Security • Smart Building & Home • Mobility • IoT

a&S INTERNATIONAL

www.asmag.com Jun/Jul 2019 241

Malls and shopping centers present some unique challenges to parking management. Visitors enter and exit throughout the day, and in some cases, night.

Best Solutions to Manage Mall Parking Lots

Home Smart Locks: Trends and Challenges

Communication Solutions to Ensure Smooth Rail Operations

Hanwha Techwin Launches the New 99-mm (3.9-inch) Super-Compact Wisenet Q mini series

Why We Should Put More **Energy** Into **Power Plant** Security

Full channel SMD Plus enables more accurate alarm results

Dahua Smart Motion Detection Plus focus on vehicle and person

- Embedded AI chip with the deep learning algorithm providing 10 times computing power to upgrade full channel SMD Plus function with up to 95% accuracy
- Send alarm only when person and vehicle intrude and filter out false alarms caused by light & leaves, applicable to indoor & outdoor scenarios
- Person & Vehicle optional for playback to achieve quick target search, saving event retrieval time
- Actively warns off intruders with SMD Plus triggered flashlight and siren

Recommended Models

XVR7000-4KL-I Series
HDCVI 4K & H.265 AI XVR

XVR5000-I Series
HDCVI 1080P & H.265 AI XVR

HAC-ME1500/2241C
HDCVI Active Deterrence Camera

HAC-ME1500/1200D
HDCVI Active Deterrence Camera

ISO 9001:2000

www.dahuasecurity.com

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

VIDEOTEC

NTX

New IP68 stainless steel thermal camera with radiometric functions

Videotec presents NTX, the new IP68 stainless steel thermal camera, developed to provide an efficient and preventative surveillance system in the most critical environmental conditions.

The NTX thermal camera offers temperature detection based on the 4 central pixels of the image, and with the advanced version, the temperature of a specific object can be measured at any point in the image by means of defining a specific area.

As well as this, the radiometric functions offer the option to set a temperature limit, beyond which an alarm will be raised.

NTX is ideal for the most demanding applications in the marine and industrial sectors, in critical infrastructures, power plants and transport sector, including railways and motorway tunnels.

ONVIF S

IP66/IP67 IP68/IP69 | TYPE 4X TYPE 6P | PoE+ | IP

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy

CONTENTS

20

Special Feature

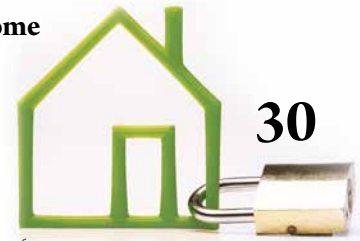
Best Solutions to Manage Mall Parking Lots

Malls and shopping centers present some unique challenges to parking management. Visitors enter and exit throughout the day, and in some cases, night.

Smart Building and Home

Home Smart Locks: Trends and Challenges

30



Smart locks for smart homes have gone from a means of simplifying entry to complex devices offering a multitude of features.

Website Articles https://www.asmag.com

How to keep video systems from being hacked

More and more, video surveillance systems are based on IP whereby video feeds are transmitted over the network.

How to select a camera system for construction sites

Across the globe, commercial and residential buildings are being constructed in cities and municipalities.

> **"Many customers are concerned about the initial investment for a solution. While high costs can deter many end-users, systems integrators and solutions providers should be able to convince customers of the long-term financial benefits that increased operational efficiency would bring."**
>
> **Arvind Mayar,** CEO, Secure Parking Solutions. Best Solutions to Manage Mall Parking Lots, p. 20

53

Market Update

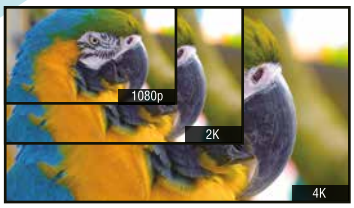
Italian Security Top 25: Still Growing, but Not Uniformly

The long-awaited "Italian Security Leaders, Top 25" is back, bearing the signature of secsolution magazine in collaboration with Plimsoll Publishing.

Techpoint

HD-TVI™ 5.0:
Universal 1-8 Mega Pixel Video
NOW WITH AUDIO over ONE CABLE!!

What GOOD is Video if you can't HEAR IT??



4K Video

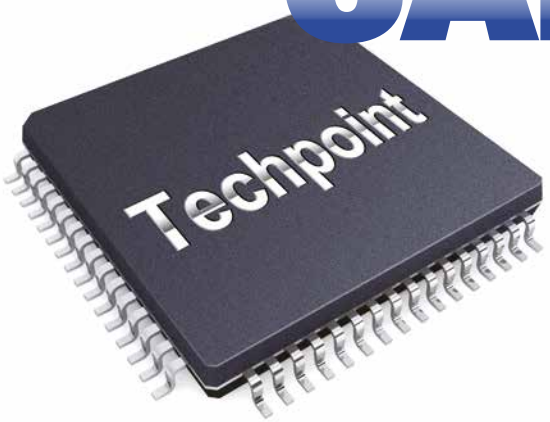
+


Audio

+


Control Signal

ALL OVER ONE CABLE!!!



HD-TVI™ 5.0

- Universal 1-8 MP support for ALL HD Analog Standards
- Audio over Coaxial and UTC cable support over 500 meters
- Universal Coaxial Protocol support
- Industry Leading Distance and Video Performance
- 80% HD analog DVR market share worldwide
- Currently shipping over 10 million channels per month

TP3813

- Support 720P/1080P video resolution
- Support Audio over Coaxial/UTP cable
- Integrated Universal Transmitter
- Integrated MCU and all essential ISP functions

TP3815

- Support 4-5MP video resolution
- Support Audio over Coaxial/UTP cable
- Support MIPI CSI Interface
- Integrated Universal Transmitter
- Integrated MCU and all essential ISP functions

TP3818

- Support 4K UHD video resolution
- Support Audio over Coaxial/UTP cable
- Support MIPI CSI Interface
- Integrated Universal Transmitter
- Integrated MCU and all essential ISP functions

TP2830

- Universal 1080P 4 Channel Receiver
- Universal 1-8 MP Analog Compatibility
- Support 4 channel Audio over Coaxial/UTP cable
- Support 2 x BT.656
- Pin to Pin compatible with TP2828/TP2826

TP2831

- Universal 4K UHD 4 Channel Receiver
- Universal 1-8 MP Analog Compatibility
- Support 4 channel Audio over Coaxial/UTP cable
- Support 4 x BT.656
- Pin to Pin compatible with TP2829/TP2827

Techpoint USA Contact:
Tel: 408-324-0588 / Fax: 408-324-0888
2550 N. First Street Suite #550
San Jose CA 95131 USA
sales@techpointinc.com / www.techpointinc.com

Techpoint Korea Contact:
Tel: 82-10-2718-6849

Techpoint China Contact:
Tel: 86-755-2361-9296

Techpoint Japan Contact:
Tel: 81-3-6205-8405

Techpoint Taiwan Contact:
Tel: 886-2-2657-6336

Techpoint

CONTENTS

Smart & Safe City

Why We Should Put More **Energy** Into **Power Plant Security**

Power plants are a crucial part of any nation's critical infrastructure.

Mobility

41 **Communication Solutions** to Ensure Smooth **Rail Operations**

As societies across the globe become more and more urbanized, the number of metro systems continues to grow.

Industrial IoT

60 How **Machine Vision** Powers **Manufacturing**

Machine vision in industrial environments works like an advanced version of the human eye, spotting defects and details on production lines or for logistics.

Products of the Month

48 **Cloud Video Surveillance is on the Rise**

6 Editor's Note
68 Show Review
72 Companies in This Issue
64 New Products
67 Show Calendar

Security and IoT for Business

36 Businesses are Using **Faces** to Gain **Security** and **Business Insights**

Stats & Figures

8 Manufacturing AI to See 24% Annual Growth
8 Intelligent Transportation Systems Market to Hit US$51.09 Billion by 2025
9 Global Edge Computing Market to Reach US$16.55 B Revenue at 32.8% CAGR by 2025
9 Smart Thermostat Market to Achieve 9% CAGR 2019–2025
9 Smart Factory Market to Hit US$244.82 B With 9% CAGR 2019–2024

a&S INTERNATIONAL

a&s International, published by Messe Frankfurt New Era Business Media Ltd., is a bimonthly professional publication that connects security and ICT suppliers and buyers in smart and safe city, building and home automation, mobility, and industrial IoT, in EMEA and the Americas.

ISSN 1997-6267 中華郵政北台字第 1571 號
執照登記為雜誌交寄

messe frankfurt

Messe Frankfurt New Era Business Media Ltd.
Taiwan Branch: 8F, No.288, Sec. 6, Civic Boulevard,
Xinyi District, Taipei City 11087, Taiwan
Phone/886 2 8729 1099
Fax/886 2 2747 6617
Website/www.newera.tw.messefrankfurt.com

Messe Frankfurt New Era Business Media Ltd., a company formed by Messe Frankfurt (HK) Ltd. and former *a&s* Group in 2009, is an integrated media service provider in the security industry. Our service covers magazines, websites, events, and trade shows. The portfolio of *a&s* magazines includes *a&s* International, *a&s* Asia (published in English), *a&s* China and *a&s* Taiwan (published in Chinese). *a&s* Adria, *a&s* India, *a&s* Japan, *a&s* Polska, *a&s* Russia and *a&s* Vietnam are licensed editions.
For changes of address or subscription problems, contact us at mfne-circulation@newera.messefrankfurt.com

Hubert Duh **Managing Director/Publisher**

Editorial
General Press
as-pr@newera.messefrankfurt.com
Jill Lai **Editor-in-Chief**
jill.lai@newera.messefrankfurt.com
William Pao **Senior Reporter**
william.pao@newera.messefrankfurt.com
John Liu **Reporter**
john.liu@newera.messefrankfurt.com

Art Design
Gaven Lee **Executive Designer**
Mao Chang **Senior Designer**

Marketing
Michelle Shih **Senior Media Marketing Coordinator**
michelle.shih@newera.messefrankfurt.com
Samantha Shen **Media Marketing Coordinator**
samantha.shen@newera.messefrankfurt.com

Corporate Management
Thomas Pin **Account Manager**
Chihung Lee **IT Manager**

asmag.com
Jessica Yang **Project Manager**
jessica.yang@newera.messefrankfurt.com

Audrey Fang **Media Operation Coordinator**
audrey.fang@newera.messefrankfurt.com

Secutech
Peggy Wu **Trade Fair Manager**
Veronica Chen **Group Manager**
Jason Cheng **Project Manager**
Michelle Chu **Project Manager**

International Advertising
[Headquarters]
Israel Gogol **Manager** israel.gogol@newera.messefrankfurt.com
Ting Lee **Assistant Sales Manager** Ting.lee@newera.messefrankfurt.com

[Branches & Representatives]
Carolina Pattuelli **Europe (Italy)** produzione@ethosmedia.it
Evris Consolos **Europe (U.K.)** evris@kemainternational.com
Adis Hodzic **Southeast Europe** marketing@asadria.com
Manish Gandhi **India** manish@abcindia.biz
Iris Lai **Taiwan** iris.lai@newera.messefrankfurt.com
Carol Guan **China** carol.guan@newera.messefrankfurt.com
Y. C. Suh **Korea** ycsuh517@naver.com
Takashi Komori **Japan** komori@asj-corp.jp
Nguyen Thu Ha **Vietnam** project1@vietfair.vn
Mariusz Kucharski **Poland** mariusz.kucharski@aspolska.pl

ThroughTek Co., Ltd.

Kalay IoT Platform

Turnkey Solution for Video Surveillance

Real Time Monitoring for Enhanced Security

3rd party AI applications and smart voice assistant integration

Seamless integration of security devices and sensors

IFSEC INTERNATIONAL 18-20 JUNE 2019 EXCEL LONDON UK

ThroughTek Booth

No. IF2433, Taiwan Pavilion

Schedule a meeting with us via marketing.en@tutk.com or visit our website at www.throughtek.com

EDITOR'S NOTE

Two Major Security Companies Get Funds from Private Equity Firms

At the beginning of the second quarter of 2019, two major security players, Panasonic and Pelco, announced alliances with private equity funds. Transom Capital Group acquired Pelco in its entirety as part of a continued effort to grow its digital business.

The Polaris Private Equity Fund acquired 80 percent of Panasonic's newly formed security business spin-off, Panasonic i-PRO Sensing Solutions Co Ltd. According to an announcement from Polaris Capital Group, the new company will focus on promoting its security solutions business and expanding R&D for machine vision for industrial and medical applications.

If we review the acquisition history in the video surveillance sector, companies that were industry leaders, such as Sony, Axis, Hanwha Techwin, Avigilon, VIVOTEK, Milestone, Mobotix, Tyco Security Products (now Johnson Controls), Nice Systems (now the Battery Ventures-owned Qognify), and Arecont Vision Costar, have all become individual companies under multiple international conglomerates. Bosch Security Systems and Honeywell Security are in the process of being fully integrated in their own building solution business sector. Interestingly, if you look at a&s Security 50 ranking, Chinese companies have all become more self-sufficient in recent years. Hikvision and Dahua are two particular examples. The pair have surpassed all of their competitors to become dominant in the industry. Several other Chinese companies also grew big via IPOs.

The decline of well-known brands and the rise of Chinese companies explains a lot about the ups and downs in the sector. But it does leave one wondering if the U.S.-China trade war and the U.S.'s recent bans on some Chinese brands will change the current industry landscape.

EDITOR-IN-CHIEF
JILL LAI
jill.lai@newera.messefrankfurt.com

EDITORIAL TEAM

SENIOR REPORTER
WILLIAM PAO

The Italy Top 25 security report has come out, showing year-on-year growth of 6.2 percent in the Italian market in 2018. This growth, however, affected less than half of the companies sampled. The report concludes that market consolidation in Italian security will continue, and that those focusing on innovation and wise management of resources will win out.

REPORTER
JOHN LIU

Adoption of smart technologies is growing across verticals. In homes, businesses, public infrastructure and more, internet of things (IoT) devices are used to help improve workflow, add convenience or generate insights. Various IoT applications are discussed in detail in this issue.

SOCIAL MEDIA **KEEP IN TOUCH WITH US!**

www.facebook.com/**asmagglobal**

twitter.com/**asmagglobal**

www.linkedin.com/company/**asmagglobal**

asmag.com Security & IoT

TRIPLE INTELLIGENCES

Tiandy 视界为世界
Vision For World

SMART CODEC
bandwidth control

256KBPS TO TRANSFER
2MP CAMERA
1GB STORAGE FOR 24 HOURS.

SMART ALARM
shape detection

ADVANCED MOTION
DETECTION RECOGNIZE
THE HUMAN AMONG
ALL THE MOVING OBJECTS

SMART IMAGE
face detection

ADVANCED ALGORITHM
MAKE SURE THE
CLEARITY OF THE FACE

Tiandy Technologies Co.,Ltd.
Email: sales@tiandy.com Tel: +86-22-58596065
Website: en.tiandy.com Fax: +86-22-58596048

STATS & FIGURES

a&s shares the latest industry research figures and analysis for industry players to gain a holistic view of the market.

Manufacturing AI to See 24% Annual Growth

Artificial intelligence (AI) is gaining traction in the manufacturing sector, which is on track to invest US$13.2 billion annually on AI software, hardware and services by 2025, registering a 24.3 percent compound annual growth rate (CAGR) from US$2.9 billion in 2018.

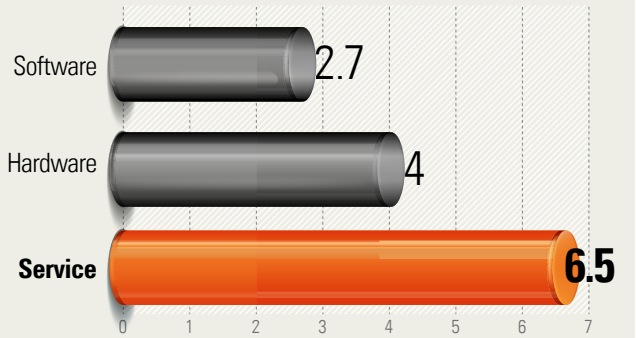
Of the $13.2 billion invested, AI services — which includes installation, training, customization, application integration, support and maintenance, etc. — will make up $6.5 billion, followed by hardware at $4.0 billion and software at $2.7 billion.

From a regional perspective, much of the revenue will be generated within the Asia Pacific region, largely due to the prevalence of manufacturing activities. Tractica predicts that by 2025, revenues in Asia Pacific will reach $4.9 billion, followed by North America at $3.9 billion and Europe at $3.0 billion.

The main drivers for investment in AI for manufacturing are the need for quality monitoring, yield improvement, predictive maintenance, energy management, and more. Tractica pointed out that the top use cases will be those that increase operational efficiencies and consequently cost reduction of production processes.

In the manufacturing sector, prediction machines run using statistical machine learning techniques and deep learning-enabled perception machines are set to be deployed. AI systems also draw from other technologies like computer and machine vision, natural language processing and various information classification techniques to harness the power of existing systems and combine the data output with machine learning or deep learning to generate insights that can be interpreted and shaped via automated algorithms, instead of requiring humans analyze a myriad data points. ■

Global AI Services Revenues by 2025 (US$ Billion)



Source: Tractica

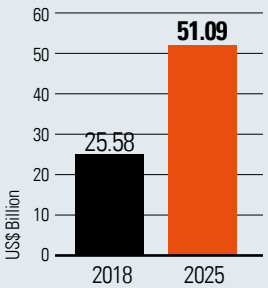
Intelligent Transportation Systems Market to Hit US$51.09 Billion by 2025

The global Intelligent Transportation System (ITS) market was valued at US$25.58 billion in 2018 and is projected to reach $51.09 billion by 2025, according to figures from Grand View Research. Advanced public transport systems are expected to witness the fastest CAGR of 12.1 percent between 2019 to 2025.

The use of ITS to reduce road accidents and to increase safety is a major driving force for the ITS market. Stringent regulations to improve driver safety in the developed markets of Europe and North America are expected to contribute to the ITS market growth. The Asia Pacific market is expected to grow at a significant CAGR of 13 percent during the forecast period, owing to increasing government initiatives and deployments of ITS.

ITS associations estimate that the use of systems such as advanced traffic management systems (ATMS) effectively reduce travel time by 25 percent and the waiting time at a signal by 20 percent to 30 percent. They also help curb emissions of greenhouse gasses. ■

Global ITS Market Value



Source: Grand View Research

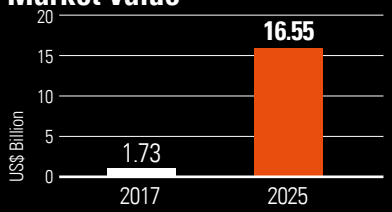
Global Edge Computing Market to Reach US$16.55 B Revenue at 32.8% CAGR by 2025

According to a report from Allied Market Research, the global edge computing market generated US$1.73 billion in 2017 and is expected to hit $16.55 billion by 2025, registering a CAGR of 32.8 percent during the forecast period from 2018 to 2025. The services segment is poised to grow at the highest CAGR of 35.6 percent during the forecast period, owing to a growing need to manage analytical data throughout its lifespan.

By application, the connected cars segment is projected to register the highest CAGR of 35.9 percent from 2018 to 2025, due to the increasing need to deliver real-time infotainment and other services in cars. However, the security and surveillance segment is expected to continue its stronghold over the industry and generate almost one-fifth of the global revenue by 2025, on account of enabling real time threat detection and reducing network latency.

Regionally, the Asia Pacific is projected to register the highest CAGR of 35.1 percent during the forecast period, due to the strong penetration of mobile devices, and cellular technologies in emerging economies such as China and India. However, North America was the largest market in 2017, capturing almost two-fifths of the market share and is expected to dominate the market through 2025. ■

Global Edge Computing Market Value



Source: :Allied Market Research

Smart Thermostat Market to Achieve 9% CAGR 2019–2025

The global smart thermostat market is predicted to increase from US$3 billion in 2018 to $6 billion by 2025, according to Global Market Insights.

The residential thermostat market value surpassed $1.5 billion in 2018 and is expected to achieve double digit CAGR from 2019 to 2025. Utility thermostat market revenue is poised to cross $500 million by 2025. Various programs which offer discounts or other incentives toward installation of devices will boost product demand. Distribution channel options could allow customers to make additional energy savings through participation in summer demand-response programs to ease pressure on power grids. In addition, increasing consumer awareness of enhanced monitoring solutions, coupled with rising penetration of smart home devices will augment industry growth. ■

Source: Global Market Insights

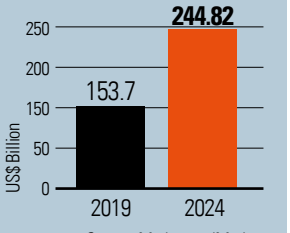
Smart Factory Market to Hit US$244.82 Billion With 9% CAGR 2019–2024

The smart factory market will reach at US$153.7 billion in 2019 and $244.82 billion, growing at a CAGR of 9.76 percent during 2019–2024, according to MarketsandMarkets. Discrete manufacturing is expected to hold a major share of the smart factory market, and MES is predicted to dominate the smart factory during the forecast period.

The growth drivers of the market include evolution of the internet of things (IoT), increasing use of enabling technologies in manufacturing, rising adoption of industrial robots in manufacturing sector driven by collaborative robots, and connected enterprise, along with mass production to cater to rising population. High capital investment and risk related to cyber and physical systems are major factors to inhibit the market growth.

Industrial robots are expected to account for the highest share of the global smart factory market. Implementing industrial robotics in smart manufacturing processes can improve productivity, reduce human errors, and increase production volume. ■

Smart Factory Market Value



Source: MarketsandMarkets

US$2 billion

The global smart smoke detector market is expected to reach more than $2 billion by 2024.

Source: Arizton

US$1.3 billion

Global home security camera market value will grow to $1.3 billion by 2023.

Source: Market Research Future

WEBSITE ARTICLES www.asmag.com

To view the most up-to-date and complete content for application cases, please visit the "Vertical Solutions" section of our website at www.asmag.com. The website collects recent security-related case studies and presents the best possible solutions for various vertical markets around the world. For more information, contact **as-pr@newera.messfrankfurt.com**

News Feature

SMART HOME | BANKING | INDUSTRIAL IoT | MANUFACTURING

SMART HOME

SnapAV and Control4 Merger to Transform the Smart Home Market

SnapAV has announced the acquisition of Control4 in an all-cash transaction for US$23.91 per share, representing an aggregate value of approximately $680 million. This highly complementary combination will leverage the increased resources of the two companies to provide integrators with a true one-stop shop. The new venture will offer a complete portfolio of products for smart-home customization, control and automation, in an effort to meet growing demand in the sector.

Control4's Board of Directors has unanimously approved and recommended that stockholders vote in favor of the transaction. Under the terms of the agreement, SnapAV will acquire all the outstanding common stock of Control4 for $23.91 per share in cash. The purchase price represents a premium of approximately 40 percent over Control4's closing price on May 8, 2019, the last trading day prior to execution of the agreement, and a premium of approximately 38 percent over Control4's 30-trading day weighted average share price ending on May 8, 2019. Private equity investment firm Hellman & Friedman -- SnapAV's majority shareholder since 2017 – will invest additional equity as part of the transaction and be the majority shareholder of the combined company. The acquisition is expected to close in second half of 2019

By merging, SnapAV and Control4 will combine the talent of their collective 1,200-plus employees, market-leading solutions, channel platform, dealer-first programs, global distribution and financial resources, enabling integrators to serve their customers better and grow their businesses.

"The combination of Control4 and SnapAV is transformative for the smart home industry," said Erik Ragatz, Partner at Hellman & Friedman and Chairman of the Board of Directors of SnapAV. He indicated that the increased resources of the combined company will enable it to invest more to drive innovation, and this combination will also allow them to give more effective support to integrators.

BANKING

Dime Community Bank Gets Impressive Video Access and Search Capabilities

Dime Community Bank serves the New York boroughs and surrounding metropolitan area with 29 retail banking branches and 24-hour ATMs.

Their previous video security system lacked sufficient onboard storage to satisfy the bank's archiving requirements, and enough cameras to provide optimal surveillance coverage. Besides, when the bank opened two new branches, Security Director David Panetta couldn't get the existing ATM transaction integration software to work.

To ensure all its branches are protected with the highest security standards, the bank deploys March Networks Hybrid NVRs and IP cameras, along with Command Enterprise video management software to secure its assets and keep employees and customers safe. Also, the bank turned to national systems integrator NAVCO to install new alarm and access control systems. To achieve its desired 100 days of archived video, the recorders are loaded with two 6-terabyte hard drives.

All 29 branches, as well as its head office and two other office facilities, are also protected by the intelligent video solution.

