

DETEKTOR



Publisher's comment

The death of an era...

Security technology market

**How will Covid-19 affect
the physical security market?**

Business news

Everbridge acquires CNL for \$37.7 million

Product news

Motorola brings facial recognition to VMS

The voice of the security technology market

**Cybersecurity credentials critical
for resilient physical security**

SPECIAL EDITORIAL FEATURE 1:

ACCESS CONTROL
– the market and the trends

SPECIAL EDITORIAL FEATURE 2:

VIDEO SURVEILLANCE
– cloud solutions will streamline the market

SPECIAL EDITORIAL FEATURE 3:

PERIMETER SECURITY
– market demands and technology trends



Strengthen your organization with Security Center

With consolidated monitoring, reporting, and a map-centric approach to security management, Security Center allows operators to become more efficient, make better decisions, and respond to incidents more rapidly.



ISSN-1651-3800 published by **armedia**

Head office:

AR Media International AB
Västberga Allé 32 • S-126 30 Hägersten
SWEDEN
Tel: +46 8 556 306 80
E-mail: info@armedia.se
www.detektor.com
www.armedia.se

Asia Office

Asha Chang
AR Media Marketing Corporation
Address: 15F, No. 55, Bin-hai Road Sec. 1,
Tamsui District, New Taipei (251), Taiwan
Office phone: +(886-2) 2622 1365,
+(886-2) 2622 1385
Mobile: +(886) 922 116272 ,
Email: asha@armediaint.com

General Information

- Detektor International is published twice a year.
- No part of this magazine may be reproduced without prior permission from the publisher.
- Detektor International welcomes manuscripts, news, releases and photographs, but cannot be held responsible for loss or damage incurred in transit or in possession.
- News releases can be sent to intnews@securityworldmarket.com

Subscriptions

Anette Friberg
Rate for two issues is Euro 51
+46 8 556 306 80

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

Rachel Ward Owens, Henrik Söderlund,
Jonny Sjöberg, Lennart Alexandrie
info@armedia.se

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Deniz Baykal
deniz.baykal@armedia.se

Printing

Stibo Complete, 2020



Lennart Alexandrie, Publisher

The death of an era... and birth of another

The Covid-19 outbreak has already had a definitive effect on our behaviours and the way we do business, as we have become used to doing things differently during the unprecedented circumstances that the virus has forced upon us. These new approaches on how to conduct and operate our businesses are very much in line with companies' needs for increased efficiency, whilst also contributing to environmental sustainability over time. In summary, we are using less physical travel and increased digital tools to communicate and deliver service. It is most likely that the changes would have taken place anyway, but the ongoing pandemic is accelerating the process.

One immediate effect on the security industry is the postponement of all the security exhibitions that were planned to take place from March to May. The most important event in the USA, ISC West in Las Vegas, originally scheduled for the 17th to 20th of March, is now re-scheduled to take place on the 20th to the 22nd of July.

Another postponed security exhibition in the international heavyweight division is Ifsec in London. It was scheduled for mid-May but has moved on to the 8th to 10th of September. Its toughest UK competitor – The Security Event in Birmingham – will be held less than two weeks later, from the 22nd to the 23rd of September. Add to this that Europe's biggest security exhibition and Ifsec's major competitor on the international market – Security Essen – also starts on the 22nd of September to be finished by the 25th of September. It is hard to see a winner resulting from this clash.

The Security Event, with its more local UK profile, will probably lose less than the two competing international dinosaurs. Receiving a decent number of international visitors will be tough, even for Security Essen, the only of the three exhibitions that is due to be held on its original dates. The decline in popularity among exhibitors for both Ifsec and Security Essen will be even worse.

Whether ISC West takes place in July remains to be seen. However, this exhibition will probably survive better than its European competitors. The event's importance for the whole

US-market is undisputed and the location of the show, Las Vegas, with its attractions and hotels nearby the exhibition venue make it a perfect place for exhibitors and visitors alike. Add to this that ISC West has not experienced a declining interest among exhibitors and visitors in recent years. And, the event is still backed up by most of the important manufacturers in the security technology market.

Meanwhile Ifsec in London and Security Essen are threatened by a declining interest for exhibiting from major international players. Their claim of being the international leaders among security events in Europe does not help any more. A targeted aim for time efficiency and environmental sustainability by many companies has already affected these events.

The old saying "all business is local" is ever more relevant today in most European countries, where security exhibitions are organised locally on a yearly basis. The local shows – combined with online information sources – are sufficient enough to keep people updated about what's going on in the security industry. Furthermore, these alternatives save time, money and better serve the demand for environmental sustainability.

Now, the corona crisis will not just affect the exhibition sector. Organisations and individuals have been forced to work differently and to use digital solutions to communicate more than ever before. This practice will probably also boost the development towards a generally higher degree of digitalisation in the security industry when the Covid-19 pandemic is over, and could even speed up the implementation of Security as a Service (SaaS), which is about time.

Securitas, the world's second biggest security company, claims they are "leading the transformation of the global security industry". Their security solutions and electronic security sales for 2018 represented just 20 percent (20 billion SEK) of the company's total sales. This shows how far behind the physical security industry still is, but also shows the potential for growth as we are entering the era of digitalisation and technology-based services..

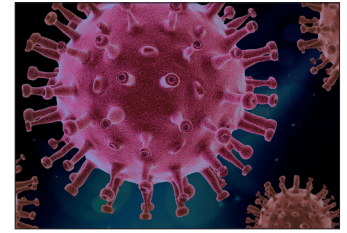


- 3 **Publisher's Comment.** The death of an era...and birth of another.
- 8 **Security Technology Market.** How will Covid-19 affect the physical security market?
- 12 **Editorial Feature: Access Control.** The market and the trends.
- 18 **The voice of the security technology market.** Cybersecurity credentials critical for resilient physical security.
- 19 **Business News.** Everbridge acquires CNL for \$37.7 million.
- 24 **Editorial Feature: Video Surveillance.** Cloud solutions will streamline the market.
- 30 **Product News.** Motorola brings facial recognition to VMS.
- 36 **Editorial Feature: Perimeter Surveillance.** Market demands and technology trends.
- 42 **Security Events Calendar.** The international overview of scheduled security shows.



