates critical information about an intrusion's size, speed and location to allow guards to respond in real time.

When any target violates speed or distance rules, it is detected by a SightSensor, which sends an alarm, video of the event and the target's precise GPS location for display in CNL Software's IPSecurityCenter PSIM. This early warning detection system provides onsite security guards with instantaneous awareness of approaching intruders, allowing them time to analyse the video, determine the threat and react. SST

Symantec Unveils Industry's First Neural Network To Protect Critical Infrastructure From Cyber Warfare

In December, Symantec Corp. launched Industrial Control System Protection (ICSP) Neural, the industry's first neural network-integrated USB scanning station that defends against USB-borne malware, network intrusion and zero-day attacks on operational technology.

Symantec ICSP Neural utilises artificial intelligence to prevent known and unknown attacks on IoT and operational technology (OT) environments by detecting and providing protection against malware on USB devices. This prevents the devastating physical consequences of cyber attacks on OT at critical infrastructure.

The threat of cyber warfare is very real and the consequences – including physical damage and personal safety – are potentially devastating. OT is mission-critical in industries such as energy, oil and gas, manufacturing and transportation, but legacy systems are often outdated and nearly impossible to secure with traditional endpoint security. The industrial control systems that power critical infrastructure often run on outdated Windows systems leaving them vulnerable to both known and unknown threats.

In addition, companies typically rely on unscanned USB devices to update these systems, increasing the potential for malware infection and targeted attacks. For example, the infamous Symantec-discovered Stuxnet worm used USB-based malware to manipulate centrifuges in Iranian nuclear plants – ultimately sabotaging a key part of the country's nuclear programme.

ICSP Neural scans reveal that up to 50% of scanned USB devices are infected with malware.

"USB devices are given away at events, shared between co-workers and reused again and again for business and personal use, introducing the risk of accidental or malicious infection. The impact of connecting an infected device to a critical system can be devastating," said Patrick Gardner, senior vice president, advanced threat protection and email security at Symantec.

ICSP Neural stations scan, detect USB-borne malware and sanitise the devices.

Behind the scenes, ICSP Neural will retrofit existing infrastructure with a central nervous system to provide protection for critical infrastructure. On the front end, a rugged aluminum design offers a simple, intuitive user experience that clearly highlights potential threats.

Better Security Through Simplicity

Simplifying the scanning process is critical to overall security hygiene, as operational technology environments are often in remote areas or field operations, far removed from an organisation's IT teams. Hence the ICSP Neural scanning process is simple, requiring no specific security or IT

> *USB devices are given away at events, shared between co-workers and reused again and again for business and personal use, introducing the risk of accidental or malicious infection. The impact of connecting an infected device to a critical system can be devastating.*

training. Once connected, ICSP Neural emits visualisations and real-time signals through the LED light ring that indicate when malware has been detected and sanitised.

Protection Against The Most Advanced Threats

The Symantec-designed neural engine harnesses Symantec's threat intelligence network to increase detection efficacy by up to 15%. It also detects adversarial machine learning attempts and initiates self-learning to provide protection against unknown threats.