3.1 million smart home devices are set be shipped into multifamily dwelling units in the U.S. by 2024.

Source: IHS Markit

MANUFACTURING

e-shelter Security Uses Sony Cameras to Monitor High-Security Data Centers

Integrated security services provider e-shelter has installed over 2,000 smart Sony network cameras to monitor high-security buildings and critical infrastructure at data center locations in Europe. As well as offering necessary hardware and infrastructure redundancy, the centers should be protected against virtual and physical attackers. To prevent unauthorized access to servers and other infrastructure without creating unnecessary barriers, e-shelter security is making increasing use of intelligent, self-learning security systems.

All cameras are connected to e-shelter security's certified emergency call and service centers, allowing appropriate intervention to be initiated in the event of an incident. Other than ensuring the physical security of the data centers, the cameras also provide protection against cyberattacks on customers' assets. High levels of integral security prevent hackers from using the Sony cameras as an entry point into the customer's own network.

e-shelter security is also using Sony cameras in logistics centers, consulting/finance industry office buildings and smart building projects.

INDUSTRIAL IoT

Bosch Digitalizes Construction Sites

Bosch Asset Tracing Solution is an internet of things (IoT)-based connectivity solution that can be easily retrofitted to existing vehicles to locate and monitor vehicles on construction sites and farms. Bosch's solution comprises a sensor box, cloud-based evaluation software, and a wide array of digital services. The solution provides relevant data needed to enhance the efficiency and utilization rate of any vehicle fleet to help keep wait, search, and transportation times to a minimum. Data transmitted by the sensors helps improve processes, decision making, and machinery utilization. Customers and users can then access the sensor data, integrating it into their existing software systems for logistics, scheduling, and operations planning.

The solution utilizes LoRaWAN to enable energy-saving communication, supporting a range of several kilometers, but with lower bandwidths than Wi-Fi standard. The standard allows users to set up their own networks, in similar fashion to a Wi-Fi network at home.

In typical applications, the service life of a sensor is three to six years. That can be extended to ten years if the measurement and transmission intervals for sensor data are reduced. The sensor's clever software algorithms limit the capture of positional data to situations in which the sensor is moved.

SMART HOME

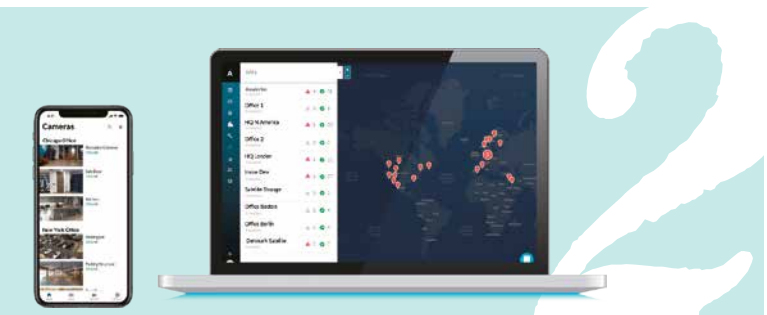
Resideo Acquires Buoy Labs, Adding Leak Prevention to Smart Home Portfolio

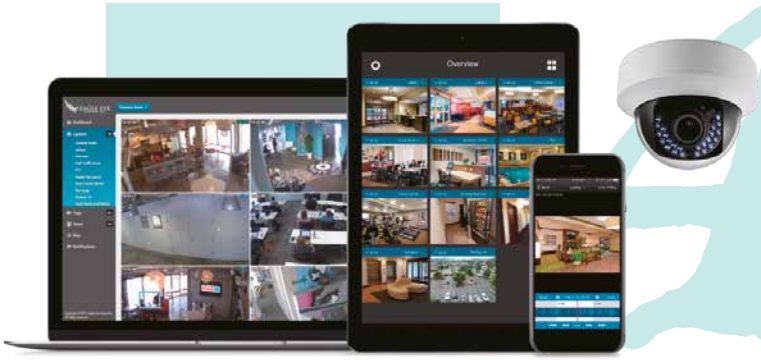
Resideo announced it has acquired California-based Buoy Labs, a firm that produces a Wi-Fi enabled solution that tracks the amount of water used in a home. The product integrates smart software and hardware that can identify potential leaks and intervenes to prevent them through its subscription-based app services. The company's Buoy product is professionally installed by a plumber to a home's main water line, either outside or inside the home, and can be powered by an outlet or battery. The app actively analyzes water use in the home, providing reports to the homeowner or their contractor of choice. Its software sends an alert to a potential leak and shuts off the water, automatically or via the app.

The Buoy product and app complements Resideo's Honeywell HomeTM Water Leak and Freeze Detector that can provide early warning of a leak or drop in temperature to help avoid expensive repairs or losses within a home.

Cloud Video Surveillance is on the Rise

Cloud video surveillance is no longer just a buzzword, with related solutions growing more popular — especially in the commercial space. Cloud surveillance eliminates the headaches of traditional systems as there is no software to buy and install, no need to acquire license keys and no need to maintain operating systems.





(1) 3dEYE Cloud Video Surveillance

3dEYE

3dEYE is easy to setup and works with all types of cameras and hardware. It can be integrated into existing security systems or can be set up from scratch to make a new security solution. Users can export clips on demand when viewing live or archived video for future access. These clips are saved in the cloud and the video footage can be exported to a computer or laptop for sharing. Users can also create customized camera layouts and zoom in on points of interest.

URL: www.3deye.me

(2) Arcules Cloud Video Surveillance as a Service

Arcules

Arcules Integrated Video Surveillance delivers centralized security for loss prevention. It also includes a predictive analytics engine that can help retail managers improve merchandising, optimize staffing and roll out promotions to increase sales. As a unified, integrated cloud solution, the Arcules Platform works with a myriad of camera brands and does not require costly servers. Video data is stored locally and in the cloud for both easy access and an extra layer of security and data protection. Owners and managers can view multiple departments and geographic store locations on any web or mobile device.

URL: arcules.com

(3) Camcloud Cloud Video Surveillance

Camcloud

This cloud video surveillance solution for businesses is designed for clients who don't want the hassle of complicated and expensive systems. With no need for hardware or advanced security knowledge, clients can get started quickly. Whether it is for one or many locations, Camcloud lets clients connect all the cameras to its cloud-based solution, delivering 24/7 on-demand surveillance. With Camcloud's cloud video surveillance solution, everything can be managed remotely. Also, Camcloud does not depend on any local hardware "boxes" to connect cameras to the cloud. In fact, Camcloud's hardware-free approach delivers low total cost of ownership.

URL: www.camcloud.com

(4) Eagle Eye Cloud Video Surveillance

Eagle Eye Networks

The Eagle Eye Cloud VMS is a cloud security camera system which provides complete cloud management, mobile and web browser viewing as well as cloud recording per client request. This cloud video system has been designed from the ground up to be all cloud all the time. Users may click and add an analog or IP camera any time, and also click and change how long to keep the recordings. In addition, users only pay for what they need.

URL: www.een.com

(5) Genetec Stratocast

Genetec

Stratocast is a service that records video in the cloud, eliminating the need for on-premises servers. With no servers or software to install, organizations can deploy their video surveillance system quickly, without the requirement for any IT involvement for ongoing maintenance or updates. Organizations can leverage Stratocast camera connections to easily set up cameras across multiple distributed locations and monitor video from a central site. Videos can be correlated with other system events, including alarms, access control and intrusion events, in Security Center.

URL: www.genetec.com

(6) Ivideon Security and Remote Surveillance

Ivideon

Ivideon can quickly equip any number of locations with video surveillance, connecting them all to a system that offers access from anywhere in the world. Whether it is for setting up a few cameras in a small store or several thousand in a major retail chain, Ivideon's solution is up to the task. There are mobile, desktop and web applications available for easy access to cameras and data on Windows, Mac OS X, Linux, iOS and Android. It works across most connection types to avoid a complex setup.

URL: www.ivideon.com

(7) OpenEye Web Services

OpenEye

OpenEye Web Services deters theft, reduces internal fraud and generates business intelligence for retail stores. The cloud-managed video platform aims to get a better return on oss prevention efforts and improve customer satisfaction while reducing the burden on IT and operations. Retail stores can investigate returns fraud, coupon manipulation, voids and under-ringing at the point of sale. In addition, the solution helps to identify fraud at all levels of the operation, from cashiers to general managers and customers.

URL: www.openeye.net

(8) Tyco by Johnson Controls Smartvue Cloud Services

Tyco

Smartvue offers private cloud options with cyber and data security plus Johnson Controls cyber and GDPR protocols. It is available in 140 countries and backed by employees in 2,000 locations worldwide. Users can connect existing cameras using a secure cloud gateway or select from over 30 cloud camera options from 1 megapixel to 12 megapixel, plug them into the network and instantly access the secure and full featured Smartvue Cloud VMS. Select from over 30 plug-and-play professional cloud cameras or securely transform existing camera systems without replacement using cost-effective Cloud VMS gateways.

URL: smartvue.live

Why We Should Put More **Energy** Into **Power Plant Security**

Power plants are a crucial part of any nation's critical infrastructure.

An attack on a power plant could not only have severe economic consequences, but catastrophic environmental and safety ones as well. And even though power plants are safer and more secure today than they ever have been, hacking has also become more sophisticated, reminding us that we must always be on high alert.

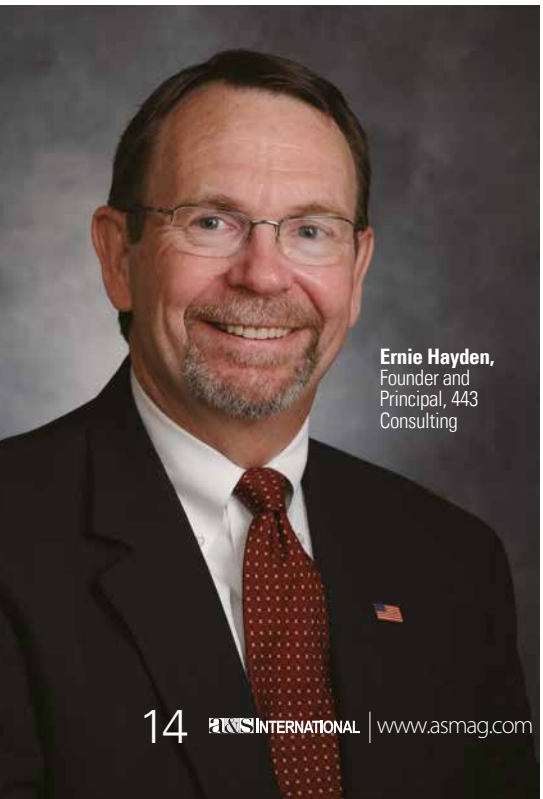
Earlier this year a series of cyberattacks on Venezuelan power grids kept the lights off for a full week in some parts of the country. Last summer Russian hackers gained access to the control rooms of several utilities in the U.S.; Russian hackers were also responsible for knocking out Ukrainian power grids in 2015 and 2016. Then there is always the looming risk of physical attacks against power plants and grids by terrorist.

In order to ensure attacks like these never happen again, it is imperative that power plants take the necessary steps to secure the safety and security of their premises, surroundings and personnel.

● **BY** Eifeh Strom, Freelancer

Power Plants Are Still at Risk and Better Security Can Help

Although less vulnerable than before, power plants remain at risk of physical security attacks, as well as other unforeseen dangers.



Ernie Hayden, Founder and Principal, 443 Consulting

Power plants are attractive targets for those looking to create chaos and disrupt national power grids. Adding a robust physical security system has made these facilities less vulnerable, but they still remain at risk.

To truly ensure an effective power plant security program has been implemented, Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI) suggest adhering to the principles of deter, detect, delay, respond and mitigate.

SMI recommends power companies utilize the CARVER Target Analysis and Vulnerability Assessment Methodology to determine the probability of attack against each critical asset within the system. SMI explained CARVER was originally created by the CIA in the 1970s as a predictive tool to identify where terrorists may strike next. It was revived after the 9/11 terrorist attacks, this time by the private security sector. "Only until you have conducted an assessment can you truly set a baseline for how secure your facility is. CARVER does this for you," they added.

One growing concern at the forefront of the threat landscape relates to the detection and deterrence of drones, or unmanned aerial systems (UAS), according to Darin Dillion, Energy Principal at Convergint Technologies.

In July 2018, the environmental group Greenpeace crashed a Superman-shaped drone into the side of a nuclear

power plant near Lyon, France. The stunt, which caused no damage, was meant to show how vulnerable these facilities are to drone attacks. Currently, technologies related to the detection of UAS are still evolving, as are the written policies and counter measures for UAS deterrence.

Ernie Hayden, Founder and Principal of 443 Consulting also pointed to the threat against Safety Instrumented Systems (SIS), the system that would shut systems down if all personnel were unable to respond to plant calamities. In 2017 the Triton malware (also known as Trisis or HatMan) attack targeted a Saudi petrochemical plant. Hayden explained that this attack disables the SIS of a plant. "By taking the SIS away, this results in the plant operating without automated shutdown capabilities — which could be very dangerous to the plant and to the general population," he said. The malware was discovered again earlier this year.

The precise ways to prevent such modifications to SIS, and therefore prevent future attacks, are still vague. Hayden recommends physical barriers to prevent casual access to the SIS, as well as placing the SIS under "lock and key" and/or posting guards in order to ensure more positive control. Training on-site staff, including vendors and contractors, to ensure they are aware of the threat and aware of the necessity to be more diligent about the threat should also be considered.

▲Critical infrastructure sites now need measures for the detection and deterrence of drones, or unmanned aerial systems (UAS).

Michael Rothschild, Senior Director of Product Marketing at Indegy highlighted how utilities are modernizing power plants and grids to enhance reliability, lower costs and ensure regulatory compliance. "Operational technology (OT) networks are increasingly connected to their IT networks, which together with increased automation increases their attack surface for vulnerability to cyberattacks. Securing automated SCADA generation, transmission and distribution networks from cyberthreats is paramount for improving grid performance and resiliency," he said.

While as a whole countries around the world have continued to step up power plant security, there is still a lot of disagreement as to who is responsible for the overall security of power plants, according to Rothschild.

"Power plants point to the government, yet not all power plants are government run or owned. As a result, the government points back to the plant operators," Rothschild explained. "Due to the interconnected nature of the grid system, its resilience to cyberthreats will only be as strong as its weakest link."

As a result, power, along with other industries considered part of the critical infrastructure sphere, must band together in order to address security vulnerabilities in the system before they are exploited.

Strict Regulations Aim to Keep Power Plants Safe and Secure

Although power plant regulations differ by type and region, they all have the same aim: to ensure the safety and security of the facility.

Power plants are highly regulated due to their importance and vulnerability. Regulations exist for everything, ranging from worker safety to cybersecurity, and can vary depending on the type of power plant.

Nuclear power plants, for example, have higher standards than others since the consequences for any breach, attack or failure is much greater. In the U.S., the Nuclear Regulatory Committee (NRC) is in charge of creating regulations and requirements for nuclear plants in order to make sure they are secure. SMI noted that after 9/11, the

Luke Bencie, Director, Security Management International (SMI).

NRC included more measures for airborne terrorist attacks and actions to reduce radiological release. In terms of cybersecurity, the NRC requires every nuclear plant submit a cybersecurity plan and implementation schedule against threats that could face the plant.

The NRC is also required to conduct "force-on-force" exercises with nuclear power plants every three years, as per the Energy Policy Act of 2005. SMI explained that these security exercises involve having someone attempt to access critical areas of the plants and inflict as much damage as possible. Additionally, the NRC requires that each nuclear plant have an emergency planning zone (EPZ) within roughly a 10-mile radius, and have emergency response exercises every two years. This is then is reviewed by the NRC and FEMA (Federal Emergency Management Agency). Plants must also have plans in place within a 50-mile radius to prevent ingestion of radioactive material.

The primary security standard for those generating electricity in North America is NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection). This series of standards lay out best practices for both cyber and physical security. Even though this is a North American standard, other countries have adopted similar best practices.

In the EU, the Directive on Security of Network and Information Systems (NIS Directive), the first EU-wide cybersecurity legislation, took effect in August 2016. Michael Rothschild, Senior Director of Product Marketing at Indegy explained that the directive establishes minimum security standards for operators of essential services such as the electrical grid. Though it chiefly applies to the EU, anyone dealing with the EU must also comply.

For those power plants not obligated to comply with national standards such as NERC CIP, Ernie Hayden, Founder and Principal of 443 Consulting noted that they are encouraged to follow the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework; this, however, is entirely voluntary. Some power plants may also be encouraged or even directed to follow other security standards such as the International Society for Automation (ISA) standards 62443 for industrial control and automation systems.

When it comes to worker safety, the Occupational Safety and Health Administration (OSHA) in the U.S. has requirements for power plants regarding their health and safety. For example, OSHA requires detector pumps for potential air contaminants that may arise in different types of power plants. OSHA also encourages companies to build on existing safety regulations and create additional company-specific policies, said Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI).

Unfortunately, a lack of rule implementation can led to fatal incidents, such as the one in Tampa, Florida, in June 2017. SMI explained that Tampa Electric disregarded rules during a maintenance job, resulting in the death of five workers. The company was handed a "willful violation" from OSHA, the most significant violation, along with a fine of over US$100,000.

"Companies should be doing frequent hazard training with employees to ensure they are following the correct safety measures," SMI advised.

It is also important to note that security standards are always evolving due to continued presence of new security threats. As such, existing standards and regulations should be a considered a minimum baseline. Instead, organizations should aim higher and work to stay ahead of future threats.

Deploying the Best Security Solution for Power Plant Protection

Securing power plant facilities requires a comprehensive security solution, including video surveillance, access control and cybersecurity.

Vulnerabilities in power plant security can lead to catastrophic consequences. Deploying the latest security solutions is one way power plants are securing their facilities.

Matthew LaRue, Senior Account Executive, at Convergint Technologies noted that there is a "disruptive digital revolution and digital transformation at hand," resulting from the many software-centric solutions that improve processes, reduce risk, derive savings and enhance overall workflow.

"Many power plants are now seriously considering the various threats to facilities and the available solutions to mitigate threats," LaRue said. Some of the solutions power plants are exploring and implementing include artificial intelligence (AI), advanced analytics, biometrics, data mining and identity access management. These solutions can decipher "real risks" and provide the opportunity for a much more proactive

Matthew LaRue, Senior Account Executive, Convergint Technologies

response, he added.

In terms of more traditional security technologies like video surveillance and access control, there are many ways the latest technologies are assisting with plant security. Ernie Hayden, Founder and Principal of 443 Consulting, noted that improvements in camera technology and deployment capabilities have made it easier to deploy cameras to important areas requiring increased security. Cameras that leverage advanced video analytics and AI are helping plant operators identify threats such as suspicious bags, placement of unusual objects, etc.

Luke Bencie, Director, and Paige Morrison, Junior Associate, at Security Management International (SMI) explained that power plants are also using video surveillance cameras in conjunction with radar. This is because some plants are located near water (as it is used as a coolant), fog and other weather can make surveillance challenging. Since radar senses motion from further away than traditional video surveillance cameras, it is useful in more challenging environments. SMI emphasized that these technologies are to be used in addition to existing video surveillance solutions, not as a replacement for other security measures.

Access control technology is being used by power plants to protect against unwelcome and unauthorized visitors, as well as to monitor who is on the premises at all times. Critical areas of the plant, including the control room, safety systems and others, require card or biometric access, and are sometimes manned by guards.

Darin Dillion, Energy Principal at Convergint Technologies, pointed out that certain technologies installed at utility power plants are used daily to ensure that strict procedures are being followed and compliance is being met. An example might be the use of access control and identity management tools used to track employees, contractors and visitors that enter and exit power plants.

"Access control databases and video files are frequently used to adhere to North American Electric Reliability Corporation (NERC) compliance. Those events and the reporting tools that are output from the respective databases are used for investigations, compliance reporting and for audit purposes," Dillion said.

In addition to secure access management systems, Hayden said some power plants were deploying extra measures like security entrance kiosks to check portable media drives for malware before they are brought inside the power block.

Olea, a manufacturer of security kiosks, offers a portable media cybersecurity kiosk to aid in safeguarding a power plant's networks and incident command systems (ICS) from malware threats due to removable media (e.g., USB drives) brought in by contractors, vendors, employees, etc. The kiosk can scan USB drives and other portable media using up-to-date antivirus systems. "For instance, the kiosk can be placed at the entrance to a production floor, factory building, etc., to specifically ensure that the USB drives are 'clean' before crossing the plant threshold," Hayden explained.

Apart from physical access, power plants must also closely monitor its network access. Michael Rothschild, Senior Director of Product Marketing at Indegy pointed out that there is a large and heterogeneous population of users that have access to the network with credentials and elevated privileges, including employees, subcontractors, partners, suppliers, maintenance workers and perhaps even customers.

"In fact, one of the biggest threats to the security of the network and SCADA operations are these insiders," Rothschild warned. "As such, it is important to give authorized personnel proper training so they know how to minimize risk and appropriate access for their role; no more and no less."

Power Plants Are More Connected, Creating New Cyberthreats

The internet of things (IoT) has been both a blessing and a curse for power plants, as being connected has opened them up to more threats.

The internet of things (IoT) has been a double-edged sword for power plants. On one hand it has offered convenience and more advanced security, but it has also opened the door to threats and attacks that were once not a concern.

Until fairly recently, power plants and SCADA systems were isolated from the rest of the world, said Michael Rothschild, Senior Director of Product Marketing at Indegy. They were not connected to the internet or other systems, making the threat of security incidents very unlikely. Furthermore, the computers used to run industrial processes generally operate for years without any updates or changes.

"The development known as the industrial internet of things (IIoT), has eliminated this buffer zone or 'air gap,'" Rothschild explained. "By connecting once isolated industrial devices to business networks, IIoT has introduced new security risks that could be right out of a science fiction novel. But they're not."

Many rogue factions had specifically targeted critical infrastructure because it is relatively easy and can cause massive amounts of damage, Rothschild said. "We have not seen many catastrophic failures, but there are numerous incidents where proof of concept of attacks have been carried out, e.g., the Ukrainian power outage of 2015, [and] the Rye Brook Dam attack of 2016.

"There are many other incidents where adversaries have gained access to their enemy's critical infrastructure to create a foothold or what we call 'red button functionality' so they can launch an attack at the time of their choosing."

IoT devices such as internet-connected cameras have also been targeted. Many users do not change the default username and password, which makes searching and hacking video feeds quite easy. There are even a number of websites that note devices connected to the internet in important facilities and show their location. The lack of urgency in changing something as simple as a camera password, leaves the entire surveillance system vulnerable.

IoT is also being used to expand sensor arrays such as pressure, temperature and level across power plants, according to Ernie Hayden, Founder and Principal of 443 Consulting. While this may be great for detailed engineering analysis, IoT devices add more traffic to the wireless network and provide more opportunities for attackers to inject malware into the systems. He added that because IoT devices are becoming more prevalent and important to the operation of the plant, they can also be the medium for a denial-of-service (DoS) attack on the plant by shutting down or overwhelming the wireless system.

"Don't forget the Mirai attack of a year ago where an attacker took advantage of flaws in many IoT devices and essentially shutdown a DNS service provider. This event showed that IoT devices need to be tested for security flaws before they are sold/deployed," Hayden reminded.

While IoT has created vulnerabilities, it has also created many opportunities. Matthew LaRue, Senior Account Executive at Convergint Technologies, noted how IoT has also allowed for more efficient energy use — using IoT smart devices has allowed consumers and companies to have improved understanding of energy usage.

Michael Rothschild, Senior Director, Product Marketing, Indegy

When it comes to protecting operational technology (OT) systems from digital security threats, Rothschild explained that it requires the same approach used to protect IT infrastructure. While the tools need to be designed for an OT environment, many of the concepts are the same. This includes: maintaining an up-to-date inventory of assets; patching systems when vulnerabilities are discovered; applying a strong access control standard; deploying a strong, multi-disciplinary threat control system consisting of both signature and anomaly detection; and performing regular device checks on OT assets to ensure they are running as expected and have not been compromised. A&S

Hanwha Techwin Launches the New 99-mm (3.9-inch) Super-Compact Wisenet Q mini series

Video surveillance cameras are essential for effective security in retail stores, helping to prevent product theft and ensure the safety of employees and customers.

Submitted by Hanwha Techwin

Nowadays, the demand for such cameras among retailers has been growing sharply, as they help store owners operate their stores more efficiently and increase sales through integration with business intelligence solutions.