Special Perimeter Surveillance Feature.

Perimeter security continues to be something that is widely talked about in the physical security industry and the market is expected to continue to grow at almost eight percent per year until 2025. *Page 36*



Security Technology Market

The \$19.9 billion video surveillance market threatened by the corona virus.

Page 8



Access Control

Mobility, face recognition and a move towards IT – these are some of the major trends in access control right now.

Page 12



Business News

ISO develops standards on biometrics interoperability.

Page 19



Video Surveillance

Memoori's 2019 world report on the physical security industry shows that video surveillance product sales reached \$19.15Bn in 2019 and could reach \$35.82Bn by 2024.

Page 24

Stop unwanted activity in its tracks.



Audio for security

By adding audio to your surveillance system, you can either trigger a prerecorded message with analytics in the camera or speak live to the scene. Adding spoken response takes you from passive surveillance to active deterrence.

Axis offers complete, high-quality network audio systems that are not only perfect for security purposes but also for public address and background music in schools, stores and other settings. In our portfolio you find speakers, microphones, amplifier, audio bridge and audio management software. They all let you enjoy the many benefits of network audio.

Learn more about our network audio systems at www.axis.com/products/audio



AXIS[®]
COMMUNICATIONS



Dahua Thermal Solution Supports Epidemic Prevention and Control

A sense of safety is one of the most basic human needs, personal and property safety are integrated into that sentiment as well. And this is exactly why people install security systems in their homes and businesses.

The year 2020 is bound to be a special year with the outbreak of coronavirus disease 2019 (Covid-19) globally. Until today, the highly contagious disease has taken away many lives, especially in China, South Korea, Japan, and as well as throughout the rest of the world.

Dahua Technology, a world-leading video-centric smart IoT solution and service provider, has been an early participant in the epidemic prevention and control in Asia, joining the global efforts in combatting the virus to minimize the impact on mankind. Since sending its first batch of thermal cameras to the hardest-hit area Wuhan on January 24th, Dahua thermal solution has been deployed in thousands of sites in China, including transportation hubs, commercial complexes,

banks, and other places, and some are on the way to multiple countries in Asia.

Dahua Thermal Solution to Measure Human Body Temperature

Hongkong, a financial capital in Asia, also suffers from the Covid-19 epidemic situation. Dahua Thermal Solution has been applied in some local business complexes, banks, company parks, and other places. To enable a safe and smooth work resumption recently, quite a few major corporations have been using Dahua Thermal Solution in their headquarters and subsidiaries to improve their workplace safety. Dahua Thermal Solution measures the body temperature of their employees, handling thousands of staff flow every day. Compared to the traditional way

of body temperature measurement – a forehead thermometer, using Dahua Thermal Solution will significantly improve speed and accuracy, and at the same time, help reduce cross-infection via non-contact measurement. To measure the temperature of 5,000 people, it will take about 4.2 hours using a forehead thermometer, as it takes at least 3 seconds to measure a person. However, it takes only 30 minutes if you use Dahua Thermal Solution, which measures 3 people per second. It also features a high accuracy of $\pm 0.3^{\circ}\text{C}$.

“Dahua Thermal Solution

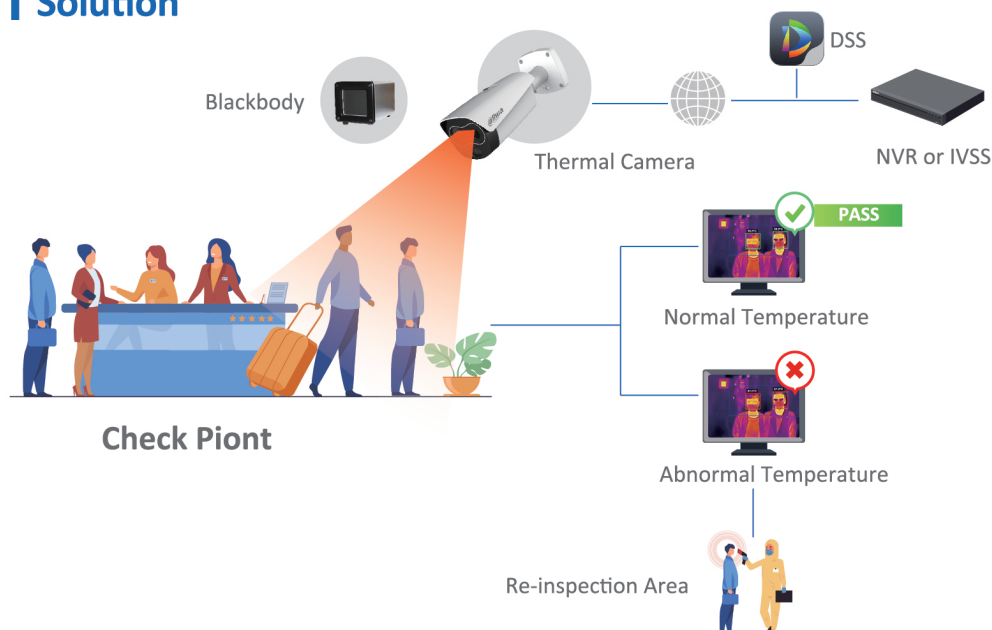
helped us detect a couple of suspected cases in just a few hours of operation, which we greatly appreciate,” a Hongkong user commented.

Dahua Thermal Solution has been on the front line since the very beginning, helping with the epidemic prevention and control in airports, railway stations, hospitals, schools, and other sites all over Asia. Featuring high accuracy, high efficiency, strong adaptability and easy deployment, Dahua Thermal Solution can also be applied to all kinds of entrances and exits, kitchens and kindergartens.

About Dahua Technology

Zhejiang Dahua Technology Co., Ltd. is a leading solution provider in the global video surveillance industry. In 2019, Dahua Technology was ranked 2nd in “Security 50” by a&s international. Dahua Technology is committed to providing the highest quality solutions and products with the latest technologies to enable our end users to perform their business successfully. The company has a high-level group of R&D engineers and technical staff working on cutting-edge technologies in camera lens, image sensor, video encoding & transmission, embedded processor, graphic processing, video analytics, software reliability, network security and other technologies.