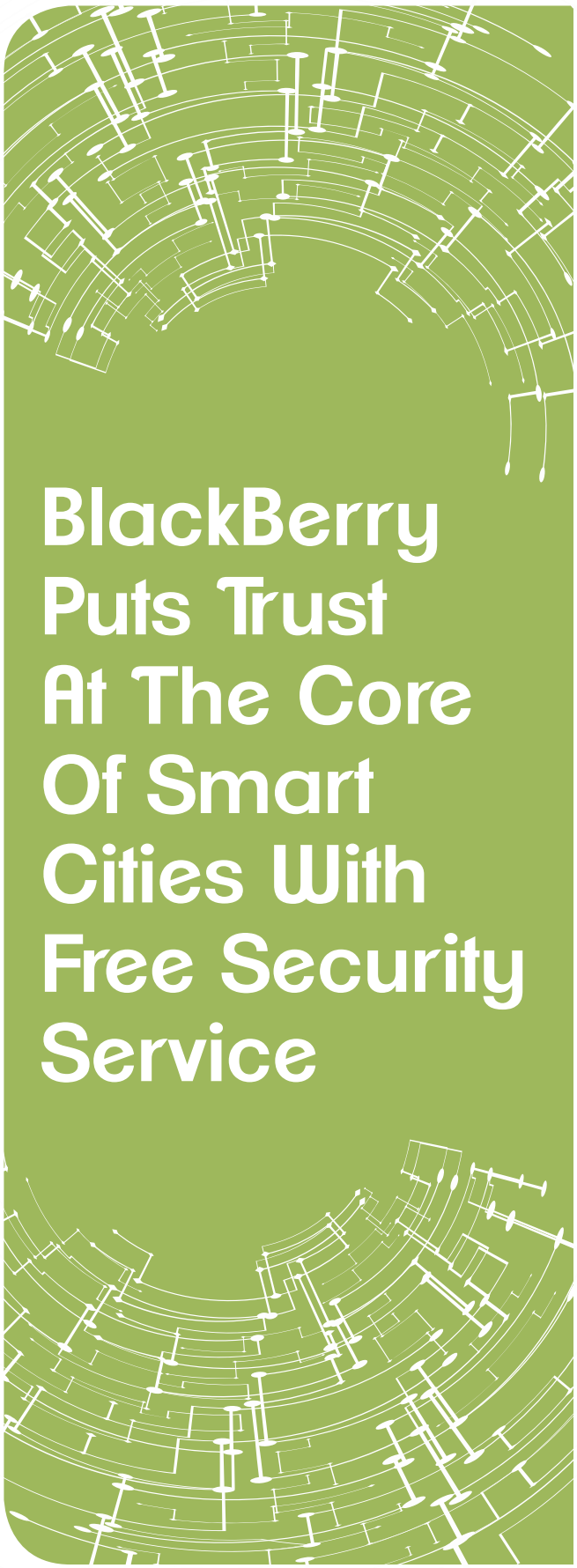
The AI-powered technology can learn in real time, leading to sustained efficacy with limited internet connectivity. These artificial intelligence and organic self-adaption capabilities can protect organisations against emerging and future attacks. The neural engine enables high-intensity detection with near-zero false positives (as low as 0.01%).

These capabilities are accomplished using just a tenth of the bandwidth of other similar solutions - an indispensable feature for systems using VSAT connections.

ICSP Neural supports a full range of OT and IoT devices and systems. The optional enforcement process prevents use of unscanned USBs with less than a 5MB installation footprint and can be deployed on operating systems from Windows XP to Windows 10 (Linux support is planned in 2019).

ICSP Neural complements the latest version of Symantec's Critical System Protection (CSP) software; a flexible and compact behavioural security engine built with application whitelisting, infused with anti-exploits for managed or standalone devices.

It is available for pre-order now and is expected to ship in early 2019. SST



BlackBerry Puts Trust At The Core Of Smart Cities With Free Security Service

The concept of 'smart cities' is about using technologies and connected data sensors to enhance infrastructure and city operations, which, ultimately, enhance the way we live and work in these cities.

However, to be truly smart, cities must be safe and secure. With millions of physical and digital connected devices powering smart cities, infrastructure like hospitals and roads as well as offices and homes are far more vulnerable to attacks and breaches, sometimes with potentially fatal consequences. A breach that compromises data also impacts any system that uses that data. This is changing how any organisation with a duty of care is planning for risk in an increasingly complex world – and this is a critical consideration for smart cities.

One city cannot manage this on its own. To be successful, it is critical for local governments and global industries to work hand in hand to ensure standards are in place and that security is built in at every layer.

This is why BlackBerry just announced a new Security Credential Management System (SCMS) service that arms private and public sectors around the world with the ability to accelerate the development of smart cities and intelligent transportation systems. The company provides technology that allows endpoints to trust one another, communicate securely and maintain privacy.