Hanwha Techwin, a leading global security company, recently grabbed the industry's attention through the release of its new Wisenet Q mini series. This recently launched line-up is super compact at 99 millimeter (3.9 inches), about 40 percent smaller than its predecessor. Thanks to its size, Wisenet Q mini series perfectly blends into any interior while facilitating an effortless installation anywhere, even on a ceiling or a wall inside and outside of retail stores.

The Wisenet Q mini series comprises four dome cameras (QND-6011/QND-6021/QND-8011/QND-8021) supporting 2–5 megapixel resolution. As an expansion of the Wisenet Q series, this newly launched line-up adopts all the advantages of the previous Wisenet Q series while supporting essential video security functions at a reasonable price. Hanwha Techwin also plans to launch various types of Q mini series, including flat-eye and fish-eye cameras, within this year to expand customer satisfaction.

This line-up features two lenses (2.8 millimeter and 4 millimeter), which allow users to select and use one according to their desired direction and angle. The "Hallway View" enables vertically or horizontally oriented monitoring in long and narrow spaces of some stores, such as corridors and aisles. It also supports HDMI output (QND-8011/QND-8021) to help users connect directly to a monitor or TV for public view, while the "Open platform" has strengthened connectivity with third-party companies.

Furthermore, the cameras are closely integrated with "Retail Insight," Hanwha Techwin's exclusive retail solution for smarter selling, another key feature of these cameras. By integrating with "Retail Insight," the cameras identify store congestion in advance and provide effective personnel management by analyzing the average number of customers and accumulated time spent in a specific area. Not only that, they analyze different types of store information (e.g. data from franchises) all at once, and produce useful reports for store management. Thus, it serves as a one-stop solution for operating stores more efficiently and contributing to sales growth.

A source at Hanwha Techwin said: "We expect a positive market response as the new cameras have improved ease of installation thanks to their compact design, while they encourage sales growth by providing analytical functions that enable intelligent store operations and management." He added, "We also plan to bolster customer satisfaction in the market by continuously launching various Q mini series." ■

About Hanwha Techwin

Hanwha Techwin is a subsidiary of Hanwha Corporation, a Korea-based company. Hanwha Techwin offers total security solutions that encompass network and analog cameras, recording solutions, video management software and compression technology. Hanwha Techwin has solidified its leading position in the security solutions market by building self-developed SoC chipsets along with the optical, manufacturing and image-processing technology accumulated over 30 years. Now, Hanwha Techwin is preparing for the future by continuing to invest in artificial intelligence (AI) and cybersecurity, in order to provide convenient and safe security solutions to customers. With the representative brand Wisenet, Hanwha Techwin will strive to provide security solutions that our customers can trust. For more information about Hanwha Techwin, please visit our website www.hanwha-security.com

About 79 million cars were sold across the globe in 2018 and this year sales are expected to remain steady, according to Statista. As these cars take to the roads, there is an increasing need for parking lots that are managed with advanced technologies.

Best Solutions to Manage Mall Parking Lots

• **BY** Prasanth Aby Thomas, Consultant Editor

Malls and shopping centers present some unique challenges to parking management. The most significant among them is that there is always some kind of movement in the parking lot. Visitors enter and exit throughout the day, and in some cases, night. There is also the need to provide convenient payment systems that are easy to user.

Technological advancements and user behavior have prompted the emergence of certain trends in this industry, according to the International Parking and Mobility Institute (IPMI), an association of professionals in parking, transportation, and mobility. Key among them are the

use of mobile technology, increased use of guidance systems, and better access control and payment options.

Then there are also concerns on changes in the automotive industry. As electric cars become popular, mall owners may create special spaces for them. Looking ahead, there are bound to be more autonomous cars and that would present a whole new challenge altogether.

The following is a look at the major requirements of parking management in the mall and shopping center vertical, potential criteria for selecting solutions, and some major solutions worth considering.

What Are the Major Security Concerns in Mall Parking Lots?

Being a place where crowds gather, malls are vulnerable to several kinds of attack. But in parking lots there are other concerns too.

The number of malls across the globe is increasing. So are the number of private vehicles that people use to get to these malls. The situation inevitably calls for improved parking lot management solutions that can take care of safety concerns as well as make processes more efficient. From a systems integrator's (SI) perspective, understanding the evolving threats in mall parking lots is integral to offering solutions that would ensure maximum protection. Speaking to a&s recently, Arvind Mayar, CEO of Secure Parking Solutions listed some of the major concerns that SIs should be aware of.

1. Bomb threats

Malls are places where a huge number of people gather every day. This makes them a target for terrorist attacks. In December last year, two people were killed and about 30 wounded when a bomb exploded at a mall in the Philippines. Similar incidents have taken place in other places too. While they may not always have occurred in the parking areas, car bombs are a serious threat that parking lot management systems should be concerned about.

2. Vehicle theft

Theft of cars or things kept in cars parked at shopping centers is also a cause of concern. Incidents such as the burglary at the Stanford Shopping Center in Palo Alto last year continue to show that parking lots are far from safe at present.

3. Accidents

Accidents are a risk wherever vehicles are being driven. In the closed spaces of parking lots, where there is limited room to maneuver cars, this risk is higher than in several other places. According to the insurance firm ThinkInsure, one in five accidents happen in parking lots. While most parking lot accidents are minor and involve low-speed impact, they can still result in serious damage and injury.

4. Fire

According to Mayar, the possibility of vehicles catching fire is a major issue that needs to be addressed when providing solutions for parking lots. Some experts point out that car manufacturers increasingly use more plastic in vehicles now than before, leading to fire-related incidents becoming a major concern.

5. Vandalism and related issues

Damage to cars by vandals is also a concern. This becomes all the more common in malls that have nightclubs or bars and inebriated people acting irresponsibly, according to Mayar. Vandalism may not always be an isolated incident and could happen as part of a theft.

According to Twin City Security, a firm that offers security services, malls are the new main streets of the U.S. This means the wide range of security concerns that could have been expected on the main street can now be expected in a mall. In the specific context of parking lots, we could say that any concern that's relevant to a car parked in the streets could also be applicable to malls.

The only difference here is the efficiency of a parking lot management solution. An ideal solution should be able to integrate with different security systems like surveillance cameras, access control systems, and fire solutions, to act in accordance with a given situation.

Naturally, security is just one benefit of a parking management solution. Operational efficiency, economic and environmental advantages would also benefit mall managers as well as their customers.

Drivers will be able to know the number of vacant parking spots available before entering the area. Some solutions even offer mobile solutions that can inform the drivers of the status through short message services. This reduces the amount of time, energy, or manpower that would otherwise be spent searching for a spot considerably. In turn, it also reduces pollution.

Major Challenges in Managing Parking Lots

Several parking management challenges can be dealt with by employing some of the latest technologies on the market.

With rapid urbanization and increased population density in cities, there is a heightened need for mobility solutions. Private vehicles are a preferred mode of transportation for many people in developed economies. As the standard of living continues to go up in several parts of the world, more and more people and companies buy new cars.

For cities, this has brought with it the challenge of creating parking spaces. The concept of the parking lot has evolved quite a bit over the years from just a place where people could leave their cars to places that are managed by automated solutions to ensure security and operational efficiency.

The number of malls and other commercial centers is also increasing in cities, attracting more and more people who prefer to drive in with their cars. This has increased the need for efficient parking lot management systems in malls, not just to make sure people have a hassle-free experience but also to avoid wasting money and resources.

Nevertheless, there are several challenges that mall management and solution providers face when it comes to managing parking lots. Some of these challenges are the reason automated systems have come into place. Others persist despite the introduction of such systems.

Manual Ticketing is Time Consuming

Before venturing into the realm of automated parking lot systems, let's take a look at why electronic solutions should be used. Manual ticketing systems take up time and require more manpower, resulting in higher costs and slower processing.

While this may be seen as an obvious issue to many, the fact is that there are still several malls and commercial entities across the globe that are yet to make the shift from manual ticketing systems.

Paper-based ticketing systems also make the job of information management difficult. In case of any untoward incidents, the management should be able to provide information about any vehicle parked in their space immediately. Automated electronic systems make this possible.

Access Control and Ticketing System Failure

One of the worst nightmares for a parking lot manager is the malfunctioning of any access control system. Since malls are often open for long hours and mostly every day of the week, parking lots will be in use most of the time. Should an entry management system fail in any way, there could be delays that leave customers upset.

> "There is a need for high-quality video surveillance that can provide clear images of the condition of a vehicle at the point of entry."

False Damage Claims

According to Arvind Mayar, CEO of Secure Parking Solutions, there are always some customers who try to claim that their car was damaged while in the parking lot, when in reality the car was already damaged before entering the lot.

To deal with such an issue, there is a need for high-quality video surveillance that can provide clear images of the condition of a vehicle at the point of entry. Adequate lighting is also required to support the surveillance systems that are being installed.

Integration

Installing new parking solutions at existing malls and shopping centers is a challenge. But perhaps what's even more difficult is the integration of these solutions into third-party systems. For instance, surveillance and fire may be managed by a different vendor. Unless all the companies involved are willing to support integration, operations could be tough.

Open standards for traffic data exchange like DATEX II become relevant in this context. Fortunately, major companies do support such standards. For instance, Siemens' intelligent parking solution offers links to third-party applications via open standards such as DATEX II. This interface can allow for the integration of data produced by a system for payment providers, enforcement and in-vehicle platforms that consume data in order to provide services that add value to the infrastructure in place.

Six Major Requirements of Parking Lot Solutions Customers

Security and convenience are key for parking lot management. But providing them is not as simple as it sounds.

Arvind Mayar, CEO, Secure Parking Solutions

Mall and shopping centers require parking lots that offer convenience and safety to their customers. But this is just the tip of the iceberg when considering customer requirements. When providing such a solution, systems integrators (SI) should know the specific demands of end-users in order to provide a hassle-free solution.

1. Ease of finding parking space

People arriving at malls should be able to know the number and location of vacant parking spots even before entering the premises. There are several ways in which solution providers deal with this. Sensors placed at parking spaces inform the system on the status of the space. Signage boards placed outside of parking lots can display the information gathered from these sensors.

Alternatively, some systems may also provide mobile-based services so drivers can send a message to the system to get an update on vacant spots. There are also app-based solutions that can inform drivers about where they can park their vehicles.

2. Security

Surveillance systems are necessary to ensure the security of cars parked. Apart from providing evidence for forensic purposes, applications like a license plate recognition (LPR) system can help to identify cars that warrant special service, like those of VIP customers.

Analytical solutions may also come in handy in detecting intruders and providing instant alerts to security personnel. Several major global security vendors have dedicated parking lot management solutions that include cameras equipped with LPR integrated into the access control system.

3. Cost-effectiveness

According to Arvind Mayar, CEO of Secure Parking Solutions, many customers are concerned about the initial investment for a solution. While high costs can deter many end-users, systems integrators and solutions providers should be able to convince customers of the long term financial benefits that increased operational efficiency would bring.

4. Multiple payment options

Customers should be given the option to pay in their preferred mode. This could be card, cash, or a mobile payment system like Apple Pay. This could speed up entry and minimize the chances of long lines forming.

The parking management software should be easy to configure and set up, and should be able to calculate the parking duration and cost. In the case of cars that have management-issued passes, the system should be able to exclude them from payment.

5. Integration and retrofitting

Solutions that can be integrated into existing systems are necessary for older buildings. Considering that there are already several malls in many developed countries, systems integrators will often have to work within certain constraints.

6. Analytics

Analytics solutions provide deeper insights into the behavior of customers, allowing management to improve the customer experience and optimize operations. These solutions can also provide information on the status of machines and if they require any maintenance. Reports can be automated and scheduled to be sent by email at regular intervals.

In short, the requirements of the customers in the field are a mix of solutions that would improve safety and business operations. For SIs, knowing the right hardware and software to put in place, integrating them with existing systems, and ensuring their seamless operations is what matters most.

Consultants Speak: How to Select Parking Management Solutions for Malls

Although several advanced parking management solutions have hit the market in recent years, many shopping centers and malls have stuck with traditional systems.

Speaking to a&s, Ian Goodwin, owner of the Parking Consultancy, pointed out that traditional systems use a barrier with a ticket vending machine where the driver pays upon exit.

However, as technology evolves and malls look to improve their systems, solutions like license plate recognition (LPR) will become more common. LPR would be especially useful in places where the parking is free but only for a limited amount of time. An LPR system can assist in tracking how long a car has been parked in the parking lot.

Given the several different brands of parking solutions on the market, the customers should know what to prioritize when making a purchase. Here we list some of the major factors to consider when buying a parking management solution.

1. Reputation and cost

This would seem like an obvious point to some, as going with a reputable brand is

Ian Goodwin, Owner, The Parking Consultancy

necessary for reliability. However, those who are familiar with the industry will tell you that reputation and cost do not always go hand in hand. Quite often, customers compromise on the quality of a product for the sake of cost. In Goodwin's opinion, zeroing in on a few brands that have a history of providing reliable products is a good way to start.

Goodwin pointed out that especially in the U.K. market, several Asian manufacturers, especially those from China offer reliable solutions that are easy on the pocket as well.

2. Sticking to a single brand

There are companies that provide either hardware or software alone for parking management. In Goodwin's opinion, it's better to stick to complete solution providers who sell both hardware and software.

"Sometimes the hardware and software may be manufactured by separate companies ... But in my opinion, it's much better to stick to in-house built software," Goodwin said.

3. Installation and support

The company should provide support for the installation and setup of the solution from scratch. Make sure the solution requires minimal maintenance while ensuring that quick after-sales service is assured. Some experts suggest ensuring the company has a local presence as a priority. This would help them understand the local conditions and provide suitable support.

Any downtime of the product will lead to losses for the management. Hence while purchasing a solution, the customers should be clear on how quickly the company will provide maintenance support in case of a malfunction.

"There should be agreements in place with the solutions provider about the after-sales service," Goodwin said.

4. Detailed reports

The solution should be able to provide a structured and detailed report on the payments made by customers, who is in a car, and, if possible, analytics data to the management. This will help understand factors like the peak time and frequency of users and help in making informed decisions on tariffs and other rules.

5. Friendly but secure

Customers who visit a mall are not going to be happy if the parking solution is not easy to use. Hence being user-friendly should be a priority. This will also make the work of mall staff easier. However, user-friendliness should not come at the cost of security.

6. Third-party integration

Being able to integrate the parking management systems with other systems like security and safety solutions will help in ensuring better management. Integrated systems can work quickly in the event of any unwanted incidents. Such solutions are also easy to operate and control from a management perspective.

Some Major **Parking Management Solutions** for **Malls**

Several companies across the globe provide parking solutions for malls and shopping centers. Even within them, there are categories like those who provide hardware alone or software alone. The best thing about most of these companies is that they are continuously trying to innovate using the new technologies that come on to the market.

Here are some of the most prominent providers of parking management solutions. These are companies that meet certain criteria related to good performance in the mall and shopping center vertical. Please note that this list is by no means comprehensive. We would welcome more companies in this field to get in touch with us and let us explore their solutions.

Park Assist www.parkassist.com

Headquartered in New York, Park Assist provides a camera-based smart-sensor system and customizable way-finding signage to manage parking in a range of verticals, including the retail sector. The system goes beyond just assisting parking activities, it can also provide business intelligence that helps companies improve their bottom lines. Some of its features are:

•Upon arrival, exterior and entry way-finding signage show vacancy counts that help parkers to choose a facility and/or parking level. •After entering, interior way-finding signage and directional in-aisle pointers provide follow-up parking guidance, helping them make on-the-spot decisions within a chosen level. •This is where smart-sensors take over — as their bright color-coded LEDs signal parkers quickly to open spaces. •When parkers return to their vehicles, Park Assist closes the loop with the exclusive vehicle locator feature. •Park Assist mobile APIs can also be used to make customer-facing features accessible through a wide range of standards-based apps for smartphones and tablets.

Designa parking solution in use a the Wörnitz Truck Stop (Source: Designa)

Designa www.designa.com/int/home.html

The Germany-based Designa offers PM ABACUS a parking solution that works across verticals. In malls and shopping centers particularly, this solution takes the entertainment aspect of malls to another level by offering raffles on tickets, potentially offering business value to the mall management. Some of its features are:

•Flexible authorization (magnetic strip, barcode, smartphone, RFID) •Integration in an authentic Cloud service •Web & app services •Lowest energy consumption in its class •Height of the control panel can be adapted to the latest car dimensions •Robust and resistant thanks to high-quality aluminum housing • Flexible when it comes to integrating new functions

Skidata https://www.skidata.com

Based in Austria, Skidata has a presence in several countries across the globe. The company's parking management solution for shopping centers offers flexibility to adapt to the customers' business requirements.

•Convenient parking for a relaxed shopping experience •Parking spaces exclusively for customers and employees •Validation solutions for customers •Payment for parking ticket with the purchase (Shop & Go) •Discounts and VIP parking lots for regular customers •Parking space reservation •Separate employee parking spaces

A HUB Parking Technology solution installed at The Two Rivers Shopping Centre, England (Source: HUB Parking Technology)

HUB Parking Technology www.hubparking.com

HUB Parking Technology is based in Italy. Apart from providing parking guidance solutions, the solution reduces risk and fraud in cash handling on the shop floor, analyze a parker's preferences and behavior, frequency and peak times and many more.

•Pick any color to distinguish the pay station from a dull grey background. •Offers many payment methods such as coins and notes but also by the acceptance of credit or debit card and Chip & PIN options. •Engendering loyalty through regular users or store-related promotions, loyalty cards and similar. •Machines which demand the least from the operator in terms of maintenance, training, and operational costs

Urbiotica www.urbiotica.com

The Spanish company Urbiotica offers technological components required for the guidance of drivers within the parking areas.

•Outdoor wireless sensing system to gather the real-time parking availability by spot or by areas •Indoor ultrasonic sensors and level controllers •Dynamic message signs and totems adapted to privately owned public parking •Web and mobile applications for guidance, system management and analyzing the use of the parking spaces and areas

Urbiotica's wireless sensing system in use at Shopping City Süd in Vienna, Austria (Source: Urbiotica)

Smart locks for smart homes have gone from a means of simplifying entry to complex devices offering a multitude of features.

Some locks can now be integrated with popular voice assistants such as Amazon Alexa and Google Assistant. Remote monitoring, smartphone-controlled access and the ability to provide temporary digital keys for short-term users and delivery drivers is also available.

While the DIY nature of early smart locks was successful in appealing to early adopters, increasing complexity and a need to reach consumers beyond technophiles means professional installation services will be crucial to market growth. Other challenges include competing protocols with limited interoperability, security concerns and a lack of user education.

● **BY** Elvina Yang, Freelancer

Home Smart Locks: Trends and Challenges

Smart Lock Benefits: Remote Access, Voice Control and Temporary Access

Smart locks started from a simple idea — giving people remote access to their homes. However, new devices on the market now offer an extended range of features, including voice control and one-touch entry.

Remote access is still the primary advantage of smart locks, but in recent years the number of functions has been extended to include new features, such as one-touch entry and integration with voice assistants. The focus here is on keeping the experience simple. It's a lock, so there's no need to complicate things, and every new feature has to reflect that otherwise consumers won't go for them," said Ramon Llamas, research director at IDC.

Smart locks now allow users to check if a door is locked or grant friends and family access from any location, all using a smartphone.

One-touch entry can automatically sense a smartphone and unlock a door when the user approaches, eliminating the need to enter a passcode, find a key or open an app.

Some smart locks are burnished with the added security of a built-in biometric fingerprint scanner, ensuring only authorized persons are granted access.

Another trend in the smart lock category is integration with voice-activated platforms and smart assistants, such as Amazon Alexa and Google Assistant. For instance, smart locks from August Home let users lock and unlock the door and check a lock's status using Alexa.

Control4's smart home systems Intercom Anywhere and Door Station feature a smartphone voice and video intercom, activated via a smart doorbell. Homeowners can also

schedule doors to be locked automatically at certain times.

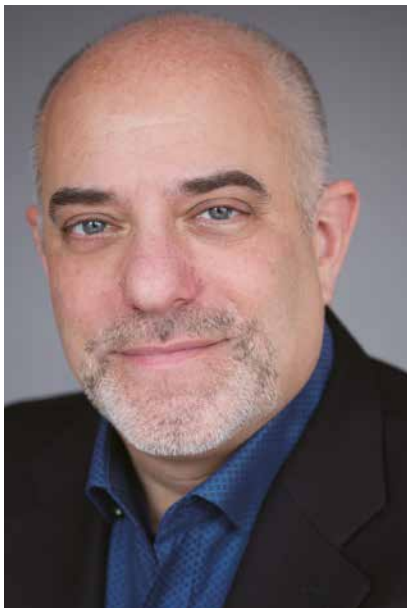
Amazon Key, an Amazon service enabled by smart locking systems and other connected gadgets, has created a new way for deliveries. Not only does key allow an Amazon delivery person to put packages inside a customer's door, with the help of smart locks and smart cameras users can also view live video of the delivery via a mobile app. Key additionally offers in-car delivery, whereby a package can be delivered to the trunk of a car using an smart locking system.

Back-End Management Tools Key for Commercial Users

Smart locks aren't only used in the home, but also in commercial buildings and rental apartments. In this market, property owners or office owners have shown a preference for multilock back-end management platforms. These allow users to check the status of all locks from a single interface, as well as receive notifications if any locks have been breached or tampered with.

"From the commercial side, keyless entry systems with back-end management tools are ideal for multidwelling units where the building owner can grant access to property managers, electricians, or plumbers that typically only require a one-time entry and should not need a tangible key to access a building," said Mitchell Klein, Executive Director of Z-Wave Alliance.

For those using short-term rental platforms, smart locks let owners provide remote access for specific time periods without worrying about circulating keys or reprogramming locks. With Airbnb, which has worked directly with smart lock providers including Danalock, August Home, Schlage and Yale, users can conduct the whole process via the site's own platform, creating a streamlined check-in and check-out experience.



Mitchell Klein, Executive Director, Z-Wave Alliance

Mass Appeal Hinges on Professionally Installed Smart Locks

While DIY smart locks won the hearts of early adopters, achieving mass-market appeal is likely to depend on professionally installed devices.

In an attempt to appeal to early adopters who enjoyed getting hands-on with new gadgets, the nascent smart home market often used the "DIY" label as a marketing tool. During this time, DIY smart locks, such as Schlage Connect, Kwikset's Kevo and August Smart Lock, emphasized the fact that homeowners could switch out their traditional lock without any outside assistance.

But as providers of smart home devices target mass appeal, firms are now underplaying the DIY aspect and have begun offering professional installation services.

"Pro installed smart locks are more popular among most consumers who are having professional security systems or whole home automation systems with extensive lighting control, entertainment integration and more installed," said Mitchell Klein, Executive Director of Z-Wave Alliance.

"This is largely due to the complexity and customization the customer wishes to have.

"Integrators have the tools to ensure not only that the device is functioning the way it was intended to, but to also confirm that all devices are properly connected to the network, automations are set up and working the entire system is secured."

Klein notes that as DIY smart home systems like Ring and abode have gained in popularity, more customers have bought smart locks to add additional security to their systems.

The Difficulties of 'DIY' Locks

For the average user "do it yourself" is often more aspiration than reality.

According to a 2018 survey conducted by management service provider iQor, 33 percent of consumers in the U.S. experienced issues setting up or operating a smart home device. Consumers spent 1.5 hours on average resolving these issues, in addition to an average of 1 hour working with customer service. 22 percent of respondents said they couldn't solve the issue after trying all possible solutions, or simply gave up and returned the product for a refund.

"While many companies claim to have DIY smart locks, the reality is that DIY is much more complicated

Source: Danalock

to do than what manufacturers think," said Hans Overgaard, the Founder and Managing Partner of Danalock.

The installation guide for the August Smart Lock Pro has 13 steps, including removing the existing thumb latch, choosing the correct adapter and installing DoorSense. The Kwikset Kevo smart lock, meanwhile, has eight steps, along with several additional instructions for each.

"The average user is capable of — at best — changing the thumbturn. This takes only two screws. If your solution goes beyond this, it is no more DIY. Perhaps for first movers, but not for the volume market .... So for now the market is very limited on DIY smart locks," said Overgaard.

He added that a big challenge was "the acceptance from manufacturers and buyers that not all smart locks are DIY, and that the market is still in a very early stage."

Specialist businesses have sprung up to cater to the increasing need for professional smart home installation services.

U.S.-based companies Handy and Puls, as well as Swiss company Mila, offer users the ability to arrange professional installation online. Big name retailers of smart home devices, including eBay, Walmart, Best Buy and , have also entered the installation business, with smart home system providers such as Control4 and Vivint Smart Home providing professional installation as standard.