Solution



- Accurate temperature measurement, safe and effective
- Non-contact screening, fast pass
- Multi-person measurement, efficient access
- Visual abnormal alert to facilitate back-tracking
- Non-mask detection for the intelligent control

Application Scenario



Airport



Metro



Commercial Building



Apartment

Product Recommendation



DH-TPC-BF3221-T + JQ-D70Z

Thermal: 256*192, 7mm
Visible: 2MP, 8mm
White light and loudspeaker alarm
Temperature accuracy $\pm 0.3^{\circ}\text{C}$
(with blackbody)



DHI-IVSS7008-1I

TPC alarm event linkage
Statistical report and export
8 channels mask detection
8 channels face recognition



DHI-NVR5216-16P-I

TPC alarm event linkage
Statistical report and export
4 channels mask detection
4 channels face recognition



DSS Express/Pro

Unified TPC device management
Real-time temperature display
Rich alarm linkage for TPC events
Multiple clients login

* Design and specifications are subject to change without notice.

Ver. 1, Mar. 2020

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



The \$19.9 billion video surveillance market threatened by the corona virus

London, UK

The corona virus outbreak has had only a minimal impact on the video surveillance market so far, but the risk of falling demand and a potential production bottleneck is spurred by labour and component shortages in China, according to Omdia, the newly formed research company following the merger of Informa Tech and the IHS Markit technology division.

Production of video surveillance equipment is heavily concentrated in China, with the country accounting for 90 percent of global production of video surveillance cameras, and 45 percent of worldwide global market revenue in 2019. As a result, the analysts suggest that any corona virus-related disruption to production, supply chains or workforces in the country could have a significant impact for a global video surveillance market totalling \$19.9 billion in 2019.

“Given China’s status as the world’s largest producer and consumer of video-surveillance cameras, the country wields a proportionately massive influence on the global market for these products,” said By Tommy Zhu, senior analyst, video surveillance, at Omdia.

“Video surveillance equipment suppliers in China currently are contending with reduced production because of a lack of manpower and delays following the Lunar New Year. Meanwhile, domestic demand for general-purpose video surveillance products

is likely to cease or suffer delays as the Chinese government focuses on corona virus control.”

Production delay

With the lockdown of Hubei province, severely affected neighbouring areas—such as the cities of Beijing and Shanghai, and the provinces of Guangdong, Zhejiang, and Jiangsu—are taking various measures to control the spread of the epidemic. One such measure was the extension of the Chinese Spring Festival holiday—initially set to end Jan. 30—to Feb. 2, with a majority of the country’s provinces, municipalities and autonomous regions ordering businesses not to reopen until at least Feb. 10. A 14-day quarantine is also being imposed on specific sectors of the population affected by the outbreak.

Meanwhile, companies that needed to start work after the holiday were ordered to obtain permission from the government, and employees were encouraged to work from home as much as possible.

“While these labour issues



Production of video surveillance equipment is heavily concentrated in China, with the country accounting for 90 percent of global production of video surveillance cameras.

have had only a minor impact so far, if the epidemic continues to spread and infections rise in number in the second quarter, the effects of the corona virus on video surveillance hardware supply will be severe, not only in China but worldwide,” Zhu said.

Logistical nightmares

Transportation and logistics issues are having a huge impact on the supply of video surveillance equipment, given the backlog incurred before the Spring Festival, combined with new restrictions in travel and transport in place both domestically and internationally due to the corona virus.

Component supplies

China is home to several major suppliers of lenses, CMOS sensors and system-on-chip devices used in cameras and other video surveillance devices. These companies have now gradually returned to

work after the Spring Festival holiday. However, staff shortages are possible because the epidemic may reduce the output of various components, even as the full impact of the virus is yet to be determined.

On the flip side, the major video surveillance equipment vendors are the top clients for video surveillance component suppliers, and supply to video surveillance is likely to be prioritised.

Looking forward

In the best-case scenario, Zhu believes that with the epidemic successfully contained by the end of March and the disruptions reduced by April, the impact of the virus on the video surveillance market will be minor. However, if the epidemic continues to spread and infections rise in number in the second quarter, then the effects of the corona virus on the video surveillance industry and on many other markets will be severe.

...and the smart home market expected to fall \$20 billion short

London, UK

Amid the continued fallout of the coronavirus crisis, the global smart home market is expected to fall nearly \$20 billion short of revenue expectations in 2020, according to Omdia.

The global smart home market will total \$101.1 billion in 2020, down from Omdia’s previous forecast of \$120.6 billion. Smart home device shipments are now projected to reach 603.5 million units in 2020, down from the earlier forecast of 693.8 million.

The smart home market consists of devices that have digital connectivity and act as part of a smart home, including appliances, security systems and climate and lighting control.

“Due to the vast number of products available, the smart-home market tends to be more resilient in the face of economic challenges like corona virus compared to other, less-diversified industries,” said Blake Kozak, principal analyst at Omdia. “Nevertheless, the

smart home market is expected to undergo a correction during 2020, where growth will slow for most countries.”

Regional ramifications

Asia is forecast to see the biggest slowdown in 2020, with a downward revenue revision equating to \$7.8 billion and 66.2 million fewer shipments than originally forecast.

In the Americas, the smart home device revenue outlook has been reduced by 10.6 percent.

Device growth in the United States is forecast to remain stronger than other countries. Growth projections could be further reduced if stock markets do not rebound or if the virus spreads to influence U.S. supply chains.

Overall, despite the diversity of smart home ecosystems, supply chain challenges combined with a restrained consumer market and installation and service delays could further slow adoption of smart home technology in 2020.

Future proofing to drive PIAM market to \$1,535 million

Northbrook, IL (USA)

According to the latest research from Marketsandmarkets, the physical identity and access management (PIAM) market size is projected to grow from USD 789 million in 2020 to USD 1,535 million by 2025, at a CAGR of 14.2% during the forecast period.

The major growth drivers for the market include the rising need for future-proofing security operations, increasing instances of insider threats, and stringent security compliances and government regulations.

Small businesses are expected to witness a higher growth in the adoption of physical identity and access management software and services. However, the large enterprises segment is expected to lead the physical identity and access management market due to the early adoption of the software. PIAM vendors help both small and medium-sized enterprises (SMEs) and large enterprises to

address the security needs of business-critical applications to protect them from sophisticated cyber attacks. According to the researchers, the adoption rate for physical identity and access management software and services is high in large enterprises and is expected to dominate the physical identity and access management market in terms of market size, during the forecast period.