BlackBerry is offering the service free to automakers and public offices involved in smart city and connected vehicle pilots.

Boosting The Trust In Systems

SCMS was first launched in North America, but it is now being rolled out globally. The service provides the mechanism for vehicles and infrastructure to exchange information in a trustworthy and private manner using digital certificates. This may include the authentication of trusted control points and sensors, including Connected Vehicle V2X Onboard Units (OBUs) and roadside equipment (RSE) infrastructure such as pedestrian crossings and traffic management systems.

As connected vehicle applications exchange information among vehicles, roadway infrastructure, traffic management centres and wireless mobile devices, a security system is needed to ensure that users can trust the validity of information received from other systems.

Blackberry's SCMS service is based on BlackBerry's Certicom technology and offers a secure and reliable hosted Public Key Infrastructure that can manage certificates on behalf of an organisation or an entire ecosystem. The service is designed to scale to support national and transnational deployments, allowing OEMs and public officials to take advantage of a turnkey cloud-based service for vehicle-to-infrastructure (V2X) certificate issuance and lifecycle management. BlackBerry can also support hybrid SCMS solutions optimised for high-volume vehicle production.

"The future of autonomous vehicles cannot be realised until intelligent transportation systems are put in place," said John Chen, Executive Chairman and CEO of BlackBerry. "By removing barriers such as security, privacy and cost, we believe our SCMS service will help accelerate the many smart city and connected vehicle pilot programmes taking place around the world."

The Canadian Minister of Innovation, Science and Economic Devleopment, the Honourable Navdeep Bains, said "Building on Canada's promising advancements in the field of autonomous vehicles, it will help our communities use information and communications technology in a way that is secure and safe to improve their residents' lives."

How Does Blackberry's SCMS Service Work

SCMS is the Security Credential Management System for V2X, a specialised public key infrastructure for connected vehicles. In Europe the SCMS is called the Cooperative Intelligent Transport Systems or C-ITS.

The purpose of the SCMS is to govern connected vehicle certificate management so that all players in the ecosystem can trust messages emanating from the system (from vehicles and from infrastructure) as being reliable and authentic. Certification Authorities (CAs) are entities that issue these certificates to individual V2X modules, but the governance model must be established through close cooperation between national governments and industry.

In this instance, where there is no real regulatory framework, BlackBerry is establishing its own SCMS using industry best practices for Certification Authorities, following WebTrust for CAs trust service model criteria.

"We only issue certificates to certified devices and trusted entities enrolled in our programme," described Jim Alfred, Vice President of Certicom Corp, a subsidiary of BlackBerry. "This ensures that communities using our service can rely upon the integrity of the V2X messages they are receiving. Once national policies (or transnational policies between the US and Canada) for V2X are established, we would rely upon them for policy oversight. For deployments using prototype systems, for example emerging cellular V2X (C-V2X) systems that are not yet industry standardised or certified, we can offer test certificates and help develop use cases that establish new connected vehicle and autonomous driving use cases."

There may be multiple CAs, but the centralised SCMS sets the policy and governs them all, managing a "global" CA trust list and subjecting subordinate CA entities to annual audits and a common policy framework. This will allow, for instance, a government entity to ask for credentials to be revoked for "misbehaving" devices.

BlackBerry's SCMS Service In Motion

BlackBerry's new service has been interoperability tested in multiple OmniAir Consortium PlugFests held earlier this year. The company's first project using the new SCMS service will be in partnership with Invest Ottawa, who will leverage it within a secure 16-kilometer road autonomous vehicle test track that resembles a miniature city, complete with pavement markings, traffic lights, stop signs and pedestrian crosswalks. The integrated public and private autonomous vehicle test tracks are equipped with GPS, DSRC, Wi-Fi, 4G/LTE and 5G, making this the first autonomous vehicle test environment of its kind in North America.