Hans Overgaard, Founder and Managing Partner, Danalock

"Many people may not feel comfortable installing a door lock themselves and might prefer professional assistance. Also, if the door opening needs to be enlarged or made smaller or a dead bolt needs to be added, people might seek a professional's help," said Lew Brown, a Partner from Bluesalve Partners, a firm providing internet of things (IoT)-related consulting.

Smart Lock Success Depends on Support for Major Systems, Protocols

There's currently no universal protocol or system to follow in the smart home market. In order to streamline the smart home experience, smart lock companies should adopt major choices via agile development.

Smart locks have been integrated into smart home platforms such as Alarm.com, Samsung SmartThings, Wink and MiOS, to create unified ecosystems and events. These include disarming an alarm and turning the lights on when a smart lock is unlocked.

The integration of smart locks with security cameras and video doorbells is also an increasingly common sight. Cameras from Arlo and Wyze, and doorbells from Ring and Nest all work with smart locks. Homeowners are able to view footage from a door as well as perform locking and unlocking remotely from their smartphones.

"It's important that all devices in a home can be united — especially smart locks — to give homeowners customized control to suit their

lifestyle," said Brad Hintze, Senior Director of Product Marketing at Control4.

Hintze gave the example of Control4's Away scene. When homeowners leave for vacation, not only can the system grant access remotely and send push notifications if someone is at the door, it can also create a rotating schedule for lights in the house to turn on and off to make it look like someone is home.

"Each smart home system is personalized to the homeowner and family, while some may prioritize the need to remotely control their door lock remotely, and others many not need to do so," said Hintze.

When homeowners create their home systems with Control4 Dealer, they are able to select a customized array of features, such as smart locking, smart lighting control and shading, and multiroom audio and TV control. Control4 also allows homeowners to upgrade their system with new devices and experiences at anytime.

Choosing a Protocol: Zigbee or Z-Wave?

Connection protocols have contributed to the streamlining of the smart home experience. However, each protocol has a different role to play in the smart home ecosystem.

"Zigbee and Z-wave are the most common for residential wireless control because they are both popular mesh networks protocols that allow for easy communication to hundreds of other device types. And they are both commonly embedded into gateways/controllers that are connected to the internet to allow for remote access," said Lew Brown, partner of Bluesalve Partners, a firm offering internet of things(IoT)-related consulting.

Protocols that are commonly seen in smartphones, such as Bluetooth and NFC (near-field communication), were often used for close proximity entrance, Brown said. While these retain importance for enabling mobile access, they are limited by their inability to grant remote access.

Source: Control4

"Wi-Fi or Ethernet connected locks are also quite common, but require the lock to be connected to Ethernet, which is not an easy retrofit option," said Brown.

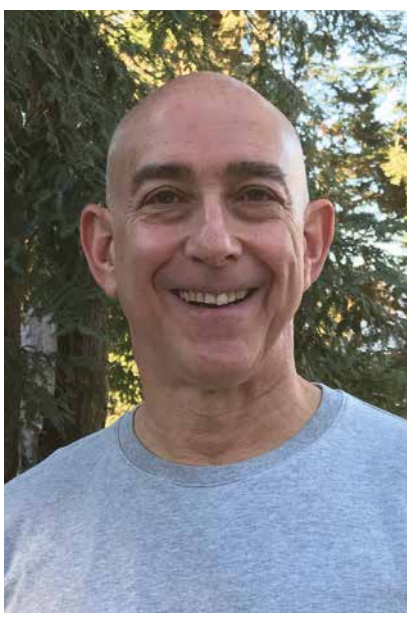
Currently, there isn't a single universal protocol dominating the market for smart locks, making compatibility with several major protocols somewhat of a neccessity.

A universal standard would, however, simplfy things for users. "Uniting all devices and protocols into one system benefits homeowners, giving them control of everything in one place. This also allows for sophisticated capability and customizations," said Hintze.

Smart lock company Danalock, whose products are Z-Wave, Zigbee and Bluetooth compatible, has achieved this through its agile development platform.

"An agile hardware platform for integrating larger proprietary protocols is super important, because the truth is that Z-Wave and Zigbee are not the only ones in the market. As a smart device manufacturer, you need to adapt. You can not expect the service or platform to do so. Agility is key," said Hans Overgaard, the Founder and Managing Partner at Danalock.

Brad Hintze, Senior Director, Product Marketing, Control4



Lew Brown, Partner, Bluesalve Partners

Smart Lock Adoption Still at an Early Stage

While the growth outlook for the emerging smart lock market is positive, companies will need to focus on customer education and the user in order achieve success.

The security benefits of smart locks are manifold, allowing for remote monitoring of a user's home, and the abilty to provide temporary access. But the possibility of a lock being breached is still a worry for homeowners. Smart lock companies and connection protocol alliances, however, are working hard to ease these concerns. The Z-Wave Alliance, for example, released the Z-Wave Security 2 (S2) Framework in 2017.

To eliminate the hassle of providing physical keys for visitors, LILIN's smart locks utilize single-use QR codes. However, canceling a QR code for a visitor could cause security issues, since they could still hold a valid code. To combat this, LILIN's QR code pass "creates backward authentication while scanning the QR code on LILIN door station to LILIN cloud for checking if the QR code is valid. The QR code access control can solve the issue of getting a physical key hidden in the floor mat of a mailbox for a B&B visitor," said Steve Hu, Product Manager at LILIN.

8.1 million smart locks were shipped in the U.S. in 2017, according to data from research firm IDC. Sales are expected to climb to 9.7 million in 2019, and up to 34.1 million by 2023. While there is still plenty of room for the smart lock market to grow, it will not happen overnight.

"It won't be instantaneous, as education to consumers is imperative to demonstrate value and drive adoption beyond the traditional door lock option," said Ramon Llamas, research director at IDC.

Llamas suggested companies try to highlight all the benefits of smart locks in order to win over smart home consumers. "In the long-term, I'm hoping to see greater interoperability with other home systems, like sensing that the household has gone to bed and the doors automatically lock on their own without any human interaction.

"Another long term challenge is differentiating devices in an increasingly crowded market, as many smart locks accomplish the same results. This could also lead to market consolidation, because no company is automatically guaranteed success and longevity."

Steve Hu, Product Manager, LILIN

Danalock would like to tackle the market challenge with an approach that makes the user central.

"The market holds huge opportunities, but the only way to succeed is by working together and not making the same mistakes as have been made over the past five years," said Hans Overgaard, the Founder and Managing Partner at Danalock.

He gave an example that service providers used to think lights and switches were the way to win consumers' heart, which proved to be untrue. To date, Google Home and Amazon Echo are the only smart home products that have been successful.

"These are the only products to actually bring something smart to the table, and something users can use everyday, and which don't complicate consumers' lives," said Overgaard.

Overgaard sees the same potential for smart locks, which replace physical keys with access controlled via our now ever-present smartphones. "It is one of the only products that actually brings a fundamental benefit to the end-user."

Smart Home Devices by Category, 2017 and 2022 (Value in US$Million)

Product Category	2017 Value (US$M)	2022 Value (US$M*)	CAGR, 2017 – 2022*
Video Entertainment	$133,091.48	$201,063.36	9%
Home Monitoring/ Security (Connected door locks, cameras, moisture sensors, door bells, and more)	$4,271.30	$12,136.50	23%
Smart Speaker	$4,401.39	$17,431.00	32%
Lighting	$1,120.53	$3,511.32	26%
Thermostat	$1,774.35	$3,875.91	17%
Others	$17,532.54	$38,963.93	17%
TOTAL	$162,191.59	$276,982.02	11%

Source: IDC Worldwide Quarterly Smart Home Device Tracker, March 2018

* Note: Forecast Values

CLIMAX GX-8 VOIP SMART CARE ALARM PERSONALIZES SENIOR CARE AND VOICE INTERACTION

In the aging trend of 21th century, home care is moving towards telehealth monitoring and telemedicine. With such growing demand for related services including video call and remote monitoring, caregiver efficiency is enhanced while still providing constant convenience to the patients. Climax GX-8 is designed to help the elderly who live at home to manage their long-term health conditions, bridging the information of healthcare to the hospital and meanwhile fulfilling care gaps at home.

Considerate Elderly Health Supports, All at Home

GX-8 can be flexibly connected with third-party Bluetooth (BLE) healthcare sensors, like blood glucose monitor, pulse oximeter, or heart rate monitor, for tracking health data and providing customized alerts when necessary. Users can directly share measurements with their doctors or physicians, ensuring stable health checking for themselves.

In addition to health trackers, GX-8 is also compatible with Pivotell Advance Automatic Pill Dispenser to keep secure of all pills, and remind the seniors to take the correct medicine at the pre-set time. The solution allows health professionals to monitor pill taking timely results and keep an eye on the patients' early treatment as needed.

For some special occasions that remote care given is insufficient and the user needs onsite assistance, GX-8 can inform the caregiver or medical personnel for immediate actions. The system also keep the user's family member in the pace with the handling progress such as professional personnel's arrival, case completion or further assistances required. The seniors are assured that they've always been taken care of.

Voice Is the Best Control Interface for the Elders

One control interface that everyone agrees for the elderly is voice command. Working with the leading voice ecosystems Amazon Alexa and Google Home via cloud, GX-8 also features voice recognition for customized emergency alert trigger and control. "Alexa, tell Climax I need help!" can be the conversation when a user is looking for emergency assistance.

With the VoIP (Voice over Internet Protocol) feature, GX-8 communicates in two-way voice calls using broadband Internet connection. Users are able to contact their caregivers or family members through voice extenders (DECT/Wi-Fi), talking pendants, call points, and voice extenders at emergencies. In the other way round, GX-8 also alerts seniors by voice in case of any events at home.

To realize independent living in a smart way, GX-8 enables the whole-home control with various protocol-of-choice. When paired intelligently with Zigbee or Z-Wave sensors, GX-8 can either turn on the hallway lights automatically when the sensor reports a senior's movement in the dark to reduce chance of fall; or adjust air conditioning incase there are sudden temperature-drop. The scenarios are unlimited to fit individual demands, ensuring a safest living experience for the senior users.

A Bluetooth pendant also works with GX-8 to activate smartphone geolocation services. That fulfils the true automation of home settings before the senior arriving the home. In the meanwhile, the geolocation service provides the alert message with location info when the user is out of home and needs emergent helps. ■

Climax Technology ▶ www.climax.com.tw ▶ sales@climax.com.tw ▶ Tel: +886-2-2794-0001

Climax GX-8 VoIP Smart Care Alarm

- Communication path: IP (Ethernet), LTE
- Built-in protocol options: RF, DECT, and Zigbee or Bluetooth
- Optional expansion via USB dongle: Z-Wave, or Wi-Fi
- Compatible cloud platforms: Amazon Alexa, Google Home, and IFTTT
- Senior care & emergency monitoring
- Connect with BLE medical devices
- Voice activation
- Smart home automation
- User-friendly smartphone app and web portal
- DAB radio

BUSINESSES ARE USING **FACES** TO GAIN **SECURITY** AND **BUSINESS INSIGHTS**

Facial recognition has become a part of daily life whether we like it or not.

● **BY** Eifeh Strom, Freelancer

Smartphones and social media all utilize facial recognition, and user acceptance has paved the way for more varied uses. While the technology is still mostly associated with security, government and law enforcement, businesses are taking advantage of it as well for both security and business intelligence purposes.

The overall global facial recognition market is growing, expected to reach nearly US$7.8 billion by 2022 at a compound annual growth rate (CAGR) of 13.9 percent, according to a report by MarketsandMarkets. The report cites the growing need for surveillance in public spaces as a major contributor to growth.

The unique capabilities of advanced facial recognition can be applied to almost any vertical. Also, since the technology requires no physical contact or credentials that can be lost, stolen or replicated, it is an attractive solution for many different applications. Add in the insights businesses can gain from its ability to easily identify and track individuals — which could provide them with valuable data to perform advanced trend analysis, productivity research workflow processing and so much more — it is no wonder more and more businesses are deploying facial recognition solutions.

Making Businesses More Efficient With Facial Recognition

Businesses are deploying facial recognition technology to increase operational efficiency and learn more about customers.

Nowadays everyone is using facial recognition and businesses are no exception. The use of facial analytics solutions to gather information on demographics and consumer buying patterns is expected to grow signifi-

cantly in the coming years, according to a report by MarketsandMarkets.

Adoption of face recognition technology is growing across industries, which is being fueled by growing awareness, advancements in the technology, and accessibility. For instance, the development of advanced facial recognition analytics that are centralized has made it relatively easy to apply to any networked camera, explained Shawn Mather, Director of Sales for the U.S. at Intelligent Security Systems (ISS).

With businesses also looking for more ways to utilize smart technologies, and with artificial intelligence (AI) and deep learning gaining momentum, the use cases for facial recognition have opened up. Additionally, improvements in video surveillance cameras have allowed "organizations to realize the full value of video surveillance investments," according to Stephanie Weagle, CMO of BriefCam.

"The growing sophistication of video content analytics (VCA) systems combined with the market's fuller understanding of the ways in which video analytics solutions can drive organizational efficiency and performance alongside security, has resulted in businesses of all types taking a deeper interest in VCA and face recognition," Weagle said.

From a retail perspective, leveraging facial recognition technology allows them to better understand customer demographics (e.g., gender, age, etc.). This data provides the retailer with a better understanding of who their customers are, which could enable them to better personalize the shopping experience and tailor their marketing strategy.

"When companies educate themselves on demographic composition, they create business intelligence opportunities to improve convenience in how people interact with their built environments and to enhance the personalization of experiences in advertising," explained Dan Grimm, VP of Computer Vision and GM of SAFR at RealNetworks.

Shawn Mather, Director of Sales, U.S., Intelligent Security Systems (ISS)

Grimm explained that companies can use facial detection and characterization, which does not retain any biometric information, to gain actionable insights of their customers. "For example, shopping mall owners will be able to make better advertising, leasing and customer service decisions if they know that between the hours of 12 p.m. and 1 p.m. they tend to see traffic of X number of persons broken down by 60 percent female, 40 percent male, with an average age of 42, based on a single IP camera properly tuned for an entrance," he added.

Businesses are also using facial recognition to create customer loyalty programs to help identify VIPs.

Mather also highlighted the use of facial recognition in workforce management. This is a trend he sees on the rise globally. The ability to accurately identify and track personnel for time and attendance management with facial recognition is especially being sought after. Facial recognition is being deployed for this purpose in a large number of industries where large, but often temporary workforces are being deployed to either permanent or temporary sites, he said.

"Perfect examples are factories and construction sites, where shifts change based on delivery schedules and production lines, and different groups of specialized workers need to be on production lines at different intervals," Mather explained.

These are just some of the ways businesses are using facial recognition technology for nonsecurity purposes today. In the near future, many expect facial recognition to become more mainstream where its use for even more business intelligence operations will continue to grow.

How Businesses Use Facial Recognition to Enhance Security

Facial recognition is helping businesses stop thefts and keep environments more secure.

More and more businesses are using facial recognition technology to improve situational awareness. Doing so gives businesses a smarter, easier way to monitor who is entering, staying and leaving their environment, while also increasing safety, security and convenience.

Doug Aley, CEO of Ever AI, noted that "mission-critical" applications form about 75 percent of the facial recognition market. This includes use cases such as security

surveillance, access control, digital authentication and government and law enforcement applications. According to a report by MarketsandMarkets, the increased need for enhanced surveillance and monitoring at public places and the increased use of the technology in industries such as the government are driving the market growth.

While the main purpose of deploying a facial recognition solution is security, it is also about "empowering individuals to use their faces as a token to gain fast safe access and authentication," said Dan Grimm, VP of Computer Vision and GM of SAFR at RealNetworks.

Stephanie Weagle, CMO, BriefCam

Facial recognition is "ideal" for environments that need to positively identify individuals for physical and data security clearance, general access permissions, compliance with mandated regulations, and financial verification, according to Shawn Mather, Director of Sales for the U.S. at Intelligent Security Systems (ISS).

In a business environment, such as retail, "this could mean leveraging footage of different shoplifting incidents, assembling a suspect watchlist using frames from video surveillance, and then responding to alerts triggered by a video content analytics (VCA) system's detection of a biometric match for the suspected shoplifter," explained Stephanie Weagle, CMO of BriefCam. From there, security or police officers could investigate further to determine whether the alert has correctly identified the shoplifter and, if so, apprehend the perpetrator before the store bears further losses.

Facial recognition can also be used to provide live analytics for industries where there are high numbers of unknown visitors (e.g., malls, retail spaces, event venues, stadiums, etc.). This also applies to large enterprises with high visitor flows, such as hospitals, universities and stadiums, that have a need to know when persons of interest appear on camera.

> "Facial recognition can also be used to provide live analytics for industries where there are high numbers of unknown visitors."

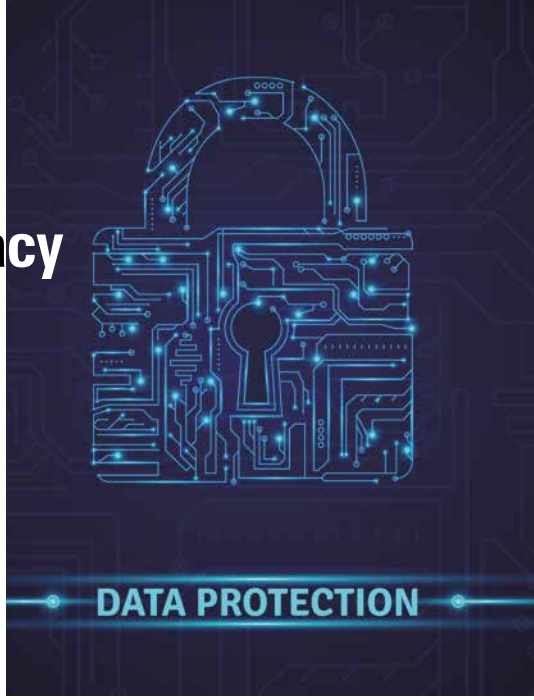
Grimm used a sports stadium as an example. Stadium operators might flag banned patrons in its database, while box owners may want notifications when VIPs are onsite, in order to properly greet them and provide a superior level of customer service. "To support effective 'watchlists' — both for threats/concerns and for VIPs — facial recognition systems must be adept at high accuracy under the real-world conditions of identifying people in live video. This means avoiding false positive matches and reliably identifying people despite variations in lighting, orientation and facial occlusions due to scarves, glasses and hats," Grimm explained.

Customers from schools, office buildings and manufacturing are also using facial recognition to provide secure access to facilities. "In these cases, facial recognition systems enhance security in ways that are superior to badges, which can be easily stolen, and also offer features that catch piggybacking instances to offer a more accurate assessment of who is entering and exiting," Grimm explained.

Facial recognition can also enhance convenience over existing access management solutions. For example, with facial recognition users no longer have to deal with situations where badges are forgotten at home or left on a desk. Grimm added that for secure access, facial recognition solutions should include anti-spoofing to prevent unauthorized access to those attempting to use a photo to gain entry.

How Businesses Should Protect Privacy When Using Facial Recognition

As facial recognition becomes more ubiquitous, concerns about privacy are at an all-time high.



Facial recognition has been entrenched in controversy lately. San Francisco recently made headlines by becoming the first city in the U.S. to ban the use of facial recognition technology by law enforcement and government agencies; however, businesses are not included in this ban.

Built-in facial recognition in smartphones has helped ease the general population's concerns over biometrics by making it a norm. However, many civil liberties groups and consumers are still just as concerned about how enterprises are using and storing facial recognition data.

The determination of privacy is often dependent on the use case. In some instances, privacy is determined by the governing entity. For example, the Global Entry program, administered by the US Department of Homeland Security, uses facial recognition to verify that the person in front of the camera is the same as the one in the passport photo. "Not only is consent and privacy in this instance 'implied,' but also legally mandatory," said Doug Aley, CEO of Ever AI.

Doug Aley, CEO, Ever AI

On the other hand, consumer expectations of privacy and consent are often contingent on the application. "We typically find implied consent in situations where consumers are expecting it (e.g., consumers expect that bad actors are not allowed entry into the country, and so the concept of face recognition to identify them is acceptable)," Aley explained. However, there is a delicate balance that will come down to the difference between mission-critical applications (e.g., where the government doesn't need permission to use an individual's face) versus general purpose face recognition for casual, entertainment-focused applications, he added.

In terms of legislation, laws regarding privacy are rapidly evolving around the world. In the U.S., states such as Illinois, Texas and Washington have specific biometric privacy laws governing the use, collection and storage of biometric data. In Europe the General Data Protection Regulation (GDPR) also has specific clauses mandating how biometric data can be collected, used and stored. For example, the GDPR states that EU residents must give explicit consent before their data can be collected, and that they have the right to withdraw consent at any given time — this is known as "the right to be forgotten."

Dan Grimm, VP of Computer Vision and GM of SAFR at RealNetworks, believes regulations are needed at a national level in the U.S., not just by jurisdiction. This would help to provide a baseline for how facial recognition can be deployed in ways that take into account the "important missions of our customers and the interest of the general public."

While making sure all facial recognition deployments abide by privacy regulations is a given, whether in the cloud or on premises, businesses can further maintain privacy by doing their part. This should include ensuring that all data is encrypted in transit and at rest; systems are built with stringent cyber protections; providing the ability for individuals to be deleted from a system; and offering an opt-in/opt-out structure that encourages users to provide consent around the use of facial recognition.

"For SAFR from RealNetworks, we find this particularly important and not only include these features out of the box, but also provide our customers with best practices for implementing facial recognition," Grimm added.

From a consumer's perspective, concerns surrounding facial recognition rests more in the hows (e.g., how it is being used, how it is being transmitted and how it is being stored) rather than the actual use of the technology, according to Shawn Mather, Director of Sales for the U.S. at Intelligent Security Systems (ISS). For this reason, he explained that privacy is much more an issue of application.

In the future, we can expect that governments worldwide will continue to develop policies to regulate the use of biometric technologies, as well as define the rights of opting out of being tracked digitally. We may even see more cities opt to follow in the footsteps of San Francisco and ban certain applications of facial recognition technology altogether.

What's Required for Businesses to Deploy Facial Recognition?

Getting the most out of facial recognition requires the right equipment; however, needs may vary by application.

The hardware needs of businesses wanting to deploy facial recognition can vary depending on the application. Not every situation requires the highest resolution camera or the highest computing power, nor does every every environment pose the same challenges (e.g., lighting, crowding, weather, etc.).

Generally, in order to deploy a facial recognition system what is needed are a well-tuned camera, local computing power, and software. Hardware systems must be paired with the appropriate computing power to run facial recognition efficiently, which depends on whether you are managing a high- or low-density environment.

Dan Grimm, VP, Computer Vision and GM, SAFR, RealNetworks

However, hardware requirements can vary greatly depending on the application and deployment architecture. For example, secure-access use cases, where you are viewing a few faces at a given time, can leverage lower-resolution cameras with lower frame rates and require less computing power (in addition to deploying fewer cameras), which effectively lowers your total cost of ownership (TCO), explained Dan Grimm, VP of Computer Vision and GM of SAFR and RealNetworks.

On the other hand, when using watchlists, deploying more cameras can improve accuracy and performance. Grimm added, "If the facial recognition platform supports a distributed architecture by doing detection at the edge and recognition in the cloud, then you've not only lowered TCO, you've also increased your ability to scale in a massive way."

In the early days of face recognition, there was often a tradeoff between accuracy and device power. "Lower powered devices, either in terms of chipset, bandwidth requirements or camera resolution, suffered from lower accuracy," noted Doug Aley, CEO of Ever AI.

Today, Ever AI has had success in being able to deploy on everything from a single core legacy processor all the way up through a cluster of high-powered GPUs, like an NVIDIA T4. "There are now other companies like ours where the accuracy tradeoff is no longer an issue," Aley added.

Nowadays, speed is where the major variability comes in — the more powerful the hardware, the faster the speed of matching and the faster the overall user experience.

Aley explained that most modern chipsets, especially from a quad-core onward, are going to be very fast. Furthermore, today's face recognition models, and the frameworks off which these models are built, are getting more adept at handling lower-power chipsets.

Shawn Mather, Director of Sales for the U.S. at Intelligent Security Systems (ISS) highlighted software integration issues over complications with hardware. Software providers, however, can overcome these challenges by making their solutions compatible with VMS solutions and electronic access control solutions.

The type of facial recognition — 2D or 3D face recognition technology — a businesses chooses to deploy may also come with its own specific set of challenges and requirements. A report by MarketsandMarkets noted that captured images from earlier 2D facial recognition technology were highly dependent on illumination, meaning poor lighting significantly affected image quality. Another challenge was the "incompatibility of integration between software tools and biometric hardware devices."

However, the report expects 3D technology to have the largest market share in the coming years. Unlike 2D technology, 3D technology is not dependent on illumination. This enables it to capture higher-quality images in uncontrolled environments, such as poorly lit or completely dark areas.