Government and defence fastest growing vertical

The government and defence vertical requires physical identity and access management solutions at a large-scale due to the voluminous

information produced across these organisations. PIAM software helps the government and defence vertical secure their infrastructure and users from identity risks with reduced costs. The increasing complexities in networks and increasing instances of insider threats and cyber attacks are fuelling the adoption of physical identity and access management solutions among governments across the globe.

High market share in US

North America has the presence of several prominent market players delivering advanced solutions to all the end users in the regions. Owing to their strong economies, the US and Canada are expected to be major contributors to the growth of the physical identity and access management market. Apart from this factor, the geographical presence, strategic investments, partnerships, and significant R&D

activities are contributing to the hefty deployments of physical identity and access management solutions. Key pure play vendors, such as AWS, IBM, HID Global, and Alert Enterprise offer enhanced physical identity and access management software and services to cater to the needs of customers. Such factors are expected to fuel the growth of the global physical identity and access management market in North America.

Key players

The major vendors covered in the physical identity and access management market and cited by the researchers, include HID Global, Alert Enterprise, ID Cube, Micro Focus, Okta, Access Security Corporation, Gemalto, IBM, Oracle, AWS, Avatier, Wallix Group, Atos, Identiv, Nexus Group, Alfrednet, Wipro, One Identity, Secur, E&M Technologies, and WSO2.

Stringent regulation upgrades drive fire alarm market

San Francisco, Ca (USA)

The global fire alarm and detection market size is expected to reach USD 75.3 billion by 2027, expanding at a CAGR of 8.5% over the forecast period, according to a study conducted by Grand View Research, Inc.

Increasing awareness towards the safety and security of assets across the globe is expected to offer significant opportunities for technological innovations in the market.

Additionally, rise in the consumer spending on fire protection devices especially across the enterprise and industrial sectors in order to reduce the risk of accidents is expected to spur market growth. Moreover, stringent government regulations and mandates regarding workplace safety, and increasing demand for state-of-the-art fire alarm & detection system is expected to fuel the market.

The need for upgrading the existing alarm and detection systems to more advanced versions that consequently comply with the new

stringent regulations will drive the market. A growing number of fire accidents has developed into the need for installation of advanced alarm and detection systems across the residential, commercial, and industrial sectors. For instance, legislative requirements from different countries including the National Fire Protection Association, USA, and Building Code of Australia have mandated the installation of fire detection devices, thereby boosting the demand for these devices.

North America dominated the market in 2019 and is expected by the researchers to continue its dominance over the forthcoming years. Whilst the Asia Pacific region is anticipated to exhibit



A growing number of fire accidents has developed into the need for installation of advanced alarm and detection systems across the residential, commercial, and industrial sectors.

the highest CAGR from 2020 to 2027. Growing industrialisation and urbanisation in emerging markets such as India, China, and Japan is expected to accelerate infrastructure spending including mass transportation such as airport security for example.

The fire detector segment is expected to dominate the market owing to stringent government regulations across various countries mandating the installation of the devices. For instance, in India, the National Building Code (NBC) was published in 2016 to imple-

ment building standards ensuring safety through the use of active and passive smoke detection systems. The segment is expected to reach USD 38.1 billion by 2027

Within the detectors segment, smoke detectors are expected to dominate and the analysts expect that trend to continue over the forecast period, anticipating it to reach USD 17.0 billion by 2027.

Prominent industry participants cited by the researchers include Bosch; Eaton Gentex; United Technologies Corporation; Honeywell; and Johnson Controls.

Covid-19 – how will it affect the physical security industry?

James McHale, CEO of Memoori, gives his view on how the physical Security Industry is being affected by the corona outbreak.

The world is getting used to a new 'C-word', Covid-19. Less than a quarter of the way through 2020 and the global pandemic already has us evoking 'fond' memories of a simpler time in 2019; when we only had catastrophic bushfires and climate change to contend with.

We are still in the beginning phase of this pandemic and our collective global efforts over the next 6 months will hopefully halt its rapacious advance. But at what cost to the world economy, and for the purposes of this article, what cost to the Physical Security Industry?

The total value of world production of Physical Security products at factory gate prices in 2019 was \$34.31Bn, which we estimated was an increase of 8.5% on 2018. Our analysis over the last 5 years, estimates the market grew over 7% per year. And over time, the industry has proven to be robust, driven forward by the consistent forces of increased global terrorism and crime.

Decline of 5 percent

However this inevitable new cycle of recession will certainly reduce demand in 2020. Our current best estimate is that the 1st quarter of 2020 will show a decline of 5 percent, caused by reduced demand in Asia, and specifically China, which is the largest single market for Video Surveillance in the world. Further declines in the next 3 quarters will almost certainly follow. The forecast for 2021 will depend on how the measures to control Covid-19 take hold. If the pandemic shows that it is under control by September 2020 then world sales of Physical security equipment could return to growth by the 2nd quarter of 2021. After all, Covid-19 is a temporary and not a structural issue.

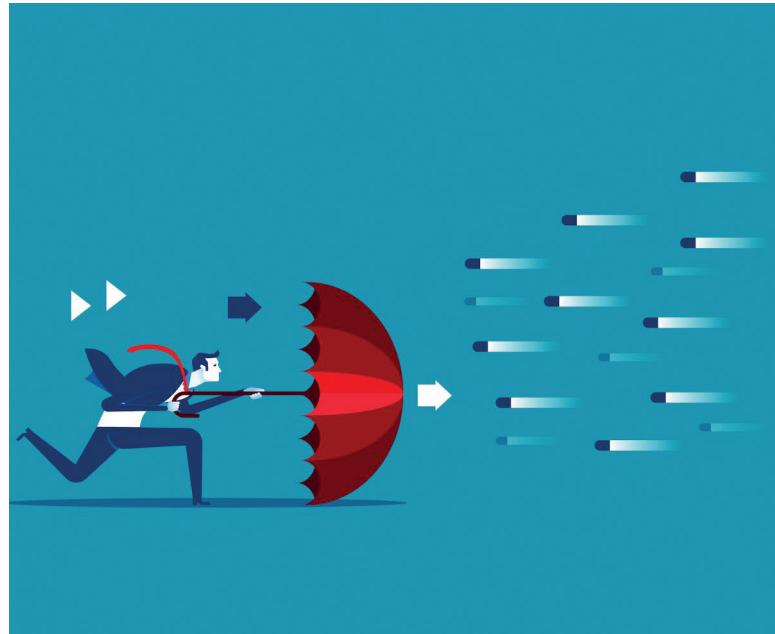
Lessons to learn

Above all the Covid-19 outbreak will force suppliers to radically rethink how they operate their business, in particular resilience to externalities. In parallel, there will be lessons to learn on having a more coordinated and resilient supply chain. The Video Surveillance business is far too dependent on Chinese OEM and component manufacturers. With many of them offline since January, what impact will that have on supply?