Roger Lanctot, Director Automotive Connected Mobility at Strategy Analytics, added, "BlackBerry is taking a major step forward in support of smart city and connected car development efforts. While regulators are still in the process of defining what such a system might look like and how it will be deployed, BlackBerry's offering will allow for the testing of various concepts and technologies right away in support of inter-vehicle and vehicle-to-vehicle and vehicle-to-infrastructure applications."

How SCMS Helps Governments And Private Sector Address Safety And Security Challenges Of Smart Cities

It is imperative to increase coordination between governments in the region as smart cities initiatives continue to gain momentum. Companies like BlackBerry, with its free CV pilot programme, will bolster coordination between governments.

Jim Alfred, Vice President of Certicom Corp

"At BlackBerry, we work with all seven of the G7 governments and 16 of the G20 governments. We believe in the collaboration of the private and public sector at the highest levels of classification to help keep data safe but as an industry, we can always do more," declared Jim Alfred. "We see a lot of opportunity for governments and private sector around the world to enable more coordinated, effective and cost-friendly critical communication networks. The end goal is to ensure that organisations are more crisis-ready and cyber-resilient, regardless of the threat." SST

LILIN Enables Voice Control Viewing Of Cameras And NVRs

Taiwan leader in advanced IP video surveillance LILIN has added voice activation capability to its line of IP cameras and network videro recorders.

LILIN Americas, an entity of Merit LILIN serving North, Central and South America, added the Amazon® Alexa® skill to its Device Hub™ device manager that allows its customers to simply ask for a live or recorded view from any supported LILIN IP camera or network videro recorder and have that view displayed on their TV monitor.

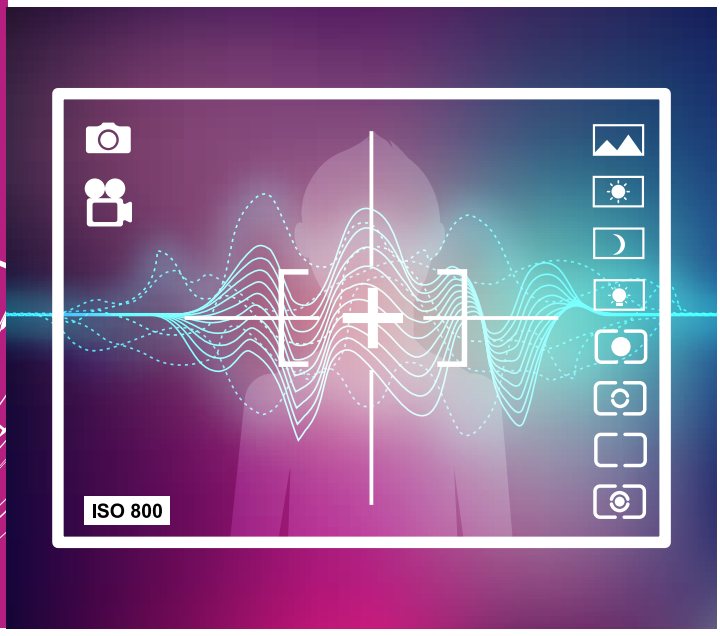
The Amazon Alexa converts the end user's command to a directive and sends that directive through the Device Hub. This fast, hands-free solution eliminates the need to navigate onscreen menus or have a mobile device in hand whenever a video is needed for monitoring.

Using the voice-controlled Alexa features of the LILINHub skill offers end users a convenient way to easily monitor their property, including viewing live camera feeds, playing back video footage from a LILIN network videro recorder and reviewing motion events, explained Joe Cook, General Manager of LILIN Americas.