Something else to consider in the years to come are facial recognition cameras, where the recognition process is done on-board at the frontend. These types of cameras, though, require strong computational power since all of the tools for recognition are on-board. While several camera companies are developing face recognition cameras, the overall market is still in a fledgling state, but may be something to look forward to in the future. A&S

Communication Solutions to Ensure Smooth Rail Operations

As societies across the globe become more and more urbanized, the number of metro systems continues to grow. A report from Technavio estimates compound annual growth (CAGR) in this sector of over 5 percent from 2017 to 2022 as investments rise and the rail-supplier market expands.

● **BY** Prasanth Aby Thomas, Consultant Editor

Some of the major trends seen in the railway business at the moment are mergers, increased digitalization, and efforts to fight cybersecurity. Although a plan by Germany's Siemens and the French Alstom to merge was vetoed by the EU on competition grounds, reports suggest that concerns such as pressure from Chinese counterparts could force companies to look for ways to join hands.

Digital technology is providing more scope for innovation, helping operators improve reliability, streamline operations, and enhance the customer experience. With the arrival of the internet of things (IoT), manufacturers are even exploring the possibility of digital twins of critical assets to simulate their operations and draw insights.

However, as digitalization becomes popular, cybersecurity concerns are also on the rise. Rail companies are forced to move from the earlier paradigm of "safe by design" to "safe and secure by design" as they assess each node of their network for vulnerabilities that could be exploited by hackers.

In this section, we take a look at how digital technology and communications systems are critical to better operations, factors and components that make a communications network robust, and onboard surveillance systems.

The Importance of Communications Systems in Rail

Digital communications systems enable reliable operations. But this is not a simple process.

For the smooth and efficient functioning of most modern transportation systems, a reliable communications system is necessary. In metro and railway systems, a communications system becomes all the more crucial due to the sheer number of components involved.

Managing train signaling systems, alarm systems, ticketing, video surveillance, and traffic management together in an environment of increasing volumes of corporate and passenger voice, video, and data traffic is impossible without robust communication solutions. In fact, this is the right of the passengers, according to industry experts.

"Smooth communications between the right people are needed to run operations in a safe and efficient manner," said Timo Harju, Business Development Manager of Vertical Markets at Airbus Secure Land Communications. "Lack of proper communications can result in a variety of issues, depending on the operational mode of the metro operator."

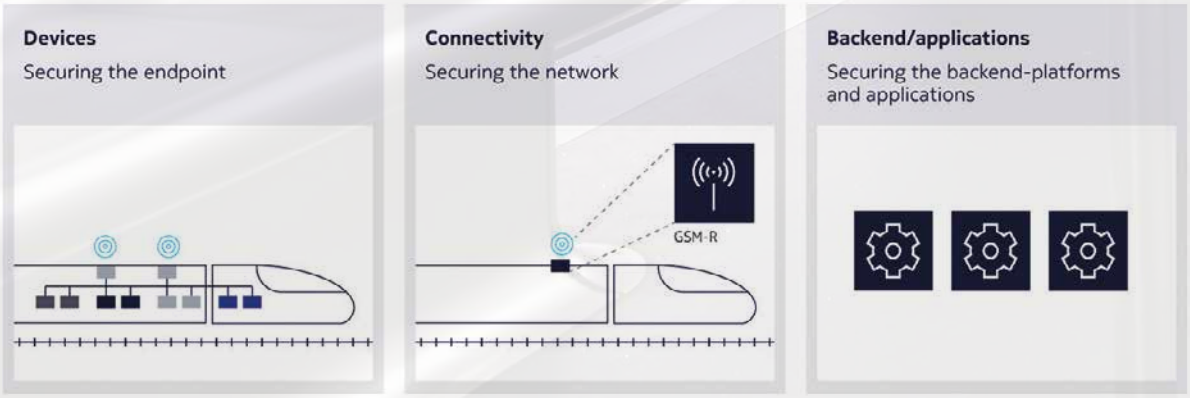
Karsten Oberle, Global Practice Lead for Railway Business at Nokia, agreed, adding that considering the critical requirements needed to operate a metro system today, it is almost impossible to function without a reliable communications network or with a network using outdated technology. Unreliable communications technology can severely impact many aspects of operations, safety, and security.

What a Lack of Proper Communications Could Lead To

Harju listed a few situations as examples that would suffer if good communication systems were not in place. The interesting point to note here is that while communications systems are necessary for the daily operations of transport, certain unexpected incidents could make things worse. For instance:

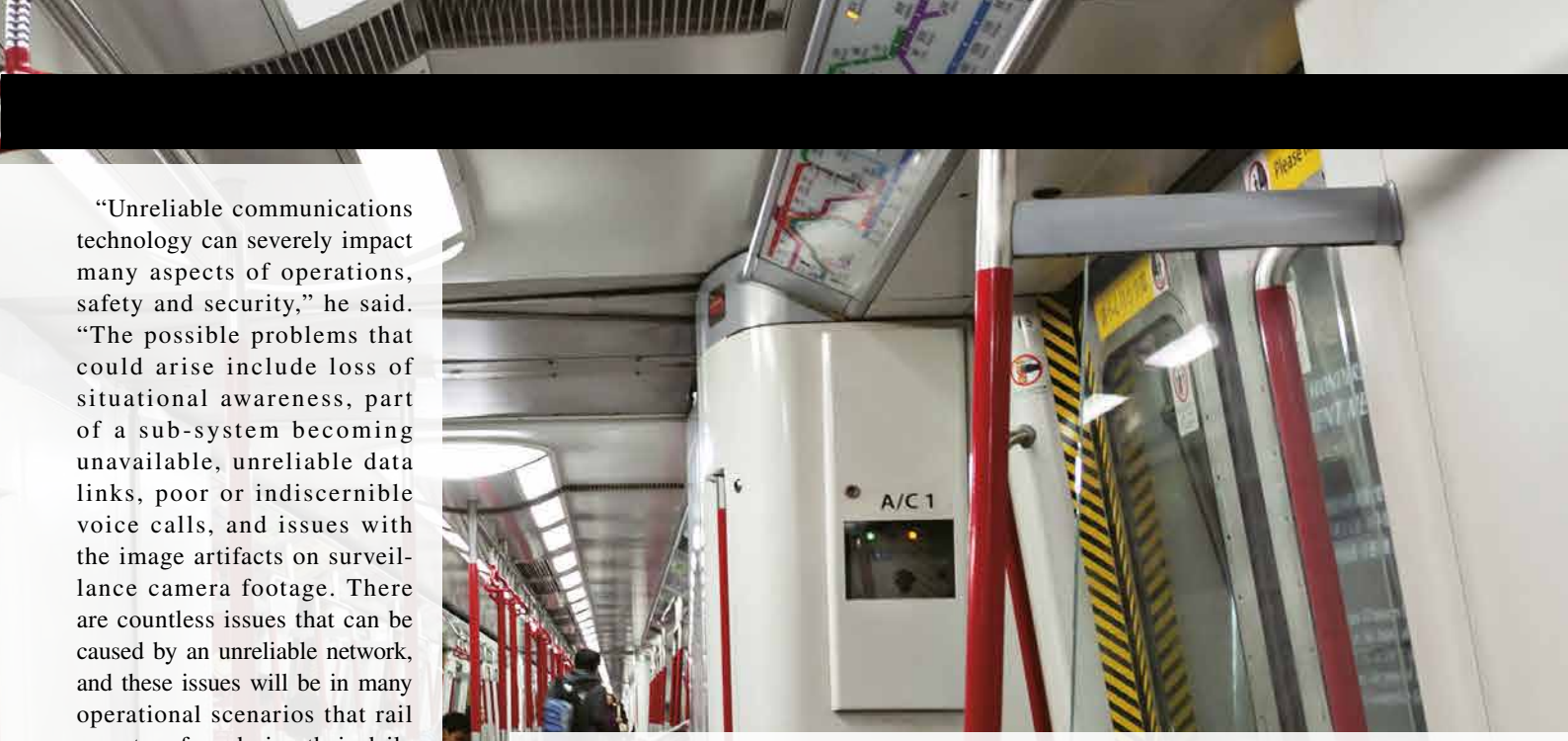
1. Getting help for a passenger in the case of a medical emergency and arranging guidance and access to the station areas for the emergency medical services
2. Having damaged equipment attended to by the maintenance teams so that the train can leave on time.
3. Coordinating schedule changes or replacement of faulty trains
4. Calling maintenance for defective station equipment such as the passenger gates
5. Making passenger announcements needed to inform passengers of any exceptions or changes in the train or metro service
6. Coordinating evacuations and/or closure of stations following security incidents
7. Ensuring safe switching operations

These are just some examples of situations and activities where a communications system plays a key role. Oberle expanded on this, further stressing that, considering the critical requirements that exist to operate a metro system today, it is almost impossible to operate such system without a reliable communications network or with a network using outdated technology.



Full protection of railway operations and railway-related IoT can only be achieved through an end-to-end security approach.

Source: Nokia



"Unreliable communications technology can severely impact many aspects of operations, safety and security," he said. "The possible problems that could arise include loss of situational awareness, part of a sub-system becoming unavailable, unreliable data links, poor or indiscernible voice calls, and issues with the image artifacts on surveillance camera footage. There are countless issues that can be caused by an unreliable network, and these issues will be in many operational scenarios that rail operators face during their daily routines."

Ensuring Durability

According to Quester Tangent, a company that provides network communications solutions for rail networks, trains have a service life that is 10 to 20 times longer than most high-tech electronics products. Because of this, rail networks today are fitted and retrofitted with a wide range of network types and technologies.

"With advances in vehicle technology, new trains are more data driven," the company notes. "Video surveillance, passenger information systems, health monitoring, and other applications place a high demand on train communication networks. And, expectations for managing and transmitting data quickly and securely have increased dramatically. More than ever, fleet operators and rail vehicle manufacturers need companies with an in-depth understanding of train communication networks to provide strong integration and increase compatibility with older fleets."

Major Factors in a Robust Rail Communications System

Control and safety are the main aspects of a robust rail communications system. But with the arrival of more connectivity, there has been a paradigm shift.

A strong communications solution enables safe, on-time and fully connected journeys. According to Karsten Oberle, Global Practice Lead for Railway Business at Nokia, some of the major factors of a robust communication system include train control and security.

Timo Harju, Business Development Manager of Vertical Markets, Airbus Secure Land Communications

Obviously, the ultimate goal of a communication system is to ensure information reaches the right recipient quickly and accurately. What differs in the application is the kind of information transferred and its purpose.

Communications-Based Train Control

Communications-based train control (CBTC) is a railway signaling system that employs telecommunications between the train and track equipment to manage traffic and control infrastructure. CBTC systems provide more accurate information on train locations compared to traditional signaling systems.

"Connectivity is essential for many metro subsystems including signaling, ticketing, control, voice applications and more," Oberle said. "Communications-based train control (CBTC) enables automation and increases the capacity and efficiency of a metro rail system. As the name implies, CBTC cannot function without a reliable communications network."

Surveillance Camera Systems

Current metro systems also rely heavily on surveillance cameras to ensure the safety

and security of the rail infrastructure and of the passengers. Without a reliable network, it is impossible to have a reliable security system supporting a very large number of cameras. A surveillance system can, for example, detect a person on the tracks, alert the operators, and warn the incoming train of the situation ahead.

However, some industry players point out that video surveillance solutions in railway networks are not as strong as they should be due to their fragmented nature.

The embedded solutions provider Kontron argues in a white paper that implementing new commercial off the shelf (COTS) open architecture provides the flexibility to integrate multiple systems, scale, and configure easily to customer requirements. These application-ready computing technologies allow developers to easily customize and configure intelligent, data-driven video surveillance systems targeted at a variety of transit system needs.

Operational Communication

A reliable voice communications system is also needed for a dispatcher to communicate with the train drivers on movement orders, according to Oberle.

"During rush hours, every second count towards efficient operations. Voice communications are also essential for staff performing maintenance work as well as critical in assisting passengers in distress," Oberle noted. "On the security side, for example, a reliable network ensures that the operations and control center can alert security staff when a public safety situation arises. And the public address system is critical for crowd control."

Timo Harju, Business Development Manager for Vertical Markets at Airbus Secure Land Communications, agreed that a robust communications network was essential for daily operations, conveying important messages to various stakeholders and, above all, ensuring security.

"The whole idea of communications is to be able to reach involved personnel, instantly, at any time," Harju said. "This maintains the opportunity to keep people informed when needed, to improve their awareness of situations, and also to improve and speed up response to critical situations which need immediate attention.

In several of the new metro lines that Airbus Secure Land Communications is equipping, disaster recovery solutions such as base station and client dual-homing are being implemented as standard. This increases system robustness, even during disasters. Communication is the key tool to coordinate and ensure smooth operations between and inside teams.

IoT Integration

The internet of things (IoT), which has made inroads into almost every industry in recent years, is expected to play a major role in railway communications systems as well, according to Kontron.

"By integrating video surveillance systems across a highly leveraged wired and wireless network infrastructure, operators gain an improved comprehensive real-time view of trains, tracks, depots, and stations," Kontron said. "Monitoring these assets through video management systems at the control center or by staff operating in the field, connected IoT-enabled video surveillance systems can see the entire network of cameras."

These allow for more advanced features like critical analytics that help operators gain actionable intelligence, which in turn aids better performance.

Key Components of

From wired to wireless solutions, is a wide network that is secured

Broadly speaking, the communications systems in rail networks can be classified into wireless and wired. Both have a role to play in rail networks, and have standards they need to comply with. Here is a look at the requirements to make each system robust.

Wired Solutions

Karsten Oberle, Global Practice Lead for Railway Business at Nokia, points to the following factors for a robust and solid wireless system.

1. The intrinsic reliability of the equipment itself. For example, a consumer or enterprise-grade network switch won't have the same reliability as that of a mission-critical grade switch that has redundancy built-in
2. High network capacity to move a massive amount of data from different applications
3. Network resiliency features to

f a Metro Communications Network

standardization is must for a metro communications network. So as much as possible against breaches.

Karsten Oberle, Global Practice Lead, Railway Business, Nokia

maintain the overall functionality of the communications network even if there are link or node failures

4. Traffic separation and quality of service capabilities to ensure that each subsystem utilizing the network has priority and performance guarantees and won't affect the performance of another subsystem. For example, a user retrieving a file from a network server shall not congest the network and affect the performance of the CCTV system
5. Expandability. Since bandwidth needs are growing at an astonishing rate, a communications system must be able to accommodate such growth without major modification or replacement of key components

"Considering these critical points, the technology that can meet these requirements is mission critical [for an] IP/MPLS network solution," Oberle said.

Wireless Solutions

As for a wireless network, in addition to the wired network requirements, there are problems with security and multiuser scenarios. Securing a wireless network isn't trivial.

"If we look in the past years, many wireless networks were compromised due to loopholes or even social engineering," Oberle said. "Network and cybersecurity are key characteristics that must be considered."

The multiuser, multiapplication scenario is also an important consideration. Since the same wireless access link is shared by several users and applications, it is important to use a wireless network solution that implements mechanisms that guarantees all users and applications can be served with resources from the wireless network and that, in case of congestion, mechanisms exist to assure the performance of the network.

A technology that meets all these requirements outlined is LTE. By having a private LTE network, a rail system can leverage a secure wireless network that delivers the best experience to their staff to perform their duties.

Widespread Network and Secure Devices

According to Timo Harju, Business Development Manager for Vertical Markets at Airbus Secure Land Communications, it is essential to have a reliable and widespread radio network also in difficult areas such as tunnels, depots, stations, and their vicinity. The core network must be redundant, and a network management system must always be implemented in order to monitor the network. "Two other fundamental points are to possess trustworthy, robust and secured devices (terminals) equipped with state-of-art applications which allow end-users to benefit from data communication, location tracking, group communication and dispatching for the Operations Centre," Harju said.

Airbus' Tetra technology, he added, offers tailored solutions according to specific requirements and needs, such as network element specific redundancy schemes, network topology, routing and spare route solutions within the Tetra network, disaster recovery plans, radio access solutions, and application-related redundancy solutions.

Complying With Industry Standards

Adhering to standards is critical to ensure the secure and efficient functioning of a communications systems. Oberle points out that both wired and wireless solutions in use are standardized.

"IP/MPLS standards are specified by IETF and IP/MPLS networks and are widely deployed worldwide by communications service providers as well as mission critical industry operators including railways," Oberle said. "LTE technology is standardized by the 3GPP forum and is present everywhere. It is the technology that powers the world's cellular networks, and private LTE solutions are in use by many industries today."

In the recent years, there have also been increased concerns on cybersecurity. It is now important to comply with relevant cybersecurity regulations and best practices to secure these critical networks against cyberattacks, and to implement a robust cyber security strategy. Railway operators can avoid potential loss of revenue and enhance their reputation as reliable providers of a hassle-free, on-time service.

Ensuring Flawless Video Surveillance Solutions for Metro Systems

Onboard video surveillance does not just aid in safety but also in gaining actionable analytical data.

Surveillance cameras have become an integral part of metro systems, as service providers try to ease safety concerns. Several surveillance systems manufacturers offer onboard solutions that are specifically tailored for metro and rail systems.

Security threats are not the only issues that security cameras can help solve. Video surveillance can be a highly effective cross-functional tool for improving operator efficiency and reducing costs, as well as enhancing the overall passenger experience, reducing delays or disruptions to service from unforeseen mechanical breakdowns, track obstructions or just traffic congestion.

Ensuring Secure Surveillance

For video surveillance, it is critical that a network be able to support a very large number of cameras and efficiently distribute via IP multicast many video streams to multiple monitoring stations and storage locations, according to Timo Harju, Business Development Manager for Vertical Markets at Airbus Secure Land Communications.

"A well-engineered end-to-end network will ensure that the critical requirements are met," Harju said. "Such network will be reliable, resilient, and support the advanced quality of service mechanism with low jitter and delay for high video performance. It will be able to accommodate current traffic needs as well as future growth."

Karsten Oberle, Global Practice Lead for Railway Business at Nokia suggests that when it comes to video surveillance in metro systems, bandwidth, quality of service (QoS), and coverage are vital. When the services of the same network are shared between different uses such as video, voice, location data, dispatching, etc., then it is also necessary for the solution to be able to prioritize traffic according to its importance.

Hardware and VMS

According to Kontron, an embedded solutions provider, hardware platforms and video management software (VMS) that support the ONVIF global standards for the interface of IP-based security products enable advanced capabilities such as video analytics, surveillance, real-time passenger information, and detection systems.

"Implementation of video analytics and other complex functions are anticipated to be very high [popular] amongst public transport organizations in the coming years; however, the integration of these new technologies multiplies the interfaces that operators must manage," Kontron noted in a white paper. "This increased interface complexity may make the efficient management of emergencies more difficult if video surveillance systems are not based on standards-based technologies as there are many analyses and tasks that need to take place simultaneously."

That many of the currently installed systems are based on multiple independent systems that operate over proprietary networks is also a challenge. Implementing ONVIF-supported hardware and VMS solves these issues by ensuring compatibility between them and enabling users to easily identify specific interoperability features.

Video Analytics for Rail Networks

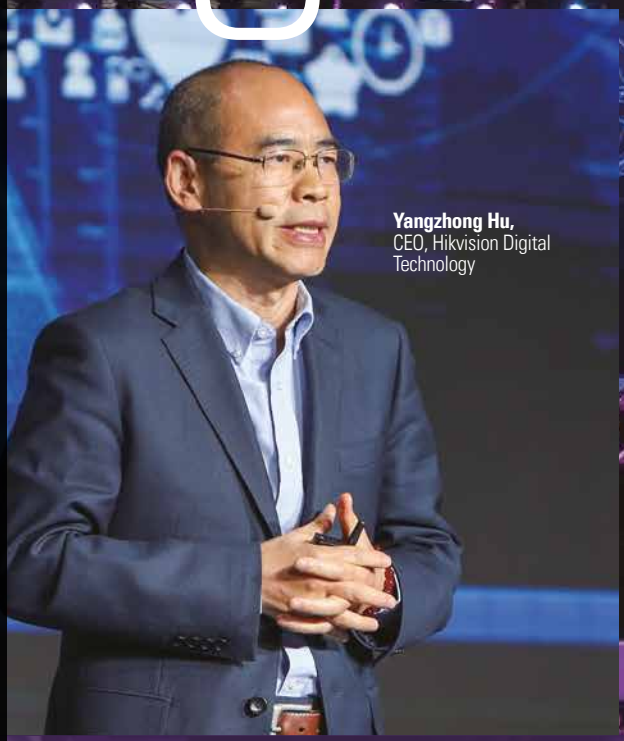
Video analytics are also becoming popular for a variety of purposes in this vertical. An example of this was seen when Siemens Mobility and Strukton Rail decided to join hands and use video analytics and artificial intelligence (AI) to automatically detect and assess the condition of insulated rail joints.

Analytics will also be useful for understanding passenger flows and behavior, enabling rail management to make modifications that would reduce congestion and improve the customer experience. Earlier video analytics used to be limited to the storage level, but now with edge-based solutions becoming popular, analytics can be performed at the camera, allowing for faster processing. A&S

ADVERTORIAL

Hikvision Gro Using AI and

Artificial intelligence (AI) has been gradually changing the way we live and do business. Hikvision Digital Technology, the world's biggest provider of security products and solutions, sees a future of "ubiquitous intelligence," where AI is used everywhere. At Hikvision's AI Cloud World Summit in Hangzhou from March 29–30, the company displayed its ambitions to grow further using AI and big data.



Yangzhong Hu, CEO, Hikvision Digital Technology

by the a&s editorial Team

Big data and business insights generated from AI technology are driving innovation and transforming many industries. AI is truly a game changer. According to PwC's "Global Artificial Intelligence Study," AI "could contribute up to US$15.7 trillion to the global economy in 2030, more than the current output of China and India combined." Hikvision envisions a future where metadata from ubiquitous sensors is analyzed to provide solutions and services for business intelligence and efficiency gains for multiple industries, such as smart cities, transportation, health care, retail, community, manufacturing and homes.

The company's success has relied heavily on its latest AI cloud platform innovations. At Hikvision's AI Cloud World Summit, Hikvision's CEO Yangzhong Hu further emphasized that to fully utilize the power of AI and the internet of things (IoT) for all types of businesses, the fusion of intelligent IoT and information networks was required.

Edge Computing and Fusion with Information Networks Key for AI Cloud

Hikvision's AI cloud can be translated into an integrated architecture of edge nodes, edge domain infrastructure and a cloud center. The edge node can refer to on-premises cameras that collect data from

ows Further Big Data

multidimensional sensors.

The edge domain can refer to intelligent applications for data collection, storage and management. The cloud-based system is utilized for data analytics. The AI cloud is designed to solve real-world challenges across different verticals.

Edge computing will play a more important role in the near future. Hu indicates that the edge node is responsible for front-end data sensing and processing. It can provide a more efficient and economical way of dealing with the collected data. The AI applications will generate a large amount of data. The growth speed of network bandwidth cannot keep up with accelerating growth of IoT data.

"It becomes a norm to process the local data first, and then send the metadata to the cloud for data analysis if necessary. The video cloud service primarily deals with semi-structured data and video clips processed from edge computing instead of continuous videos," Hu explained.

However, only relying on this architecture could still limit the potential of AI. Achieving ubiquitous intelligence in our lives and businesses required the fusion of intelligent IoT and information networks as the foundation, Hu said.

The company's new concept, "AI Cloud Data Fusion Platform," integrates data from cloud centers, information networks and the

edge. In order to get the best out of AI and IoT technologies, intelligent IoT data needs to be organized according to the format of information networks. By combining demand from information networks and intelligent IoT, all of your data can be efficiently managed and organized.

"Without the information network demand, the outcomes from utilizing intelligent IoT would be compromised. We believe that, as a fusion platform, the AI cloud will be able to support our customers in their quest to unleash the full potential of AI and IoT," Hu said. "Ubiquitous intelligence will be the new normal of the AI era; intelligent applications and their data generation will be the engine."

Enabling Collaboration in an AI Cloud Ecosystem

AI is a must for any company wishing to upgrade their capabilities to remain competitive. However, in reality it's hard for a number of companies to acquire such intelligent technology. AI applications are emerging in a scenario-based and fragmented manner. The implementation of AI is restricted by technology bottlenecks on data, algorithms and computing power, as well as product and system levels. Deep learning technology also requires a large amount of data for training. Most companies don't have sufficient high-quality training data and enough AI algorithm engineers.

In light of these barriers, Hikvision has launched an AI algorithm training system. This enables partners to train algorithms easily for specific customer application needs and deployments.