A recent analysis by IHS Markit suggests that "Global manufacturing contracted at the fastest rate in over a decade during February... led by a record slump in activity at China's factories".

Offers opportunities

Like with every crisis, there will be opportunities for those Physical Security companies that are prepared to adapt to the new Covid-19 reality. For example, Access Control readers that can eliminate physical contact such as through mobile phones could see a rapid increase in demand. And AI Video Analytics could very likely be required to play an important role in keeping order on our streets, while law enforcement departments are being stretched to cover new responsibilities.



We are still in the beginning phase of this pandemic and our collective global efforts over the next 6 months will hopefully halt its rapacious advance.



James McHale, CEO of Memoori.

The public sector has to pump in money

Specific vertical markets such as Retail, Hotels and Leisure are likely to be hit hard in a recession. It will be the public sector that will have to pump prime the world economy with infrastructure projects in Transport, Hospitals and Education and likely the pharmaceutical industry will need to invest more in new facilities to meet the inevitable demand for medicine and vaccines to combat the virus.

James McHale, CEO of Memoori

Hands-off!

How do you protect sensitive belongings in public spaces?



Hands-on!

ASSA ABLOY
Opening Solutions

Code Handle®: The convenient way to keep the public out of:



Archives

Important or irreplaceable documents deserve extra security



Store rooms

You can't always keep your eyes on everyone in your premises, especially when it's busy



Toilets

If the toilet is for customer use only, Code Handle keeps it locked without the hassle of a key



Offices

Because not everyone in the office should be reading what you left on your desk



Drug storage

Controlled drugs and other medicines are safely protected by a secure PIN and handle

Learn more about Sharing spaces, not belongings at:
campaigns.assaabloyopeningsolutions.eu/codehandle

Experience a safer
and more open world

The global market for access control products reached \$8Bn in 2019

Memoori's Physical Security report for 2019 shows that the market for access control products reached over \$8Bn in 2019, a growth of 8.2%. The company forecasts that by 2024 the world market will be worth over \$12Bn, a CAGR of 8.48 percent.

However, the Covid-19 outbreak may have a serious impact on the industry's sales revenues for 2020, which is not included in this report.

Demand has been driven by growth in IP networking products, access control as a service (ACaaS), biometric readers and identity access management. Integration with other physical security systems and building automation systems (BAS) is now a common requirement. More recently the research company suggests that there is a growing demand for access control systems to lead on building occupancy management systems. The latter has quickly become a complement to access control delivering valuable information on the location of staff and visitors and in the event of an emergency to rapidly clear the building.

There has been significant growth in ACaaS over 2019, probably as high as 20 percent, according to Memoori.

"Our Findings showed that all of the leading suppliers are bullish about the future and are now investing heavily in their cloud services and signing up third parties to deliver their software," says James McHale, CEO at Memoori.

No technical barriers to growth

Access control unlike video surveillance does not consume much broadband and Memoori suggests that there are no technical problems that stand in the way of ACaaS other than the preference of end users to own and house their own system on premise. Many that are about to replace old systems are investigating the economics of either finding the CAPEX to invest in a new one or pay a monthly fee for ACaaS. The latter is an increasingly attractive option.

However, the access control sector is still a much smaller business than video surveillance and today is less competitive, additionally, so far, it has not had to cope with the same price pressures from Chinese manufacturers. This may change, as two major Chinese manufacturers are now active in developing their access control business in western markets and could further change the competitive landscape.

Move towards open standards

The industry has in the past been reluctant to adopt more open standards, but within the last couple of years, some of the leading suppliers are becoming more open. The researchers expect that industry development towards more openness will now gain momentum.

Further moves into IP networking and integration with biometrics, identity management and building occupancy management systems, should maintain the growth momentum that has built up over the last few years but it will ultimately require some standard to be adopted. If manufacturers prefer to continue to be insular and proprietary, it will not be good news for continued growth, as traditional proprietary systems mean limited options for customers and restricted possibilities for integration and scalability.

IoT integration

Winning new business in this global market is becoming more competitive and will require continual product development, which is absolutely essential in order to maintain growth. It is



Memoori predicts that M&A and integration with other sectors will drive the global access control market.

inevitable that as the market will gradually become more open, the heritage real estate business will lose much of its protection. New opportunities will also open up through IoT integrations, and this will require strategic alliances with other smart building companies.

Memoori analysts expect identity authentication to be an important factor in the growth of access control over the next ten years.

"We are now entering a new stage of development where IoT will redefine the concept of identity and access management (IAM), because it will become an integral part of every IoT solution," states James McHale.

A change to come

The analysts suggest that this will take access control out of its silo within the security department and pass to those that set and manage corporate network policy.

James McHale states also that several access control and IAM companies have been involved in acquisitions during the last three years and he believes here are more to come. His prediction for the future access control business is based on the trend towards mergers and integration.

"In the long term: integrating the three security branches – video surveillance, access control and intruder alarm, including perimeter

surveillance – may well bring about change in the routes to market for access control systems."

The corona outbreak

James McHale is aware that the figures in Memoori's report "The Physical Security Business 2019 to 2024" do not include the impact from the corona outbreak.

"Given the unpredictable nature of this crisis it is very difficult to assess exactly what its medium to long term impact will be," he says.