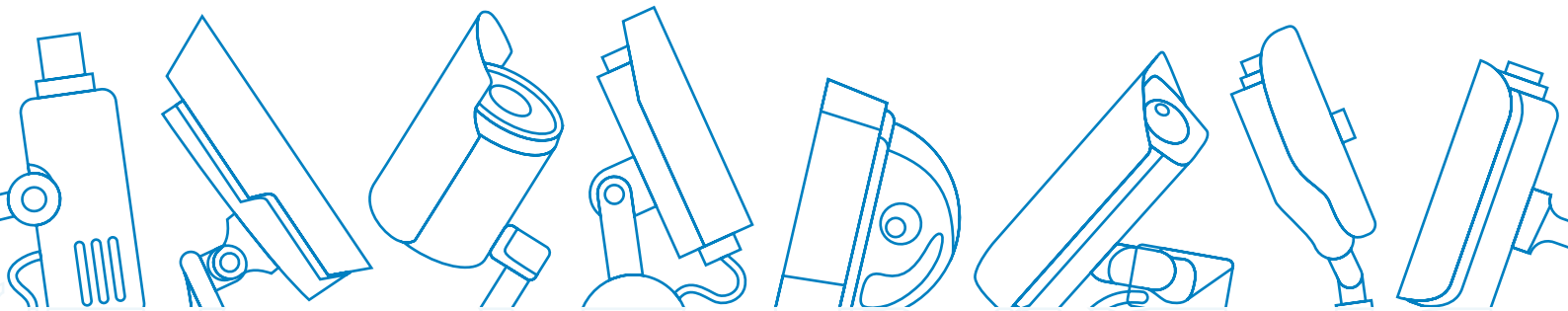
"All the end user needs to do is tell Alexa the command to view the front door camera and the live view will display. This integration is another example of LILIN enhancing the end user experience."

In addition, Device Hub provides a security professional the ability to remotely monitor multiple sites in one centralised dashboard via the LILIN Device Cloud with the up-to-date status of connected LILIN devices. The LILINHub App has a site mapping feature that plots multiple site locations within Google Maps.

The Alexa skill is available on all new LILIN Device Hub. SST



Our tribute to Safety & Security...



TradeCards Global mobile application is offering **50% discount** for one-year organisation listing to suppliers and service providers that serve our Safety & Security Community. With the reduced price of USD500 / *SGD700 for one-year organisation listing, suppliers and service providers get to enjoy an ***additional 10MB of product listing*** tagged to your organisation listing.

Visit **www.tradecardsglobal.com** to sign up for a new account and your organisation listing. Input "**SECURETRIBUTE**" as promo code before proceeding to payment page. The promo code is valid until 31 December 2019.

*Rate excludes 7% GST applicable for Singapore-registered companies

TRADECARDS GLOBAL

Supporting mobile version of:

SEAB · SOUTHEAST ASIA CONSTRUCTION · Security Solutions Today · bathroom +kitchen today · lighting today

GET IT ON Google Play

Download on the App Store

Will A Cheap Flying Car Be A Reality By 2022?

NFT Inc., a small, newly established startup has an ambitious plan: to build a competitively priced flying car. The innovative startup is developing a new brand for the flying car market: affordable door-to-door drive and fly autonomous commuter transportation solutions that operate in the airspace above cities.

The fully electric Vertical Takeoff and Landing (eVTOL) vehicle will enable people living within 100-150 miles outside a major city to easily commute to work in under one hour, door to door. The vehicle will be the size of a big SUV, with two versions - electric and hybrid – priced competitively against regular cars.

NFT hopes to test an initial prototype as early as 2019 and commence mass production in 2021-2022.

Incorporated in 2018, the company is founded by husband-and-wife team Guy and Maki Kaplinsky who are both serial entreprenuers. The co-founders' second start-up, IQP Corporation, was a pioneer in the Internet of Things sector and their application development platform was sold to GE Digital in 2017.

"The need for change is obvious, due to the increasing congestion in large cities and the ever-increasing traffic problems," Guy Kaplinsky told Ynet.

"Soon, we won't only drive and move around on the ground, we'll also use a flying car, which would enable us to land on roofs and in parking lots on the upper levels of buildings."

While big names like Hoover and Airbus are also working on manned electric-powered aerial vehicles, NFT's concept is different in that the dual-use vehicle can move both in the air and on the ground.