Hikvision also welcomes more partners to collaborate and grow their businesses together using AI and IoT, through the open architecture of its AI cloud platform. The platform is designed to enable collaboration between partners across edge computing,

Hikvision's **AI Cloud** Innovates **Commercial Sector**

Hikvision's AI Cloud has been adopted by many first-tier enterprises in China. At Hikvision's AI Summit, the company's partners in the commercial sector explained how they utilize Hikvision's AI Cloud platform to optimize efficiency and add value to their business.

Dr. Shiliang Pu, Senior VP, Hikvision Digital Technology

AI is seen as a growth engine for innovation in many industries. The retail industry benefits from AI technology that provides business intelligence, such as analysis of customer behavior. Smart technologies help retailers to understand footfall in their stores and optimize their merchandising strategies, as well as improve operational processes. In addition, the store owners can keep their store safe through event search and prediction.

According to a study from Cisco, IP video will account for more than 80 percent of internet traffic by 2022. Videos are commonly used for data analysis in the cloud, as well as for smart retail applications. Surveillance cameras are also widely used for stock taking.

Hikvision's open platform offers all-inclusive service and is equipped with scenario-based AI technology. The company's AI-enabled open platform features an AI algorithm-training system, offering a fast and easy way to deploy AI across different verticals. Dr. Shiliang Pu, Senior VP at Hikvision Digital Technology, said that generally it took a few months for data collection, algorithm training and application deployment, but that with Hikvision's platform this could be completed in less than an hour.

AI Makes Smart Retail More Profitable and Secure

Pu said that Hikvision's AI open platform could be used for inventory management at retail stores. A store owner could upload photos, select products and categories, and choose the online training algorithm model. The training process can be completed in 20 minutes. The store owner could then deploy the trained algorithm on the platform and supported cameras, after which the AI-enabled cameras will be able to check inventory automatically and send reminders when certain products are in short supply.

Hikvision also provides advanced data-analysis services for the retail sector. Its AI-enabled cameras can recognize people and cars, as well as provide other business intelligence for managers to make decisions. Heat mapping can be used to monitor and measure the size of target traffic, in order to find out customers' preferences over time in a specific area. It can also be used to analyze visit times and dwell times. This is especially useful for retail outlets, such as shopping malls and supermarkets. The insights provided allow store managers to intelligently design a store's layout and optimize the placement of products to improve sales.

Aibee, a top AI startup in China, has successfully employed Hikvision's AI solutions in shopping malls. The company utilizes the Hikvision AI Cloud platform in shopping malls at scenic spots, airports, etc. to optimize operational efficiency and reduce labor costs.

Yuanqing Lin, founder and CEO of Aibee sees great growth potential of AI technology for smart retail applications. "The camera can track consumer behaviors like identifying loitering with long-term

industry applications, service platforms and standard systems.

Data Security and Privacy Essential in IoT Applications

As more and more devices become connected and provide vital information, paying close attention to data security and privacy is essential. A report from Gartner said that "Over 20 billion connected things are expected to be in use by 2020. More than 25 percent of identified attacks in enterprises will involve the IoT, although the IoT will account for less than 10 percent of IT security budgets." The increasing number of cyberattacks has had a great impact on the surveillance industry. Such attacks present a security threat to IoT devices. Hu thinks it's essential to protect personal data privacy in accordance with the regulations of different countries, regions or industries. Outside of this, users themselves can also decide the ways in which they share and protect their information.

Hikvision released its "Cybersecurity White Paper" last year and set up internal data security and privacy protection standards. Furthermore, the company has also been an active participant in the Forum of Incident Response and Security Teams (FIRST), an international organization that aims to help companies respond to security incidents more effectively.

Steady Steps into the AI Future

Proliferation of AI technologies is increasing in various industries around the world. However, there is still a long way to go before ubiquitous intelligence is achieved. Hikvision hopes its open AI cloud platform, and efforts on data security and privacy protection will enable more collaborations with partners and further development in the industry.

object tracking. By analyzing the data of incoming rates, the store management can understand in-store and window-shopping customer flows." He said data and analysis provided business intelligence to the shopping center operators.

An operator can understand a customer's journey floor by floor to further analyze and predict their buying behavior. Through this, they can better attract footfall and manage customer flows. "Previously, mall operators designed store layout by product categories. Now, the operators make the layout plan based on customer behavior. With analysis of customer flow data, store managers can optimize the allocation of the workforce to ensure better customer service, and schedule staff strategically for peak and off-peak times."

A well-known retailer has also utilized Hikvision's open platform. The company uses recorded video to inspect daily operations and monitor abnormal events. The representative said, "We can find out how to save time and manpower when it comes to daily operations, so as to optimize operational process. Also, we can analyze and predict abnormal events to find out problems and ensure store security." Instead of analysis of sales data, the company thinks this technology is useful to analyze and predict customer behavior. "We can know when customers come into the store and what they purchase. Also, we can analyze customer behavior [such as] whether they prefer to eat in or take away."

Another retailer also said, "We introduced AI technology to build product recommendation engines, and find out better products for our customers." Moreover, the company has implemented over 500 software automation bots that adopt machine learning technology to do manual and repetitive tasks in areas like accounts, logistics, and transportation, saving an estimated US$30 million a year.

The company said that controlling and preventing unexpected events had been a pain point for the company. To combat this, the company installed surveillance cameras that support facial recognition at entrances to detect malicious and violent persons. "In 2018, we successfully prevented over 1,000 hazardous events."

When AI & IoT Meet the Winemaking Industry

How can AI technologies revolutionize the winemaking industry? Brewers in the Chinese winemaking industry hold thousands of years' worth of wisdom. It takes years to master the art of winemaking, which is regarded as a handicraft industry. With the help of disruptive technology like AI and data visualization from Hikvision, this traditional industry is now being transformed.

Maintaining flawless taste and stable quality has been a major challenge for Chinese winemakers. Understanding market demand has also been another pain point. The makers of Baijiu (literally "white liquor") started to adopt AI and IoT technologies to ensure stable product quality.

Smart video cameras installed in the production line allow managers to check production procedures and wine storage conditions via a smartphone. Previously, quality-control staff had to conduct manual inspections to check for impurities. With AI algorithms and automated visual inspection technology, winemakers can inspect the production process via images and data analysis, reducing failure rate quickly and easily.

Beforehand, brewing techniques were passed down generation by generation, without the help of data digitalization and standardized production processes. Now, the production process is recorded and each bottle of liquor is tagged with a 2D barcode. This allows consumers to better understand the production procedures and ingredients in the wine. With precise sales figures, winemakers can also forecast material preparation and inventory needs better.

Huge Opportunities in Commercial Sector

In the commercial sector, AI and IoT have proven themselves effective in providing business intelligence. However, there are still many pain points, especially in the traditional manufacturing sector, which still awaits experts with more solutions. The commercial market is big and has great potential, but it's also highly fragmented. It requires a very good understanding of systems integration and domain know-how. Hikvision are here to provide an open platform for partners to develop intelligent solutions together for commercial customers. ■

Good Way Enables Smart Homes With Over-the-Top Media Services

At Secutech 2019, Good Way Technology showcased a smart home solution that can be set up quickly using a home's existing entertainment systems.

by John Liu

Good Way's Z-Wave dongle can be plugged into the USB port of high-resolution media players like set-top boxes and TV boxes. The dongle acts as a bridge and can connect up to 253 smart devices, such as light switches, smoke sensors, carbon dioxide sensors, water sensors and motion sensors.

What Good Way provides is an easy-to-set-up solution, with the dongle serving as the control point for all the Z-Wave devices, whether they are made by Good Way or not. "This makes upgrade easier and allows for fuller expansion in the future," said Calvin Lee, VP of Good Way's Smart IoT Business Unit.

The dongle also offers voice control. Users can speak to the TV remote to turn on and off Z-Wave devices. It is worth noting that the remote is not the only voice control media. A smartphone with Google's voice engine built-in can also do the job.

End-users also have the choice of installing wall-mounted panels that can activate between four to six scenes, or turn multiple devices off and on simultaneously.

Good Way is working with telecoms companies that want to offer smart home services. With the dongle inserted into their media hardware, telecoms or cable providers are able to provide Z-Wave-enabled smart home services "without establishing another system on their own," Lee said. "This allows telecoms to quickly enter the smart home market."

This way, telecoms companies can provide subscription-based smart home packages, for energy saving, safety and security, or other purposes, based on customers' preferences.

Good Way also offers the Micro USB Dongle that can be inserted into a smartphone or tablet, so that the phone can serve as a Z-Wave gateway, making it possible to establish a Z-Wave smart home ecosystem.

Z-Wave is one of the most popular wireless protocols in smart homes. One of its main advantages is that its signals will encounter no interference with other protocols like Wi-Fi and Bluetooth.

Occupancy Sensors

Another product showcased at Good Way's booth at Secutech 2019 was its occupancy sensor. Unlike normal infrared motion sensors that detect only large movement, the occupancy sensor can detect small movement. For example, it can detect slight movements of the head or hands even when a person stays mostly motionless in front of a computer.

This is useful in situations where lighting needs to be switched on and off automatically, depending on the presence of a person. Also, the sensor can tell management how many people there are in a room. The air conditioning may therefore be turned up or down accordingly. The automation of lighting and air conditioning helps to save energy.

In this case, the occupancy sensor accomplishes what AI-enabled cameras do. "Users get to know the number of people in a room, but there are no high costs incurred to implement AI," Lee noted.

Commenting on the latest smart home trends, Lee said in the past companies have put emphasis on pursuing technological know-how and specifications. However, big names such as Google, Amazon and Ring are now using voice control to provide better customer service. Their solutions feature low complexity and are "easy to use, easy to install and easy to operate," Lee said, adding that coupled with these companies' new AI engines, smart home was on track to take off soon. ■

Market Update

Italian Security Top 25: Still Growing, but Not Uniformly

The long-awaited "Italian Security Leaders, Top 25" is back, bearing the signature of secsolution magazine in collaboration with Plimsoll Publishing. In 2018, the Italian security market reached US$2.1 billion, driven by 179 companies that improved their performance in 2017 (6.2 percent). This growth, though, affected less than 50 percent of the sample and this could open up new scenarios in the competitive panorama of 2019.

Please note the original monetary value was in euros. This was converted to US dollars based on an exchange rate of 1 euro to $1.11 on May 31.

• **BY** secsolution magazine

Market Update

For the second year running, the security sector in Italy is expanding, with a value of $2.1 billion (as against $2 billion registered 12 months ago). The increase is due not to the number of companies operating in the supply chain (363 compared with the 397 mapped in 2018), but to a general increase in business.

The 363 companies included in the sample have seen a 7.3 percent increase in revenue, continuing a path of expansion that has lasted or six years running, though at lower levels compared with those shown on the balance sheets for 2016 (12 percent) and 2015 (8 percent).

The average company in the sector has a business turnover of $5.7 million, has 93 employees and makes $376,000 in before-tax profit. In other words, for every $111 of revenue, almost $7.8 are created in profit gross of tax. The average profit margins are 8 percent higher than the previous year.

The Italian security sector is therefore on the up, both in terms of aggregate and average revenue and in terms of general profitability. The number of subjects sampled and considered relevant, however, has slightly fallen (-34), as a result of the closure of several companies and the acquisition of others. In conclusion, the sector, taking into account the volumes registered in 2018 and despite the companies exiting the market, has experienced real growth of 6.2 percent.

This phenomenon of market concentration is destined to become more acute over the next few months. 181 companies (50 percent of the sample) have reduced their revenue, and 46 of these are making a loss. In the absence of profound strategic and operative changes, many players in this category may unfortunately not survive until 2020.

As a result of the ongoing technological changes and the largescale operators that are investing heavily in innovation and new marketing channels, it is envisaged that the number of leader companies in the Italian security sector will diminish by a further 20–30 units over the next 12 months.

But some clouds have silver linings. The reduction in the number of leading operators on the market will strengthen those companies that succeed in expanding where others have failed.

Top 25

Key to interpreting the state of health of the sector is an examination of the results achieved by the principal players in the market.

As in previous editions, the Top 25 were selected on the basis of the availability of their 2017 balance sheets in the Chamber of Commerce (as of Nov. 30, 2018) of their core business (relevant to the security sector) and of their having an Italian VAT number. With a collective revenue of around

Top 25 Companies by Revenue

2018 Ranking	2017 Ranking	Company Name	Revenue (US$ million)	Revenue Growth	Sector
1	1	COMELIT GROUP	88.4	6%	Producer
2	3	ALLNET.ITALIA	65.9	19%	Distributor
3	N/A	BETAFENCE ITALIA	61.9	23%	Producer
4	2	NOTIFIER ITALIA	60.4	8%	Producer
5	6	AIKOM TECHNOLOGY	47.3	19%	Distributor
6	8	HIKVISION ITALY	44.9	16%	Producer
7	5	CIMA	40.7	-1%	Producer
8	8	TECNOALARM	39.6	2%	Producer
9	4	HESA	37.0	-10%	Distributor
10	9	PROJECT AUTOMATION	35.3	-8%	Systems Integrator
11	11	BENTEL SECURITY	34.7	-4%	Producer
12	10	SAIMA SICUREZZA	29.6	-20%	Producer
13	17	DAHUA TECHNOLOGY ITALY	28.3	4%	Producer
14	12	INIM ELECTRONICS	27.6	-2%	Producer
15	18	KEYLINE	26.5	12%	Producer
16	13	SELESTA INGEGNERIA	25.9	7%	Producer
17	14	DORMAKABA ITALIA	24.3	-4%	Producer
18	15	GUNNEBO ITALIA	22.1	-5%	Producer/Distributor
19	29	ANIXTER ITALIA	22.0	43%	Distributor
20	25	EL.MO.	21.3	-7%	Producer
21	16	UTC FIRE & SECURITY ITALIA	20.6	-15%	Producer
22	22	VIDEOTEC	20.2	5%	Producer
23	20	ELECTRONIC'S TIME	19.7	-1%	Distributor
24	18	DISTRIBUZIONE APPARECCHIATURE SICUREZZA	19.1	-11%	Distributor
25	21	SICURTEC	18.3	-4%	Distributor
		TOP 25 Average	35.3	3%	
		Average total sample	5.7	7%	

$884.3 million, the Top 25 of the sector now represent 42.4 percent of the total market, an increase of 10 percent compared with last year's figures. This level of concentration, though increasing notably, is still below the average found in countries such as Germany, France and the U.K., where the Top 25 constitute over 50 percent of the national market.

The average dimension of the Top 25 is six times greater than that of the 363 sampled companies. Nevertheless, the fact that the business turnover in the last quintile of the top classification (from the 21st position to the 25th) is equal on average to $19.6 million, means that this category is not inaccessible for new entries during the next year.

In this edition, Anixter Italia Srl (a distributor) has displaced a rival in the Top 25 and is now in 19th position. Entering the Top 10, on the other hand, is Betafence Italia which, with revenues of $62 million, is third in the sector, behind Comelit Group and Allnet.Italia.

The Top 10 represent 24 percent of the market and, with a few exceptions, all 10 have seen growth rates of over 7 percent, while maintaining positive profit margins. The revenue achieved by the group of companies placed tenth to twentieth, though, has remained stationary (from $20.6 to $35.1 million).

The Top 25 averages annual growth rate of around 3 percent, lower than that registered in the three previous years and below the average of the sample of 363 companies in the security sector (7 percent). The average number of employees in the Top 25 has continued to grow (from 83 to 93), while the number in the total sector is stationary (19).

Profit margins for the Top 25 remain positive and have increased slightly, with an EBITDA/Sales ratio reaching 10 percent: an income of $111 is therefore translated into a gross operative result of $11.1. The improved capacity of leading companies to generate significant cash flows will hopefully result in improved investment opportunities for the sector and will facilitate management of seasonal and crisis-related liquidity problems.

Top 25 Companies by Growth

2018 Ranking	2017 Ranking	Company Name	Revenue (US$ million)	Revenue Growth	Sector
1	94	**S.C.A.M.E. SISTEMI**	14.6	78%	Syst Int
2	9	**SMITHS DETECTION ITALIA**	11.9	70%	Producer
3	101	**ANIXTER ITALIA**	22.0	43%	Distributor
4	3	**KSENIA SECURITY**	6.5	30%	Producer
5	8	**FUTURTEC**	16.5	28%	Distributor
6	21	**SECURITY TRUST.IT**	11.3	27%	Syst Int
7	32	**SURVEYE**	7.7	27%	Syst Int
8	28	**TRANS AUDIO VIDEO**	18.2	26%	Distributor
9	69	**BETAFENCE ITALIA**	61.9	23%	Producer
10	99	**MICROCONTROL ELECTRONIC**	6.4	21%	Distributor
11	49	**CO.GEN.**	6.0	20%	Syst Int
12	4	**AIKOM TECHNOLOGY**	47.3	19%	Distributor
13	11	**ALLNET.ITALIA**	65.9	19%	Distributor
14	5	**HIKVISION ITALY**	44.9	16%	Producer
15	57	**SAIET TELECOMUNICAZIONI**	9.4	16%	Syst Int
16	13	**ADVANTEC**	12.8	16%	Syst Int
17	77	**BOSCH SECURITY SYSTEMS**	16.7	13%	Producer
18	64	**MICRONTEL SOCIETA' PER AZIONI**	6.1	13%	Producer
19	62	**CIAS ELETTRONICA**	6.9	13%	Producer
20	81	**BETTINI**	9.3	13%	Pro/Distr
21	40	**KEYLINE**	26.5	12%	Producer
22	83	**ELMAT**	18.3	11%	Distributor
23	68	**CIODUE**	12.7	10%	Producer
24	35	**ZUCCHETTI AXESS**	16.3	9%	Producer
25	12	**OMEGA**	6.5	8%	Distributor
		TOP 25 Average by Growth	19.3	23%	
		Average Total Sample	5.7	7%	

The Best in the Sector

This edition on Italian security leaders must start with an analysis of the companies that obtained the best results in 2017. The 25 companies classified as the "best in the sector" are those which have grown significantly, strengthening their financial solidity and achieving particularly high returns on their investments and equity.

The Top 25 "best of the sector" grew by 16 percent, enjoyed an average ROI of 9 percent, an ROE of 17 percent and are classified by ratings agency Plimsoll as financially "solid" or "good." In reality, the sample is extremely varied and includes subjects such as Vitekna Distribuzione Srl (with a modest growth of 2 percent, but with profit margins

in double figures) and operators such as Surveye Srl (which has expanded its revenue by more than a quarter, but which has an EBITDA/sales ratio in line with the average for the sector). Nevertheless, it is these companies that should be closely monitored over the next year. By adopting strategies that are not always conventional and by offering a different portfolio of products and services, in fact, the "best of the sector" dictate trends and influence — more or less significantly — competitive dynamics and the consumer habits of the end user.

It is easy to understand, by examining the results shown in the table, the market positioning each operator is achieving. Betafence Italia has undertaken a strongly expansive path aimed at increasing its market share, with reduced focus on returns. Producers such as Cooper Csa Srl, Tecnosicurezza Srl and Urmet Ate Srl, on the other hand, are subjects in good health, commercially dynamic, but above all with high profitability and efficient operative structures.

Companies With the Biggest Growth

The list of the Top 25 subjects in the security sector that have grown most rapidly has changed significantly over the last 12 months, as might reasonably have been expected. To maintain growth levels of over 10 percent for two years running is, in fact, a goal that few are able to achieve, especially when certain company dimensions have been reached.

The obstacles to be overcome in order to sustain growth in the double figures over time are of various natures: loss of the novelty effect, price wars with local or national competitors, difficulties met when attempting to expand in geographical markets unexplored but already occupied, problems obtaining the necessary resources (in terms of personnel, warehousing and machinery) with which to handle increased orders, finding the necessary skills to make suitable investments in order to finance ongoing operations.

Just how difficult it is to maintain impetus in the sector, is demonstrated by the fact that only nine companies listed in the previous publication have remained in the Top 25 for growth. Smiths Detection Italia Srl, Ksenia Security Srl and Futurtec Srl are tangible examples of organizations that have faced the aforementioned difficulties with extreme success. They have grown by over 25 percent for the second year running.

Growth is not always accompanied by high profit margins. In some cases, expansion in the market has been dictated by a strategy aimed at grasping larger market shares in the short term and gathering the fruit (i.e. the financial return) in the medium/long term. Not infrequently do we find companies in the

Top 25 Companies by EBITDA Sales Margin

Company Name	Revenue (US$ million)	Revenue Growth	EBITDA Sales Margin	Sector
CONSIAG	6.9	-41%	61%	Systems Integrator
INIM ELECTRONICS	27.6	-2%	36%	Producer
PILOMAT	10.0	3%	34%	Producer
TECNOALARM	39.6	2%	29%	Producer
VENITEM	8.5	-11%	27%	Producer
ZUCCHETTI AXESS	16.3	9%	26%	Producer
COMBIVOX - SOCIETA' A RESPONSABILITA' LIMITATA	9.5	-2%	23%	Producer
SELESTA INGEGNERIA	25.9	7%	22%	Producer
MICRONTEL SOCIETA' PER AZIONI	6.1	13%	22%	Producer
AVS ELECTRONICS	10.7	-8%	22%	Producer
CIMA	40.7	-1%	21%	Producer
S.C.A.M.E. SISTEMI	14.6	78%	21%	Systems Integrator
KSENIA SECURITY	6.5	30%	20%	Producer
COMELIT GROUP	88.4	6%	18%	Producer
NOTIFIER ITALIA	60.4	8%	18%	Producer
SERTEC	6.4	0%	16%	Distributor
BENTEL SECURITY	34.7	-4%	16%	Producer
SENSITRON	7.9	-1%	16%	Producer
GIUDICI & POLIDORI	9.1	-2%	12%	Distributor
VAGO	8.2	1%	11%	Systems Integrator
CIAS ELETTRONICA	6.9	13%	11%	Producer
VITEKNA DISTRIBUZIONE	5.6	2%	11%	Distributor
SICEP	8.1	0%	11%	Producer
SECURITY TRUST.IT	11.3	27%	10%	Systems Integrator
LINCE ITALIA	6.6	-6%	10%	Producer
TOP 25 Average	19.1			
Average Total Sample	5.7			

security sector showing strong growth but poor profitability, thereby proving the intrinsic difficulty of aligning their organizational processes with the increased business volumes. Among the Top 25 companies in this category, no fewer than 12 have an EBITDA/Sales ratio below the sector average (5 percent). The others are all in a positive zone, with four of them exceeding 20 percent.

In conclusion, the analysis of the Top 25 by growth shows that the security sector is not lacking in opportunities for development for those adopting farsighted decisions and using their available resources efficiently. Increasing sales in 2017 has not been easy for everyone (let us remember that 50 percent of the leaders in the sector have reported diminished revenue). Remaining at the top for the second year running has been harder still (only 9 subjects have kept their place in the Top 25 by growth).

Producers

With an aggregate revenue of $1.1 billion, producers represent almost 50 percent of the security sector in Italy. They occupy the first positions in the classification of the largest companies and dictate the growth rhythms of the sector. The classification of the Top 25 producers in this edition shows interesting changes with respect to the previous year. There have been a few alternations among the first positions (with Betafence leaping to second place and Hikvision Italy to fourth), as well as the entry of Dahua Technology Italy Srl (which has absorbed Videotrend), Keyline Spa (with a growth of 12 percent) and Smiths Detection Italia Srl (with revenue up by 70 percent) in the list of principal security producers in Italy.

Going into greater detail and examining the results by product category, particularly positive results emerge in the fire prevention and video surveillance sectors, and a small amount of growth (1.7 percent) in the anti-intruder category (with two producers out of three reporting lower sales).

Producer/Distributor

Maintaining the same categorization adopted in the previous edition, we have classified eight subjects as producers/distributors. These are companies that make parts and also act as distributors on behalf of other producers. The companies identified all have their registered offices in Lombardy and Piedmont. They generate an overall revenue of $73.7 million, but are struggling to grow. Five out of eight have reported diminished sales by over 5 percent, the second consecutive year of contraction for four of them.

Distributors

The distributors active in the security sector have an aggregate revenue of $662.5 million. They represent 32 percent of the total market and have 1,521 employees in Italy. In this edition, the 141 companies belonging to this category grew by 12 percent and are continuing the strongly expansive path already registered the previous year (31 percent).

Systems Integrators

The total business of the 81 systems integrators analyzed in this edition amounts to 14.5 percent of the Italian security sector. With an average revenue of just over $5.6 million and a negative growth rate (-0.5 percent), this category seems to have taken a step backwards compared with last year. Their trading problems seem, in reality, to affect mainly small/medium subjects operating in provincial contexts. The largest companies (the Top 25), on the other hand, are growing steadily (6 percent) and are maintaining good profitability levels. 14 companies out of 25 have increased their revenue and only two are working at a loss.