"However this would seem to be an inevitable new cycle of recession that will reduce demand in 2020. Our current best estimate is that the 1st quarter of 2020 will show a decline of 5 percent, caused by reduced demand in Asia, and specifically China, which is the largest single market for Video Surveillance in the world", states McHale.

"Further declines in the next 3 quarters will almost certainly follow. The forecast for 2021 will depend on how the measures to control Covid-19 take hold. If the pandemic shows that it is under control by September 2020 then world sales of Physical security equipment could return to growth by the 2nd quarter of 2021. After all, Covid-19 is a temporary and not a structural issue," concludes James McHale.

Access control technology trends:

Mobility, face recognition and the transition from physical to virtual security

Mobility, face recognition and a move towards IT– these are some of the major trends in access control right now according to the industry professionals who spoke with Detektor/securityworldmarket.com recently.

By Henrik Söderlund

Servaas Kamerling, Product Director EMEA, UTC, believes that one of the major trends in access control is that the market is growing closer to the world of IT and that there is greater flexibility when using the systems.

“In the past security used to belong to the security management team. What we are seeing now, is that the users are exponentially growing. People like department heads and HR managers are becoming involved in the decision making for access control. An HR department can create credentials and the department manager can approve access for an employee, it does not necessarily need to be the security manager”, he says,

Mobile solutions

Servaas Kamerling also stresses that many people want to use smart phones to increase mobility and flexibility. Jaroslav Barton, Director of Product Marketing, PACS, HID, stresses that one of the main trends is moving away from RFID cards into smart phones. He says: “Smart phones are used by nearly everyone today and they provide high levels of security, you can store your ID information in it and smart phones can provide a level of security similar to that of a high security ID card.”

Antoine Larrera de Morel, Sales Director, Stid Group, thinks the biggest trend is the transition from physical to virtual security, thanks to the development of mobile applications for access control and replacing cards with mobile solutions.

Detektor International previously noted that mobile credentials grew by almost 150 percent between 2017 and 2018, and IHS Markit believes the download of mobile credentials will increase

from 9.8 million in 2019 to 120 million in 2023.

Integration with video surveillance

Gary Harmer, Sales Director for Hikvision in the UK, says many end users want to integrate access control into a video surveillance solution.

“So if there is an event on an access control system, such as a door forced open, you can get the associated video”, he says.

Baudouin Genouville, Suprema’s Business Development Director for EMEA, lists

some features he believes are required in order to succeed in the market:

“You need to have a system that is open, that can integrate with video, and not just with your own

Now we see more and more companies using biometrics as a main technology for identification and opening doors. Baudouin Genouville

brand but with others available on the market. The software must be web based and it must be cyber secure. And you need to be able to provide mobile credentials”, he says.

Biometrics more common

Biometric readers are expected to grow in the coming years. There is a lot of talk both about fingerprint and facial recognition.

“In the past, biometrics were used for access control only to a small extent. We were only protecting the cash rooms and the R&D centres where there is some very specific knowledge. Now we see more and more companies using biometrics as a main technology for identification and opening doors”,



Mobility, face recognition and a move towards IT– these are some of the major trends in access control right now

says Baudouin Genouville.

He believes that fingerprint readers are faster, smoother and cheaper than face recognition readers and 95 percent of Suprema’s sales are fingerprint readers. Baudouin Genouville estimates that the price of a face recognition

“From this point of view face recognition sounds perfect, however, facial recognition solutions today are not 100 per cent secure, and they are still very expensive.”

Two-factor authentication

Servaas Kamerling believes there will be a mix of face recognition and fingerprint in the future. The choice depends on what is most convenient for the specific application. He says: “A card is very quick, when you go to biometrics there is always a level of implementation, and throughput time and depending on where you store the templates, it can become more complex. However, biometrics has improved and has really become a consistent component that is part of the overall secure IT system, whether that be for single access control or for dual authentication.”

Antoine Larrera de Morel believes that the trend is that facial recognition is often used as a second technology in two-factor authentication. “With facial recognition installed, you will be recognised no matter whether you want it or not”, he says.

And the integrity issue is something that has been debated lately, for example, both in the EU and in the US and probably even more in the future.

reader has been about ten times as high as a card reader and 2.5 times a fingerprint reader, but that they recently launched a face recognition reader at the same price as a fingerprint reader.

“Not 100 per cent secure”

When it comes to biometrics, Vanderbilt President David Sullivan prefers face recognition to fingerprint readers. “That is because of the speed of development we are seeing. There is no physical action, you literally can walk towards it, it sees you, it unlocks. If it does not recognise you it does not”, he says.

Jaroslav Barton believes that biometric solutions that are seamless and user friendly will be most popular in the future. He says:



HID Global's new Signo line of readers:

"Driving the next wave of flexibility and convenience with mobile access"

HID Global has released the HID Signo its signature line of readers with the aim of creating a new industry benchmark for the most adaptable, interoperable and secure approach to access control.

According to the company, the new readers dramatically simplify system deployment and management, meet the advanced security requirements of today's dynamic environments and set organisations up for smarter, more connected access control.

tions, HID Global.

"HID Signo is built on an open platform and delivers on our commitment to innovation with its unprecedented flexibility and robust set of forward-looking features that optimise workplace experiences. Our goal is to put

HID's novel approach to access control also lays the foundation for a future of cloud-connected systems that will enable new applications and innovative capabilities"

"With the industry now seeking to use access control systems as a backbone for creating intelligent environments, consultants, integrators and end users are increasingly demanding more versatile, high performance solutions," said Harm Radstaak, Vice President and Managing Director of Physical Access Control Solu-

more choices in the hands of our customers and give them peace of mind in knowing they can continually adapt their systems as requirements change."

Interoperability

For ultimate versatility, the readers are interoperable with over a dozen physical and mobile

credential technologies so organisations can use their technology of choice and easily migrate to the latest solutions at their own pace. Additionally, with support for Apple's Enhanced Contactless Polling (ECP) to enable Student IDs in Apple Wallet, HID Signo is driving the next wave of flexibility and convenience with mobile access.

Smart features

HID's new readers are packed with smart features, such as automatic surface detection that recalibrates and optimises read performance based on the mounting location. For rugged, outdoor performance, the readers are also IP65 rated with no additional gasket needed, and feature a capacitive touch keypad resistant to harsh weather conditions.