According to Research and Market, the market reach of manned aerial vehicles based on electric engines is expected to reach US$7 billion in 2028.

NFT is headquartered in California with an R&D center in Israel. Its senior engineers in Israel boast engineering experience from the Israeli Air Force and defense industry, academia and private industry. NFT Inc. employs 15 people in Israel and has a team of five working in Silicon Valley. SST

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

Southeast Asia Building

SINCE 1974

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

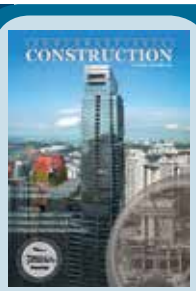
Bathroom + Kitchen Today

SINCE 2001

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Southeast Asia Construction



SINCE 1994

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Today

SINCE 2002

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Security Solutions Today

SINCE 1992

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

IMPORTANT

Please commence my subscription in _____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:
Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

PLATINUM PARTNER

Dahua Technology	Singapore	+65 6538 0952	sales.sg@dahuatech.com	www.dahuasecurity.com	IFC

GOLD PARTNERS

Robert Bosch	Singapore	+65 6258 5511	enquiry.apr@sg.bosch.com	www.boschsecurity.com	OBC
Microengine Technology	Malaysia	+603 7957 2008	enquiry@microengine.net	www.microengine.net	7
Delta Scientific	U.S.A.	+1 661 575 1100	info@DeltaScientific.com	deltascientific.com	3

SILVER PARTNER

Altronix	U.S.A.	+1 718 567 8181	info@altronix.com	www.altronix.com	5

See us at following upcoming events!

Event	Date	City	Country	Website	Page
IFSEC Southeast Asia 2019	19 – 21 Mar 2019	Kuala Lumpur	Malaysia	www.ifsec.events/kl	15
IoT Asia 2019	27 – 28 Mar 2019	Singapore	Singapore	www.internetofthingsasia.com	17
ISC West 2019	10 – 12 Apr 2019	Las Vegas	United States of America	www.iscwest.com	IBC
International ICT Expo 2019	13 – 16 Apr 2019	Hong Kong	China	event.hktdc.com/fair/ictexpo-en/HKTDC-International-ICT-Expo	1
Secutech 2019	8 – 10 May 2019	Taipei	Taiwan	www.secutech.com	9
IFSEC International 2019	18 – 20 Jun 2019	London	United Kingdom	www.ifsec.events/international	11
IFSEC Philippines 2019	13 – 15 Jun 2019	Manila	Philippines	www.ifsec.events/philippines	13
BMAM Expo Asia 2019	27 – 29 Jun 2019	Bangkok	Thailand	www.bmamexpoasia.com	19

SAVE THE DATE

ISC WEST
INTERNATIONAL SECURITY CONFERENCE & EXPOSITION

SPONSORED BY: SIA SECURITY INDUSTRY ASSOCIATION

APR 9-12 2019

SIA Education@ISC: April 9-11, 2019
Exhibit Hall: April 10-12, 2019
Sands Expo | Las Vegas
www.ISCWest.com