Geographical Distribution

Forty-six percent of the leading companies in the Italian security sector have their registered offices in the North-West (chiefly Lombardy and Piedmont) and contribute 51.3 percent of the total market revenue. With a strong presence of producers and a company mortality rate of 3.4 percent, the companies in this geographical area are growing by an average of 4 percent and maintain average profit margin levels above 9 percent.

With an aggregate revenue of $379.2 million, the surveyed companies from central Italy have grown by 4 percent, maintaining the excellent income results registered in 2018 (Ebitda/Sales at almost 11 percent). They now represent over 18 percent of the total market (compared with the modest 15 percent observed at the last data collection).

More complex and disturbing is the situation in Southern Italy, where the number of subjects active in the sector has fallen to 32 (from 39 observed in 2018). With average dimensions of $3.9 million and a strong presence of distributors on the territory, the Southern companies are a minus point in this edition.

Conclusions

The data observed and the analysis made in this edition of Italian Security Leaders, Top 25, show that the security sector grew by 6.2 percent in 2017, reaching market dimensions of $2.1 billion. The number

of Italian enterprises currently mapped has fallen to 363 (from 397 in the previous survey) and a slight strengthening has been observed in terms of the profitability levels and average financial solidity in the sector. This is in line with trends towards consolidation noted in other similar industries in Italy and abroad. The leading security companies in Italy are now on average larger than last year ($5.7 million), more productive ($296,000 revenue per employee) and more profitable (EBITDA/Sales equal to 5 percent as against 3 percent the previous year).

Among the segments expanding particularly strongly, those for distributors (12.2 percent) and of producers of video surveillance devices (10.9 percent) and fire prevention equipment (10.6 percent) are to be noted. The number of distributors active in Italy, moreover, runs against the general trend for the sector (10 compared with the previous survey), testifying to the interesting development opportunities existing in this sector. Nevertheless, the growth observed in the security sector this year is not uniform and concerns only 50 percent of the companies sampled. Eighty-four companies (23 percent of the total) saw declining revenue for the second year running and deteriorating levels of financial solidity

The segments most affected by declining growth are those of systems integrators (-0.5 percent), producers/distributors (-1.3 percent) and enterprises in Southern Italy (-0.5 percent and in sharp numerical decline).

The security sector seems, therefore, to have set in motion for the next 24 months a further reduction in active enterprises and a greater polarization between companies that are financially solid and growing and those that are struggling to remain in the market. It is not unlikely that, as in the past, further mergers and acquisitions will take place over the next few months, with the goal of strengthening synergies and competitiveness and optimizing investments.

With new players and technologies on the threshold, the security industry in Italy is heading for major changes over the next five years. Innovation, strategic alliances, understanding of market trends and wise management of resources are all factors that will determine the success or the decline of the 363 security leaders. a&s

Top 25 Producers (Manufacturers)

2018 Classification	2017 Classification	Company Name	Region	Revenue (US$ million)	Revenue Growth	Sector
1	1	COMELIT GROUP	Lombardia	88.4	6%	Various
2	N/A	BETAFENCE ITALIA	Abruzzo	61.9	23%	Physical security
3	2	NOTIFIER ITALIA	Lombardia	60.4	8%	Fire-fighting
4	5	HIKVISION ITALY	Lombardia	44.9	16%	CCTV
5	3	CIMA	Emilia-Romagna	40.7	-1%	Physical security
6	4	TECNOALARM	Piemonte	39.6	2%	Anti-intrusion
7	7	BENTEL SECURITY	Abruzzo	34.7	-4%	Anti-intrusion
8	6	SAIMA SICUREZZA	Toscana	29.6	-20%	Physical security
9	N/A	DAHUA TECHNOLOGY ITALY	Lombardia	28.3	4%	CCTV
10	8	INIM ELECTRONICS	Marche	27.6	-2%	Anti-intrusion
11	N/A	KEYLINE	Veneto	26.5	12%	Physical security
12	9	SELESTA INGEGNERIA	Liguria	25.9	7%	Physical security
13	N/A	DORMAKABA ITALIA	Lombardia	24.3	-4%	Physical security
14	11	EL.MO.	Veneto	21.3	-7%	Various
15	10	UTC FIRE & SECURITY ITALIA	Lombardia	20.6	-15%	Various
16	13	VIDEOTEC	Veneto	20.2	5%	CCTV
17	16	BOSCH SECURITY SYSTEMS	Lombardia	16.7	13%	Various
18	14	ZUCCHETTI AXESS	Lombardia	16.3	9%	Access Control
19	15	COOPER CSA	Lombardia	15.4	5%	Anti-intrusion
20	12	ATRAL ITALIA	Emilia-Romagna	14.9	-25%	Anti-intrusion
21	20	TECHNOMAX	Lombardia	14.1	6%	Physical security
22	17	CESPRO	Toscana	13.2	-9%	Physical security
23	22	CIODUE	Lombardia	12.7	10%	Fire-fighting
24	18	COMETA	Toscana	12.3	-10%	Physical security
25	38	SMITHS DETECTION ITALIA	Lombardia	11.9	70%	Fire-fighting
		TOP 25 Average		28.9	4%	
		Total Average		5.7	7%	

ADRIA SECURITY SUMMIT

powered by intersec

CONFERENCE & EXHIBITION

Date: 18 – 19. 09. 2019.

Country: North Macedonia

Venue: Hotel Aleksandar Palace, Skopje

Save the Date

1,500+
PARTICIPANTS

70+
EXHIBITORS

15+
WORKSHOPS

6
SPEAKERS

12
CASE STUDIES

Adria Security Summit Powered by Intersec is a unique annual corporate conference and exhibition event dedicated to the regional security industry. It is distinguished by its top quality level of organization, selection of renowned speakers, presentation of the leading global companies and the largest recorded number of visitors for the events of this type. Its truly regional character is confirmed by the support it receives from each of regional professional associations, diversity of visitors and rotating venues.

CONTACT US: Phone: +387 33 788 985; E-mail: summit@asadria.com

www.adriasecuritysummit.com

How **Machine Vision** Powers **Manufacturing**

Machine vision in industrial environments works like an advanced version of the human eye, spotting defects and details on production lines or for logistics.

• **BY** Elvina Yang, Freelancer

Machine vision can read barcodes on objects, flag wrong colors on packaging, and discover tiny defects that humans may have difficulty seeing.

With the help of machine learning, machine vision can fill an even greater role in Industry 4.0 factories, performing predictive maintenance, starting in-truck processing for shipping and allowing humans and robots to mingle in the same areas without creating safety hazards.

Machine Vision is Replacing the Human Eye in Industry 4.0

Machine vision has supplanted the human eye in Industry 4.0, reading barcodes, detecting tiny defects, and recognizing visual information in even the darkest of conditions.

Traditionally, a person was required to physically stand and supervise a machine and its procedures. At a logistics warehouse, this meant employees would need to check the label of packages and put them in the right locations manually. Nowadays, all these tasks can be automated using machine vision.

Jerome Gigot, Senior Director, Marketing, Ambarella

"Machine vision can be characterized as capturing visual data from the environment, interpreting it to make sense of if, and deciding what actions to take," said Jerome Gigot, Senior Director of Marketing at Ambarella.

"This is conceptually similar to human vision — the eye captures visual data from the environment, the brain interprets it, and finally the brain decides whether to act on it."

Machine vision systems, particularly those using cameras linked to multiple edge computing servers located inside a factory, can be used to automate certain industrial processes. This includes routine inspections, quality assurance, process control, predictive maintenance, safety inspections, inventory management and barcode reading.

The Mechanics of Machine Vision

Basic components of a machine vision system include a processor, a camera and a camera interface to digitize images. With the help with other components, such as light sources, lenses, image processing software, object-detection sensors

and input/output hardware, a machine vision system is complete.

"In a machine vision system, the sensor subsystem is the 'eye,'" said Gigot.

This "eye" consists of a lens to focus the light on the image sensor, and an image sensor converts this light into digital data, or "pixels," which presents different colors and luminance data.

Some machine vision applications, such as barcode scanning, use only black and white images, since color information is not required to make an intelligent judgement for these types of functions. In some other cases, such as identifying paint defects, color information is critical.

Previously, digital images collected by machine vision systems were sent back to a PC or an FPGA (field programmable gate arrays) back-end system for analysis. By placing this video processing capability directly into the camera, the time taken to identify images is reduced, speeding up the whole production process.

"With the latest advances in chip technology and the advent of dedicated silicon to process vision data — such as the latest series of Ambarella CVflow system-on-chips (SoCs) — this processing can be done in the camera itself, right next to the sensor," said Gigot.

Meaningful Machine Vision Requires Video Data

The first step a machine vision system will take to understand images collected by cameras is to adjust these images through processes such as sharpening, cutting or zooming. This processing provides meaningful information for computers to read.

As humans, we have a set of eyes capturing images, which then are sent to the brain for image identification. For machines, cameras and other visual sensors perform the function of the eyes, with software, artificial intelligence, FPGA (field programmable gate arrays) chips, CPUs and GPUs filling in for the brain.

Lian Jye Su, Principal Analyst, ABI Research

"Image processing can be seen as the first step in analyzing video data, before it is fed to the system's computer vision algorithms," said Jerome Gigot, Senior Director of Marketing at Ambarella.

Processing software can sharpen an image to improve readability, change the exposure for a clearer shot, or zoom in and crop certain information, such as a barcode or address located on a package.

"The type of data that will be analyzed heavily depends on the manufacturing function that needs to be performed," said Gigot.

Industrial objects, for instance, can be inspected by size, shape, color and texture. These same variables can be also used to recognize agricultural or biological objects.

The second step is to have an algorithm that first distinguishes between the many different pieces of an image, then identifies the edges and models its subcomponents.

In manufacturing, computer vision isn't limited to a single niche purpose. Some decode barcodes, while others inspect for defects. The latter is powered by neural networks that can compare how a piece of equipment looks versus how it is supposed to look. When the algorithm finds an anomaly, it flags the issue for the user. Other possibilities include monitoring, predictive maintenance, safety inspection and inventory management.

Gigot offers the example of food processing. At a food processing plant, a neural network detects and instructs the system to remove bad apples in real time as they speed through the scanner and before they shipped out to stores.

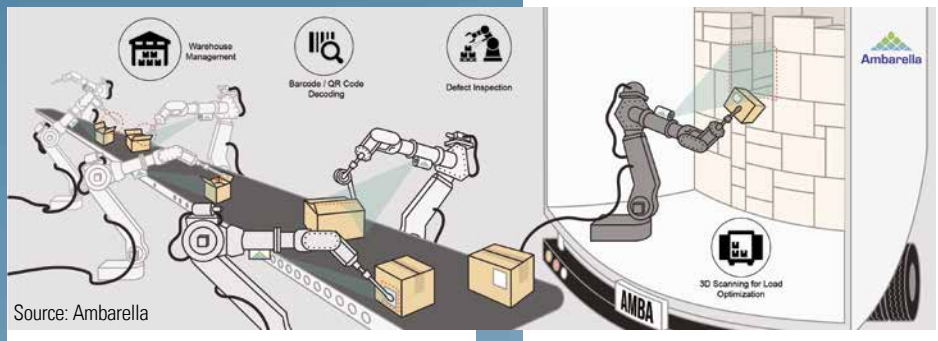
Seeing Beyond Vision With Predictive Capacity

"In addition to cameras, machine learning-based machine vision can also incorporate data collected from various sensors, including LiDAR, radar, ultrasound, and magnetic field sensors. The rich set of data will provide further insight into other aspects of production processes," said Lian Jye Su, Principal Analyst at ABI Research.

Conventional machine vision only detects product defects and quality issues predefined by humans. With the help of machine learning algorithms, machine vision can pick up unexpected product abnormalities or defects, providing flexibility and valuable insights for manufacturers.

Machine vision-powered predictive maintenance utilizes machine learning, and other connected devices to monitor data and components in order to taking corrective actions before machinery breaks down. It creates a zero-downtime situation for manufacturers, creating cost savings.

Another use of machine learning-equipped machine vision systems is for monitoring worker safety. Devices can track people and predict the movement of equipment, helping to prevent dangerous interactions between people and machines.



Source: Ambarella

Unleashing the Potential of Industry 4.0 With Machine Vision

Machine vision can do more than just read barcodes or find defects on the production line.

Machine vision can read text, organize in-trucking for logistics and allow humans and robots to work and interact safely in the same areas.

Traditionally, machine vision in manufacturing was used for tasks like barcode reading and defect detection. However,"with the advent of technologically-advanced, low-power machine vision chips, new use cases are appearing in the manufacturing area," said Jerome Gigot, Senior Director of Marketing at Ambarella.

Warehouse management, Gigot said, was a great example of where the latest machine vision technologies were being used to enhance operational efficiency and safety, as well as ensure manufacturing quality control.

Previously, a barcode reader scanned a package, then a human worker or robot used the collected data to carry the package between different points within the warehouse or to a loading area.

"Both methods have limitations," said Gigot. "Due to safety concerns, robots do not typically roam in the same area as humans — 'robot zones' and 'human zones' tend to be separate."

With the latest progresses in machine vision, robots powered by 3D vision and neural network processing are able to move around freely and safely in the same work areas as humans. Such systems can distinguish a person from an inanimate object, as well as take actions to maintain safe distances and avoid collisions.

"Collaborative robot and autonomous mobile robots on the factory floor now have machine vision capabilities to help them identify objects and obstacles, pick up objects and help them to navigate in unstructured environment," said Lian Jye Su, Principal Analyst at ABI Research.

"Ultimately, manufacturers will benefit from either or [both of] these solutions as they can push carts and deliver parts within or between the factories, optimizing workflows, minimizing workplace hazards, and freeing up valuable staff resources," said Su.

Gigot offers the example of machine vision robots loading packages inside a truck. "With the latest advances in machine vision, a robot will be able to perform a 3D scan of the inside of a shipping truck, and then decide on the optimal placement for each package."

Such robots are able to scan packages that are already in the truck, and find and decrypt barcodes. It can then decide whether to organize packages by final destination or to load-balance the vehicle.

More Possibilities

Other areas, such as product and component assembly, can also be enhanced using machine vision.

The ultimate goal of manufacturing is to ensure products and components coming from the production line meet quality, safety and production guidelines. For packaging operations, machine vision can provide a 360-degree view to make sure products are placed in the right position for packaging in terms of cap closure, position, label and print quality.

Outwith barcodes or a GTIN (Global Trade Item Number), a packaged product often has descriptive text on it. When this printed text can be read by machines, the system can further check against a database to ensure the printed labels are valid. If the product code doesn't match with the text, the package will be rejected on the production line.

"The increasing number of stock keeping units (SKUs) and short product life cycles necessitate the deployment of industrial solutions that can be automate and augment different manufacturing processes. As such, one of the most important elements in the factory floor is to be able to recognize objects, something that only humans could do well until machine vision became more advanced," said Su.

Machine Vision Market Goes to the Next Level

Edge-computing, costs considerations and machine learning will influence the development of machine vision in the next five years.

Beyond edge computing, costs and machine learning, big data processing and yield analytics will also play a key role in the development of machine vision.

Machine vision in manufacturing "will continue to be [focused on] quality control and automation, areas that are well established by traditional industrial machine vision player and techniques, and that will be further supported by machine learning-based machine vision innovation," said Lian Jye Su, Principal Analyst at ABI Research.

Besides cameras, machine learning-based machine vision incorporates data collected from various sensors, including LiDAR, radar, ultrasound and magnetic field sensors. This rich set of data then provides further insights into other aspects of the production process.

"As compared to conventional machine vision which can only detect product defects and quality issues which can be defined by humans, machine learning algorithms deployed for machine vision can go even further," said Su.

"These algorithms can pick up unexpected product abnormalities or defects, providing flexibility and valuable insights to manufacturers."

Some startups are also working on extending the power of machine vision to other applications in manufacturing. Su mentioned names like Instrumental and Landing.ai. These firms have developed products that leverage image data collected from cameras to venture into other smart manufacturing services, such as big data processing, process optimization and yield analytics.

Frank Lamb, Founder, Automation Consulting

The Next Stage in Machine Vision

As machine vision technology advances, costs could also come down. "As costs decrease, cameras or pixel arrays are finding their way into places where analog and discrete sensors used to be," said Frank Lamb, the founder of Automation Consulting.

"As Industrial IoT (IIoT) becomes more widespread, I see smaller pixel arrays being used for more custom applications to save money. This is in opposition to buying packaged systems for major vision vendors," said Lamb.

Ambarella, a computer vision semiconductor design company, expects the next key technology in machine vision to be edge computing.

Current machine vision systems use PCs for processing. This is suitable for situations such as sites with a fixed assembly line where the main function of the camera system is to scan packages zipping by. However, if the camera can process the data itself, rather than streaming the video to another device for analysis, it could bring another level of mobility to the warehouse, such as warehouse robots or mobile scanning systems.

"We believe that the new generation of technologically-advanced, low-power computer vision chips — capable of performing machine vision at the edge — will increase intelligence in mobile robots and scanners, enable use cases that were not possible before, and improve efficiencies in manufacturing workflow," said Jerome Gigot, Senior Director of Marketing at Ambarella.

"In the next five years, the machine vision market will move towards AI- (artificial intelligence) based technologies," said Su.

More cameras could be deployed for urban infrastructure purposes, and on commercial and consumer vehicles and robots, to enable automation and augmentation of work processes, Su suggested. Machine vision may also be seen in smart cities, automotive and mapping, logistics and warehousing.

Don't Forget Customer Education

"Educating customers on what machine vision can and can't do, and how to maintain their systems, is a challenge," said Lamb. "People tend to think you can install a system and it will solve all of their problems and work 100 percent of the time. This is simply not true."

For an existing factories, how to embrace Industry 4.0 and the latest machine vision technologies — including accommodating automation systems and data exchanges from the internet of things (IoT) — will also be a challenge.

"If the customer isn't willing to learn how the system works before it is installed and, and isn't willing to invest in maintaining and adjusting when necessary, the application will not be successful," said Lamb.

VIDEO SURVEILLANCE

Axis Communications

AXIS P1375 AND AXIS P1375-E NETWORK CAMERAS

www.axis.com

These new indoor and outdoor network cameras offer 2-megapixel video quality, as well as signed firmware and secure boot and Lightfinder 2.0 technology, which significantly improves colors and low-light performance. Supporting H.264 and H.265, storage requirements and bandwidth are significantly lowered by 50 percent or more.

- HDTV 1080p at up to 60 fps
- Lightfinder 2.0 and Forensic wide dynamic range (WDR)
- Zipstream with support for H.264 and H.265
- Electronic image stabilization
- Barrel distortion correction and defogging functionality
- Scene profiles and corridor format

Bosch Security Systems

FLEXIDOME IP STARLIGHT 8000I CAMERA

www.boschsecurity.com

This camera features intelligent dynamic noise reduction and intelligent streaming combined with H.265 video compression. This can reduce bitrate by up to 80 percent, substantially reducing network strain and storage costs. With Starlight technology, the camera can capture high-definition images in extreme low-light situations.

- IP66 water resistance, IK10+ vandal resistance and anti-corrosion coating
- Operating range of minus 50 to 60 Celsius
- Supports 6 megapixel HD 1080p, or the 4K Ultra HD resolutions with frame rates up to 60 fps
- Built-in intelligent video analytics

FLIR

SAROS DH-390 DOME

www.flir.com

This camera can deliver wide-area monitoring regardless of unfavorable lighting or weather conditions. With IR and visible LED illuminators, the camera can deter intruders with white light illumination. Moreover, it supports advanced accurate target detection and classification to help reduce false alarms.

- Multiple FLIR Lepton thermal sensors
- 1080p or 4K HD resolution to realize accurate visual identification of intruders
- IR and visible LED illuminators
- Advanced onboard analytics
- Two-way audio and digital input/outputs

Hikvision Digital Technology

4MP DARKFIGHTERX CAMERA

www.hikvision.com

Hikvision's 4MP Network IR PTZ Camera features DarkFighter technology that uses one lens to capture the color of objects, and another captures light details. The camera can deliver full-color images at 0.0005 Lux light level. It's also equipped with an auto wiper and a rain-detecting sensor.

- Up to 35x zoom and 16x optical zoom
- 120 dB WDR, 3D DNR, chromatic defog
- Supports H.265+/H.265 video compression
- Rapid focus
- Up to 250 meter IR distance with Smart IR
- IP67 rated

Hanwha Techwin

WISENET T SERIES RADIOMETRIC THERMAL CAMERAS

www.hanwha-security.com

This camera features temperature measurement to monitor incidents. Equipped with a 35/19/13 millimeter lens, the camera can detect vehicles up to 3 kilometers away. It uses a hybrid color palette, and temperatures out of the defined range are expressed in white hot color or in black and white.

- Operating temperature: -20 to 130 Celsius
- Built-in gyro sensors to offer accurate stabilization
- IP66 and IK10 rating weather protection
- H.265, H.264 or MJPEG compression
- WiseStream II complementary compression technology to improve bandwidth efficiency

AETEK

A5020-E EPOC CAMERA HOUSING

www.aetektec.com

A5020-E is a long range EPoC (Ethernet and power over coax) camera housing with IR illuminator specially designed to accommodate today's indoor PoE IP box/brick style camera reaching 500m & keeping 25W PoE budget remotely. It allows IR illuminator, heater, blower, and multibrands of PoE IP box/brick camera to be powered over single RG6/RG59/RG11 coaxial cable.

- Aluminum die cast body
- Powered by EPoC
- Spacious dimensions for camera equipped with long varifocal lens
- Window heater for demisting & deicing
- Adjustable sunshield

Avigilon

ACC 7 VMS

www.avigilon.com

Avigilon's ACC 7 video management software includes Focus of Attention that uses artificial intelligence (AI)-powered Avigilon self-learning video analytics and unusual-motion detection technologies to determine what information is important and should be presented to security operators. It also features an optional dark theme for low-light environments.

- Features the Focus of Attention user interface for live video monitoring
- AI-powered self-learning video analytics
- Unusual-motion detection
- Provides actionable information immediately to users
- Optional dark theme for low-light environments
- ONVIF Profile T compliant

Dahua Technology

NVR4000-I SERIES

www.dahuasecurity.com

Dahua's AI NVR Series integrates perimeter protection and facial recognition. Its face recognition technology offers real-time facial analysis by identifying, capturing and recording faces with metadata. It supports configurable multiple face database, as well as common and stranger mode to sound an alarm when encountering suspects on the blacklist.

- Analyzes targets based on deep learning algorithms to differentiate people and vehicles
- Artificial intelligence (AI)-powered face recognition technology, real-time facial analysis
- Configurable multiple face database, common and stranger mode
- Multichannels that can search for a person of interest
- Supports ePoE and EoC

Coretronic Intelligence Robotics

INTELLIGENT AUTONOMOUS SECURITY FLYING ROBOTICS

www.coretronic.com

Coretronic's intelligent self-controlled drone features artificial intelligence (AI), providing automatic inspection, threat response and live monitoring. The system is equipped with high-speed computing and an induction control platform to achieve fully automatic flight, precision landing and automatic charging operations.

- Autonomous takeoff, patrol, landing and recharging, and collision avoidance
- Real-time video analysis, recognition and tracking
- Multicamera module with optical zoom x10/thermal lenses
- Propulsion system redundancy for safe RTL
- Safe and robust design.
- Weatherproof with IP54 protection and Beaufort scale- 6 wind resistance

ACCESS CONTROL

HomeScenario

HBT-300 INTERCOM

www.homescenario.com

The HBT-300 is a smart building intercom station which combines the functions of an SIP/IP intercom with alarms, access control systems, video monitoring, and smart home control. It is compatible with Android and multiple apps can be added to expand functionality. The HBT-300 is elegantly designed and made from high-quality materials, making it a perfect fit for luxury buildings.

- 10.1-inch HD quality display Android system
- Aluminum frame with tempered glass front panel
- Supports IP intercom, alarm system, access control, video surveillance, etc.
- Also works as smart home controller
- Supports cloud-based SIP intercom

Fermax

MARINE ELITE OUTDOOR PANEL

www.fermax.com

MARINE ELITE is a customizable vandal-proof outdoor panel. The designers can design a specific marking for the building or home according to the project. The marking of the audio and video door-entry panels, like address indicators and name of the building, is done by laser engraving.