Reader ecosystem for proactive actions

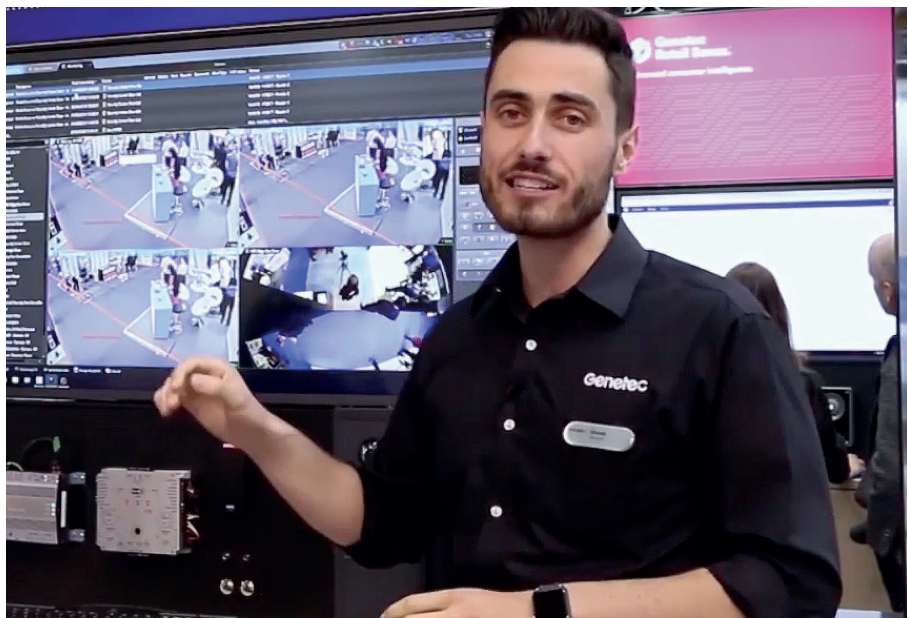
HID Signo's connectivity-by-design model empowers administrators to remotely configure and diagnose readers as well as

monitor status through a centrally managed and connected reader ecosystem. Additionally, configuration can be further streamlined through the controller via the Open Supervised Device Protocol (OSDP).

"HID's novel approach to access control also lays the foundation for a future of cloud-connected systems that will enable new applications and innovative capabilities, such as the ability to proactively anticipate and address system issues before they occur," Radstaak added.

High security

Delivering multi-layered security with built-in support for OSDP Secure Channel and HID's proven Security Identity Object technology, the readers store cryptographic keys on certified EAL6+ secure element hardware and custom authentication keys can be used to further enhance security. HID's patented velocity-checking feature also protects against brute force rapid electronic attacks.



Derek Arcuri, Team Lead, Industry and App Marketing at Genetec.

Beyond access – the top 3 trends in access control

Leveraging an access control system can provide improved compliance and efficiency as well as increased understanding of the built environment. There are 3 trends that can take organisations beyond today's access control, according to Derek Arcuri, Team Lead, Industry and App Marketing at Genetec.

These are the three trends:

1) Increasing threats to network cybersecurity

Threats to network security are increasing. An access control system can have vulnerabilities anywhere from the server to the reader and credentials. The challenge is to protect a system today and in the future.

At Genetec, we work with partners to ensure that our customers have the best tools for maintaining cybersecurity. These include more secure credentials, TLS protocol, and secure measures for client workstations and servers.

2) Greater emphasis on improving efficiency, safety, and compliance

Automation is a great way for organisations to achieve their goals of improved efficiency, safety, and compliance.

When it comes to maintaining all the components of an access control system, keeping elements up to date can be challenging and time-consuming. With Security Center, organisations can bundle and manage updates directly in the configuration tool.

The relationship between safety and compliance is clear. Regulatory bodies set maximum occupancy thresholds for everything from elevators to conference rooms. But enforcing compliance is not easy. By automating these rules within an access control system and counting people as they enter an area, organisations can take control of compliance and ensure safety within their environments.

3) Improved understanding of the security environment

When an organisation, like a hospital, upgrades its facilities, decisions are often based on site surveys. While these provide qualitative data, working with quantitative data, particularly in relation to patient flow and accessibility, can lead to better design.

This same principle will also be important as organisations move towards a mobile workforce. While this can lead to increased collaboration and reduced budget costs, real-estate planning for such a workforce presents a new set of challenges. Where once the majority of employees had regular, predictable schedules, this will no longer be the case. How will organisations prepare for this?

The ability to pull and consolidate access control data from multiple systems is crucial for making informed decisions about space allocation. When organisations can visualise their data in easy-to-run reports in Security Center, they get a clear understanding of their environment, enabling them to better plan for the future.

Derek Arcuri, Team Lead, Industry & App Marketing at Genetec

ASSA ABLOY
Opening Solutions

SIMPLY THE
BEST*



* According to industry media
in 2018 and 2020

Aperio® H100:

Three times awarded by the industry

Learn more:

campaigns.
[assaabloyopeningsolutions.eu/
aperio-h100](https://assaabloyopeningsolutions.eu/aperio-h100)

Wireless access technology

– makes any business more secure and cost efficient

Swapping mechanical locks for electronic access control upgrades a door's security significantly. Yet not every access control problem has the same solution. A single-office small business will not need the access management functionality of a complex, multinational utility with a large or mobile workforce.

In this article, Thomas Schulz, EMEA Marketing and Communications Director at Assa Abloy, gives his view on the development of wireless access technology and gives some examples of solutions and its benefits.

Wireless access technology brings control to more doors than would ever be cost-effective with cabling. Powerful, secure wireless locks are easy to install and energy-efficient to run. There's a solution – standalone, integrated or cutting-edge – for first-time adopters, just as there is for many of the planet's most complex organisations and locations.

Lightweight solutions – no software to install

Code Handle is a secure handle with a built-in PIN keypad. It adds reliable digital security to any sensitive interior door. With Code Handle, you don't need an access control system. It runs autonomously without software or wiring. A secure PIN code makes sure only authorised people unlock your door.