COMPREHENSIVE SECURITY FOR A SAFER, CONNECTED WORLD

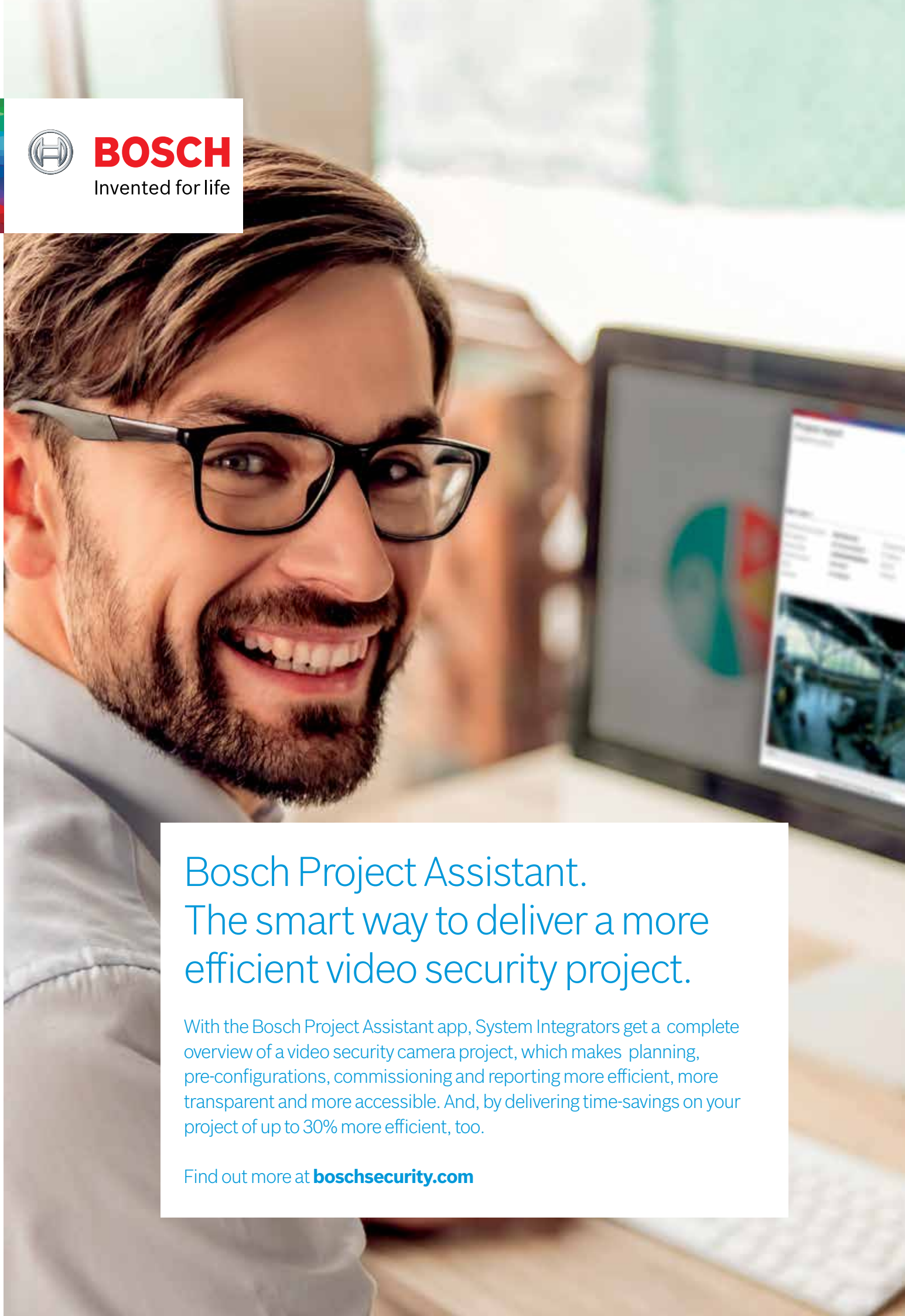
- Discover the industry's latest products, technologies & solutions
- Direct access to 1,000+ leading exhibitors & brands
- Network with 30,000+ Physical, IoT and IT Security Industry Professionals
- 85+ SIA Education@ISC Sessions

CONNECTED SECURITY EXPO @ ISC WEST FEATURING:

&

UNMANNED SECURITY EXPO @ ISC WEST

www.ISCWest.com/Register



BOSCH
Invented for life

Bosch Project Assistant. The smart way to deliver a more efficient video security project.

With the Bosch Project Assistant app, System Integrators get a complete overview of a video security camera project, which makes planning, pre-configurations, commissioning and reporting more efficient, more transparent and more accessible. And, by delivering time-savings on your project of up to 30% more efficient, too.

Find out more at **boschsecurity.com**