- Available with push buttons or keypad, camera, display
- Surface box in the chosen color
- Elements can be arranged vertically or horizontally
- 2.5-millimeter thick stainless steel panels
- Laser engraving of addresses and building names

Open Options

DNA FUSION

www.ooaccess.com

DNA Fusion is designed for enterprises looking to take full advantage of the distributed network architecture model. It removes many of the limitations to enterprise deployment inherent in typical access control applications. DNA Fusion allows you to monitor several systems through a common interface, including audio and IP video recording.

- Quick results on personnel, access, door status, and event history
- Integration with all major brands of wireless, Wi-Fi, and PoE locks
- Quick reporting with trace history
- Drag and drop throughout
- Simple sharing of personnel data

Hundure Technology

PXR-92MWS-BE BLUETOOTH READER

www.hundure.com

The reader supports multiple interfaces. The user can use a BLE-enabled smartphone to unlock the door or as a remote controller with a mobile app. It also supports Mifare Card, Wiegand and RS-485. Certified by IP65, the product is suitable for indoor and outdoor environments.

- Supports Mifare Card
- A smartphone can be used to unlock door via Bluetooth (BLE)
- Dual interface: Wiegand and RS-485
- IP65-rated ingress protection
- Wide operation temperature range.

LIH CHERN METALLIC Enterprise (LCM)

SMART DOOR LOCK

www.lavo.tw

LCM's smart door lock allows users to open the door via fingerprint or password. The lock can also remotely open the door via a mobile app and ZigBee gateway. The lock features a sturdy and elegant look, and is made of full zinc alloy die-casting and stainless steel.

- Supports ZigBee wireless technology
- Remotely opens or closes door lock via an app
- Entry mode: fingerprint, password, key
- IP56 water/dust proof
- Time limit unlock for fingerprint and user password

Tapplock

TAPPLOCK ONE+

tapplock.com

Tapplock's smart fingerprint padlocks identify users with over 99-percent accuracy and unlocks in 0.8 seconds. It allows users to gain access via their fingerprints and can also be opened using Morse code or Bluetooth. It features proprietary 128-bit encryption with security protocols for enhanced protection.

- Stores up to 500 fingerprints per lock
- Anti-shim and anti-pry, IP67 waterproof rating
- Views locks, deploys and revokes fingerprints remotely and set access privileges
- Manage users, locks and access history using Tapplock's app and software
- Sets custom lock permissions for users and manage them via groups
- Sends mobile notifications for account related events and exports audit reports

LIPS

LIPSFACE AC770

www.lips-hci.com

IPSFace AC770 is LIPS's 3D facial recognition system based on biometric authentication with advanced 3D vision anti-spoofing powered by powered by Intel RealSense Technology. It's ideal for applications that require ultra-fast and a contactless authentication experience, such as offices, stations, airports, banks and financial institutes.

- Instant facial recognition with less than 0.3 second recognition time
- Deep learning face features — 99.6 percent LFW (Labeled Faces in the Wild) score
- LIPS adaptive AI deep Learning algorithm is included
- Scalable up to 20K enterprise level database, including multi-pictures of each person

ProdataKey

TOUCH IO

www.prodatakey.com

With the ProdataKey touch io Bluetooth reader, users do not need to unlock a phone, or to remove it from a pocket or purse in order to gain access through a door. A unique ID is randomly-generated and authenticated by the Bluetooth reader at each use.

- Issues mobile credentials in seconds using an email address
- An unlimited number of mobile credentials per reader
- Operating distance as far as 30 feet away, as defined by the customer
- Compatible with legacy systems, capable of reading traditional proximity cards

AUTOMATION & CONTROL

ADT

COMMAND CONTROL PANEL

www.adt.com

This panel can create dynamic scenes and rules. In case of a fire, the system can be connected to a thermostat, as well as lights and doors, making it easier and safer to notify everyone to get outside. When a person arrives at home, the panel snaps a photo with its built-in camera.

- 7-inch wireless touchscreen panel
- Supports broadband and LTE cellular communications
- Two-way encryption RF sensor technology
- Multicriteria sensor with built-in detectors for smoke, carbon monoxide and heat
- Geofencing technology generates automations and alerts to trigger events with reminders

Qolsys

IQ PANEL 2 PLUS

qolsys.com

This panel includes a 7-inch HD touchscreen, and a built-in 5-megapixel camera. It includes a special daughter card for backwards compatibility of three different legacy wireless frequencies. It provides live view, live answer, Bluetooth touchless disarming features, and supports LTE and Wi-Fi connectivity.

- Hands-free Bluetooth disarming with up to five smartphones
- Supports LTE and Wi-Fi working simultaneously
- Remote control via a mobile app
- Captures images when entering your code
- Built-in glassbreak protection to protect what matters most

Leviton

DECORA SMART 4-BUTTON WI-FI CONTROLLER

www.leviton.com

This controller can be paired with its app and Wi-Fi devices to create a whole-home lighting control system and lighting scenes like All Off, Movie Time or activities like Go to Bed. Advanced settings are available, like adjusting fade rates, brightness levels, bulb types, LED functionality, countdown timers.

- Creates lighting scenes or activities via the My Leviton app
- Multiple 4-Button Controllers can be utilized and placed in different places at home to provide single-button convenience
- Customizes the buttons for different lighting needs
- Advanced settings available — adjustment of fade rates, brightness levels, bulb types, LED functionality, countdown timers

Hubitat

ELEVATION

hubitat.com

With the Hubitat Elevation, users can create and control customized environments with apps that simplify and streamline the automation setup. The device supports groups and scenes by combining devices to set scenes, and controls them based on time of day, modes and triggers.

- Built-in apps and rule-making capabilities
- Compatible with popular digital assistants, such as Amazon Alexa and Google Assistant
- Compatible with Zigbee, Z-Wave, Lutron, LAN and cloud-connected home automation devices
- Features Rule Machine, Hubitat Safety Monitor, Simple Lighting, Mode Manager and Hubitat Dashboard
- Open developer platform — grants users the ability to develop their own code, applications, integrations and drivers

SHOW CALENDAR

World Security Exhibition Directory

Exhibitions marked with ★ indicate a&s portfolio's scheduled participation. See a&s personally at these shows. Please refer to the "Yearly Show Calendar" at www.asmag.com/main/global_events.aspx.

6

IFSEC Philippines 2019

- Date: 2019/06/13–06/15
- Venue: SMX Convention Centre, Pasay City, Metro Manila, Philippines
- Tel: +63-2-551-7564
- Email: IFSECSEA@ubm.com
- URL: www.ifsec.events/philippines/

FIREX International 2019 ★

- Date: 2019/06/18–06/20
- Venue: ExCeL London, U.K.
- Email: FIREXcustomerservice@ubm.com
- URL: www.firex.co.uk

IFSEC International 2019 ★

- Date: 2019/06/18–06/20
- Venue: ExCeL London, U.K.
- Email: ifseccustomerservice@ubm.com
- URL: www.ifsec.events/international/

7

Indo Security ★

- Date: 2019/07/17–07/19
- Venue: Jakarta Convention Center, Jakarta, Indonesia
- Tel: +62-21-8650962
- Email: info@indosecurity.com
- URL: www.indosecurity.com

8

Secutech Vietnam ★

- Date: 2019/08/14–08/16
- Venue: Saigon Exhibition & Convention Center, Ho Chi Minh City, Vietnam
- Tel: +886-2-8729-1099 ext. 768
- Email: stvn@newera.messefrankfurt.com
- URL: www.secutechvietnam.com

9

Adria Security Summit ★

- Date: 2019/09/18–09/19
- Venue: Hotel Aeksandar Palace, Skopje, Macedonia
- Tel: +387-33-788-985
- Email: summit@asadria.com
- URL: www.adriasecuritysummit.com

by Secutech International

President Tsai Ing-Wen greets VIP buyers and senior management from Messe Frankfurt at the opening ceremony of the 2019 edition of Secutech in Taipei. (L-R: Stephan Buurma, Member of the Board of Management of Messe Frankfurt Group; Hubert Duh, Executive Director of Messe Frankfurt (HK); Shi- Jie Xu, CEO of Taiwan Architecture & Building Centre; and Owen Chen, Chairman of VIVOTEK) *Source: www.president.gov.tw/NEWS/24360*

Intelligent solutions for security and beyond: **Secutech 2019 praised for bringing Asia's AI and IoT ecosystems together**

Another productive edition of Secutech wrapped up in Taipei earlier this month, with visitors praising the fair for the quality of its exhibitors and for its product variety. Together with four concurrent events, the fair hosted 335 exhibitors of security, mobility, smart building, info security and fire safety products at the Taipei Nangang Exhibition Centre from 8 – 10 May 2019.

Thanks to the expansion of the IoT sector, the possibilities to integrate security products with processes such as building management have grown. With this in mind, the 2019 edition of Secutech was organized to be much more than a business platform for security products. In fact, two of the fair's four concurrent events, "Mobility" and "SMABIoT," not only presented buyers with security solutions, but they also offered products such as smart building and fleet management systems.

Regina Tsai, the Deputy General Manager of Messe Frankfurt New Era, spoke at the conclusion of the fair about the positive reaction to the fair's product variety: "We are delighted to have welcomed 19,956 trade visitors through the doors over the past three

SHOW FIGURES AT A GLANCE

19,956 international visitors from **57** countries

335 exhibitors from **15** countries

+160 seminar sessions

319 business matching sessions

8 thematic zones and pavilions

days, including system integrators, consultants and distributors from Asia and beyond. The feedback has been encouraging, with visitors commending the fair for offering the complete chain of products across different sectors: from total surveillance and access control systems to security subsystems all the way down to individual components such as camera lenses."

As a platform for international buyers to connect with Taiwan's advanced solution providers, Secutech is recognized by the Taiwanese Government as a positive force for the local security industry.

In remarks at the opening ceremony of the most recent edition, Taiwanese President Tsai Ing-Wen said that the fair helped to promote Taiwanese innovations to the world: "I am pleased to join you all at this security industry event, to learn how AI and IoT technologies can be used in daily life for disaster prevention. My thanks go to the organizer for arranging multiple forums and seminars about information security and successful applications of AI technology. By gathering industry stakeholders from across Southeast Asia to discuss the development of smart applications and products, the fair supports our New Southbound Policy and provides an opportunity to showcase the innovative and robust side of Taiwan to the world." She continued: "Through the joint efforts of the government and the industry, the IoT sector reached a value of over one trillion NTD last year. Meanwhile the security industry has opened up value-added markets and recorded more than 60 billion NTD in export value."

"I am here at the fair because I can find a full range of components, software solutions, and integration opportunities for both home automation and security. Taiwanese companies have very high R&D capabilities and good quality control. Both today and yesterday I have been able to meet with plenty of Taiwanese exhibitors, and I have already begun exchanging emails with some of them. I will certainly return to the fair again in the future."

Michael Bell, President and CEO, Inter-Tel (Japan)

Exhibitors optimistic that new technologies will continue to drive cross sector opportunities

Thirteen themed zones and pavilions were spread across 20,215 sqm of exhibition space at the fair, providing sourcing opportunities for AI software, cloud services, access control systems, IoT security and much more.

One of many discussion points between exhibitors and visitors at the fair was the topic of convergence. Tony Luce, the Director of Sales, Marketing, and Business Development for Network Optix (Nx) spoke about how new online technologies are narrowing the gaps between sectors and creating more business opportunities: "Traditionally, security surveillance technology has been proprietary, but because of the expansion of cloud services and web based platforms over the last five years, we are seeing a lot more interoperability. There are now more opportunities to integrate, and integrations are faster and easier to do. A lot of convergence is taking place because the line between a retail analytics product and a security product, for example, is

completely blurred. You can use the same technology to accomplish two different goals."

Talking about the benefits of exhibiting at Secutech, he said: "We have been coming to the fair for a few years now. We come back because it's a good place to engage with partners and inform the market about new solutions. Taiwan drives a lot of hardware solutions and OEM opportunities. The quality of visitors that come here tend to be a little bit higher from an engineering perspective, allowing us to have higher level conversations."

At the concurrent Mobility event, Joseph Huang, a Sales Manager at Vecow, shared similar sentiments about the effectiveness of the show, explaining that the fair allows his company to promote their new solutions to an international audience: "We are a local company and this is our first time exhibiting at the concurrent Mobility event. The fair gives us the opportunity to meet with relevant international buyers and system integrators. We can share our new product information with potential clients at the fair and hold business discussions to find co-operation opportunities. So far, on only the first day we have met with high quality visitors including government staff that are working on a transportation project in Malaysia."

Buyers commend product variety

With its four concurrent events, the fair offered visitors plenty of cross-over sourcing and integration opportunities. From surveillance cameras, access control systems, and police equipment, to GPS tracking systems, on-board cameras and firefighting gear, visitors had a broad berth of products to source at the fair.

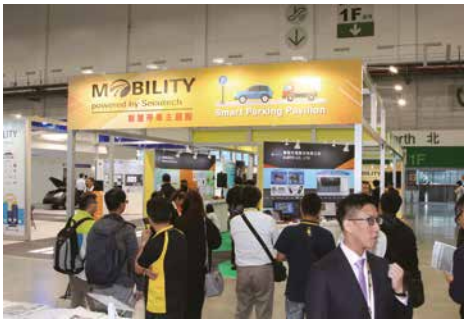
"I am here at the fair because I can find a full range of components, software solutions, and integration opportunities for both home automation and security," said Michael Bell, the President and CEO of Japanese company Inter-Tel, who traveled to the fair to attend the concurrent SMABIoT event. "We provide telecommunication and senior services solutions to local residents and businesses. Taiwanese companies have very high R&D capabilities and good quality control. Both today and yesterday I have been able to meet with plenty of Taiwanese exhibitors, and I have already begun exchanging emails with some of them. I will certainly return to the fair again in the future."

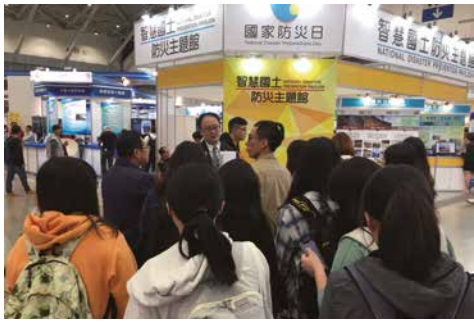
Echoing Mr Bell's positive sentiments, Amon Bazongo, a first time visitor to Secutech and the Co-Founder and CEO of Rwandan company

"The exhibition has changed along with the market; it's not only security anymore. That's why I was interested in the traffic and mobility area. I found something interesting at Secutech that we can use to have different development in our business. It's worth it to come to Secutech."

Aldo Punzo, Product Manager, Bettini (Italy)

Themed pavilions and zones highlight real-life business applications that are opening up new market opportunities.





"I come to Secutech every year. As a visitor, I like to get the most that I can so it's great that Secutech features solutions in security, transportation, smart buildings in one show. I liked that I got a chance to talk to these manufacturers about their solutions."

Bancherd Rachtapattanakul, Founder, Cybertracx (Thailand)

Well-attended conferences and workshops at the event encouraged information exchange on important topics in the industry for the global and Asian market.

Yanfoma, said: "My company provides IT services and we have customers that have asked us to do system integration with access control systems. I have met with several Taiwanese companies, including one that have invited me to their office after the fair. These types of interactions help to build trust."

Speaking about the product variety at the show, he added: "I have been very interested in exhibitors that have integrated machine learning into recognition systems. I also saw some small IoT camera modules that can be easily integrated into a security system."

Fringe program educates the market on AI and IoT trends for security, building, transportation and disaster management

Aside from networking and sourcing opportunities, visitors to the fair also had the chance to educate themselves on new market trends through the fair's three-day fringe program.

Each concurrent event hosted its own series of forums and seminars, with topics ranging from BIoT innovations and future IoT transportation trends, to the uses of AI for security and disaster management.

Joel Liu, the Vice President of HomeScenario was both an exhibitor at the fair and a speaker at the Smart Living Solutions Forum. After his presentation, he said that there is a lot of promise for AIoT to be implemented in Asia's smart building sector: "Asia is still a growing smart building market compared to Europe and the USA, so there is a lot of potential for growth. My talk dealt with how smart building solutions can be built using AIoT and security subsystems. AIoT has become a buzzword in recent years, with many different ways of using the technology. By talking at the seminar, I was able to systematically present our solutions in detail to a large audience. This is something that we don't have the time to do when visitors come to our booth. The response from the audience has been very encouraging."

While much excitement at the fair surrounded the new application possibilities for AI and the IoT, these were not the only technologies being discussed at the seminars and forums. Vince Kuo, a speaker at the Asia Pacific Cold Chain Logistics Seminar explained that RFID technology can also be used across different vertical markets: "In the past, our company, GIGA-TMS, used RFID technology specifically for security purposes, however the technology can be used in many different ways, so we also started using it for the purpose of monitoring and tracking in cold-chain logistics. The concepts that we discuss are relatively new, so the forum is a good opportunity to deliver a focused presentation about topics that the audience may not be aware of."

The next edition of Secutech will take place from 22 – 24 April 2020. Secutech is organized by Messe Frankfurt New Era Business Media Ltd and is part of a global network of Safety Security and Fire trade fairs. For more details, please visit www.secutech.com. Alternatively, please call Ms Emily Lin at +886 2 8729 1052, or send an email to emily.lin@newera.messefrankfurt.com. AKS

Companies in This Issue

Smart & Safe City
- 443 Consulting
- Convergint Technologies
- Indegy
- Security Management International (SMI)

Special Feature
- the Parking Consultancy
- Secure Parking Solutions

Smart Building & Home
- Bluesalve Partners
- Control4
- Danalock
- IDC
- Lilin
- Z-Wave Alliance

Security and IoT for Business
- BriefCam
- Ever AI
- Intelligent Security Systems (ISS)
- RealNetworks

Mobility
- Airbus Secure Land Communications
- Nokia

Industrial IoT
- Ambarella
- ABI Research
- Automation Consulting
- Future Market Insights
- Piltz
- Universal Robots

Market Update (Top 10 Companies in Italy)
- Aikom Technology
- Allnet.Italia
- Betafence Italia
- Cima
- Comlit Group
- Hesa
- Hikvision Italy
- Notifier Italia
- Project Automation
- Tecnoalarm

Products of the Month
- 3dEYE
- Arcules
- Camcloud
- Eagle Eye Networks
- Genetec
- Ivideon
- OpenEye
- Tyco by Johnson Controls

Advertiser Index

*The index is provided as an additional service.
*The publisher does not assume any liability for errors or omissions.

Surveillance

Page No.	Advertiser	Major Item	Country	Email
35	CLIMAX	SMART HOME / HOME SECURITY& AUTOMATION	TAIWAN	Charlene_Yin@climax.com.tw
INSIDE FRONT COVER	DAHUA TECHNOLOGY CO., LTD.	SURVEILLANCE	CHINA	overseas@dahuatech.com
52	GOOD WAY TECHNOLOGY	SMART HOME SOLUYION	TAIWAN	stevensw_wu@goodway.com.tw
19	HANWHA TECHWIN CO., LTD.	SURVEILLANCE	KOREA	customerservice@hanwha.com
BACK COVER, 48-51	HIKVISION DIGITAL TECHNOLOGY CO., LTD.	SURVEILLANCE	CHINA	overseasbusiness@hikvision.com
25	IDIS CO., LTD.	SURVEILLANCE	KOREA	sales@idisglobal.com
3	TECHPOINT INC.	CHIPSET	USA	dma@techpointinc.com
7	TIANDY TECHNOLOGIES CO., LTD.	SURVEILLANCE	CHINA	sales@tiandy.com
5	THROUGH TEK CO., LTD	SMART HOME / HOME SECURITY& AUTOMATION	TAIWAN	Marketing.en@tutk.com
1	VIDEOTEC S.P.A.	IP CAMERA / SOFTWARE / VIDEOSERVER	ITALY	info@videotec.com

Access Control

Page No.	Advertiser	Major Item	Country	Email
47	GIGA-TMS INC.	RFID MODULE / LOCK / READER	TAIWAN	promag@gigatms.com.tw

Advertisers are responsible for their own advertisement content. The publisher is not liable for any legal, patent or trademark disputes from advertisements or among advertisers.

Next Issue

Mobility | **Fleet Management**
Special Feature | **Data Security**
Smart & Safe City | **Seaports**
Smart Building & Home | **Connectivity**

depa | DIGITALTHAILAND

ASEAN THAILAND 2019
ADVANCING PARTNERSHIP FOR SUSTAINABILITY

DIGITAL THAILAND BIG BANG 2019

ASEAN CONNECTIVITY

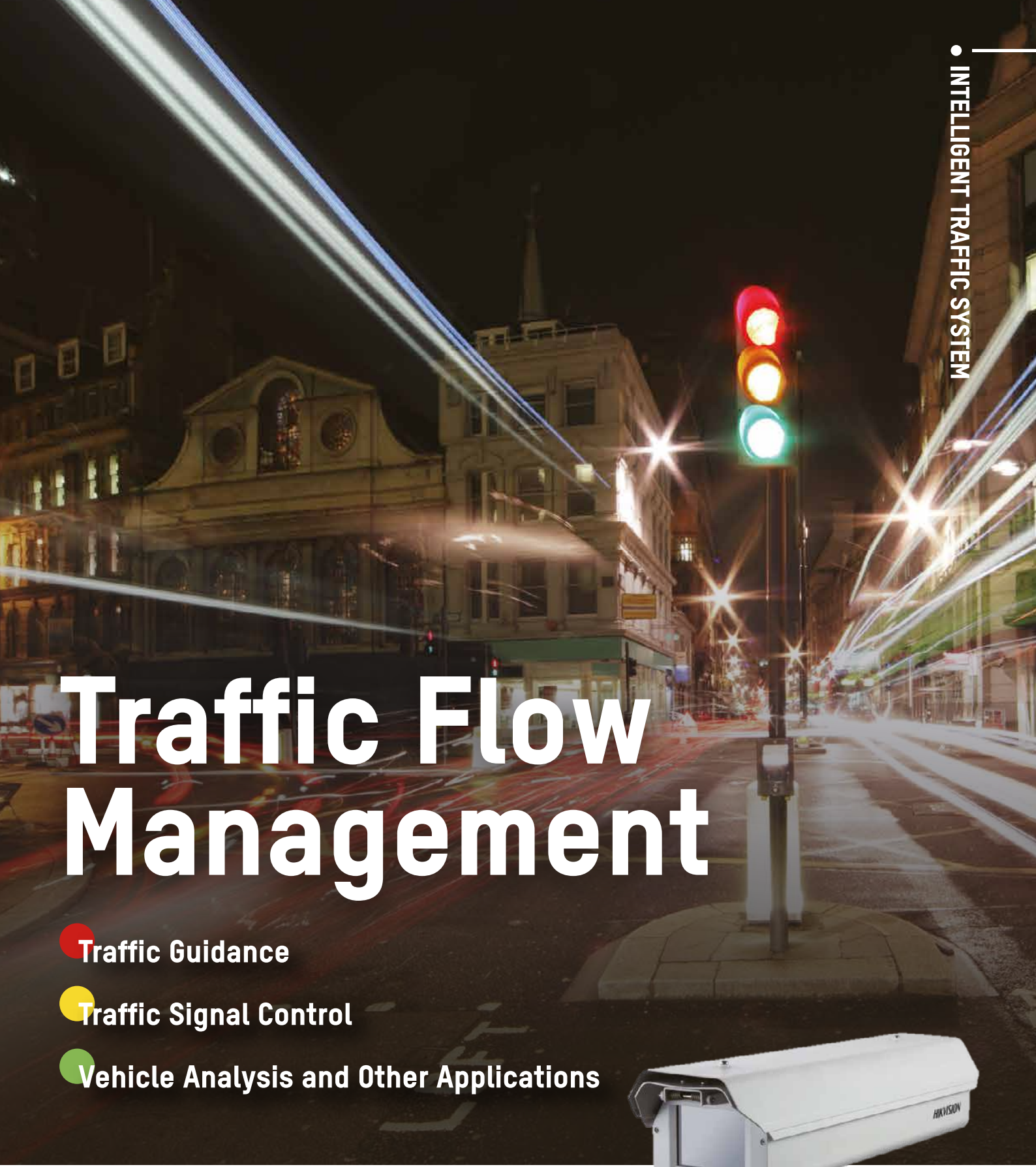
28-31 October 2019 | **BANGKOK, THAILAND @Bitec**

Co-located with

secutech
THAILAND

Security + AI

Thailand's leading security, fire safety and smart living fair empowers sustainable city developments



INTELLIGENT TRAFFIC SYSTEM

Traffic Flow Management

- Traffic Guidance
- Traffic Signal Control
- Vehicle Analysis and Other Applications

Hikvision Headquarters
T +86 571 88075998
overseasbusiness@hikvision.com

@HikvisionHQ @HikvisionHQ @Hikvision

HIKVISION®

www.hikvision.com