When you switch lock-and-key technology for Code Handle, there are no more cumbersome keys to carry or track, for a storeroom or stock room, a customer toilet or medicine cupboard, or any setting where doors with easy public access need securing. Press a 4-digit code on the handle's keypad and the door opens. Close the door and your Code Handle locks itself automatically.

Key management – a burden in small buildings

Many small and medium-sized businesses do not have the luxury of a specialist security team to ensure the safety of their building or site. For these businesses, Cliq Go is an app-based extension of

the Cliq programmable key access control solution.

With Cliq Go, any non-specialist – a managing director or executive assistant – can issue and programme access rights in new keys. They can cancel any that are lost or misplaced, or when employees leave. Restricting cleaners' access to specific times or days takes a few swipes on a screen. Key-operated Cliq locking cylinders are wireless, so there's no drilling at the door and no extensive cabling around your offices.

Smartair is an access control system which provides an easy upgrade from keys to digital credentials – stored on an RFID card, fob, wristband or smartphone. Lost or stolen keys no longer present a problem, because these secure electronic credentials can be cancelled or reissued anytime. Virtual keys can be sent or revoked over the air in seconds.

In Denmark, one school's mechanical keys were replaced entirely by a Smartair online access control system. Over 80 doors and cabinets around Vejle Friskole are locked with Smartair wireless devices. Using the intuitive Smartair software, managers have an instant overview of who has been at the school, and when.

Large businesses with one control panel for multiple functions

In more complex businesses, access control must fit within a larger security, building management or smart building system. Integration is critical. In a survey for the



There is a wireless access control solution for any size of businesses.

most recent Assa Abloy "Wireless Access Control Report", almost all survey respondents agreed having access control integrated across the building is important. Nine in 10 said the last 5 years have seen its importance grow.

Assa Abloy's wireless lock technology Aperio is built on an open platform specifically for seamless integration. Aperio wireless cylinders, handles, escutcheons and locks work with security systems from more than 100 different manufacturers. At Ghent's Hospital Maria Middelaers, for example, Nedap's AEOS platform integrated with Aperio wireless locks controls every door, credential and user from a single, integrated interface.

Utilities with dispersed workforces have widely adopted Cliq Connect, another extension to the Cliq programmable key access system. The Cliq Connect app pairs a programmable Cliq Connect key remotely with the Cliq Web Manager back at headquarters. To change a keyholder's access permissions, a system administrator accesses the Web Manager and updates it. The keyholder then makes an encrypted Bluetooth connection between their programmable Cliq Connect key and the app to instantly update permissions from the cloud.

The Cliq Connect solution makes ZeFil's mobile workflows

smoother, because administrators can change access rights wherever site users are. A keyholder no longer needs to update their key in person, carry additional programming devices, or return to base. All they need is a smartphone and the Cliq Connect app. Everyone saves valuable time.

Mobile, the credential of the future?

Lost credentials pose a serious threat to workplaces. Mobile access helps here: it's harder to lose your smartphone, and likely you will quickly spot if it goes missing. If your phone is stolen, password, pattern and fingerprint ID security keep thieves out.

Assa Abloy's Openow mobile access solution integrates seamlessly with the Smartair portfolio of wireless locks. Smartair Openow mobile access control enables security managers and site users to manage virtual "keys" inside a smartphone app. With Openow mobile access, facility managers can amend every virtual key's access rights whenever they want and wherever they are. If a security administrator cancels a virtual key, it vanishes immediately from the user's Openow app.

Thomas Schulz, EMEA Marketing & Communications Director Digital and Access Solutions
ASSA ABLOY Opening Solutions EMEA



HELLO **SIGNO**

The Signature Line of Readers from HID Global

Meet Signo at hidglobal.com/signo



Powering **Trusted Identities**

©2020 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, and the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

Cybersecurity credentials critical for resilient physical security

Steven Kenny, Industry Liaison Architecture and Engineering at Axis Communications, examines the potential threats that stem from improperly secured systems and looks at what measures can be taken to ensure their security.

Smart technologies and environments play an increasingly important part in our everyday existence. Smart cities are evolving, using connected devices and applications to manage and maintain basic services that capitalise on efficiencies, and generally improve our lives. Smart homes and businesses are adopting the ubiquity of connected devices to enhance productivity, reduce friction and transform how systems interact with one another.

“**One of the biggest threats to security is a lack of understanding around the vulnerabilities that exist in physical devices.**

The connected future, postulated by conversations around the Internet of Things (IoT) over the past 10 years, has arrived. Yet few realise that these technologies are still in their relative infancy. The devices, the connectivity touchpoints, the vulnerabilities – these present relatively new challenges that have to be overcome to ensure data, citizen and corporate security. For the IoT to succeed, it must be developed with a clear eye on both the physical and virtual environments, using best practice and reliable, certified partners to ensure a resilient security posture.

The cybercrime landscape continues to present a significant threat, particularly with regards to the IoT. According to Gartner, more than 13 billion connected devices are expected to be in use by 2020, and McKinsey estimates that, by 2025, IoT systems could contribute around £155-270 billion to the global economy thanks to more efficient energy and labour management.

Yet, amidst these statistics lies the concern, as highlighted by the UK government's Cyber Security Of Consumer Devices report, that insecure devices can compromise privacy, they can be hijacked and they can be used to disrupt services and lives. The UK National Cyber Security Strategy was established specifically to focus on security across both the physical and cyber realms, and regulations are being continuously updated to ensure that security remains at the forefront of the technology conversation.

The introduction of regulations such as the General Data Protection Regulation (GDPR) and the NIS Directive (directive on the security of network and information systems) have been put in place to ensure that organisations are paying attention. With GDPR, an organisation is held liable for any breach, especially if this is found to have been achieved through poorly managed security systems and applications. One of the biggest threats to security is a lack of understanding around the vulnerabilities that exist in physical devices.

Often, cybersecurity – that is, security focusing on the virtual threat – is given priority. Few realise that a layered cybersecurity approach is critical, as is working with products, services and solutions that are certified, compliant and designed with these risks in mind. A truly robust and holistic

approach to security recognises that each piece of technology plays a role in ensuring that a whole system is secure.

Ensuring high levels of security throughout the supply chain continues to present a challenge. Physical IoT devices, such as IP cameras, that do not meet the required standards ultimately pose a threat to the entire chain, no matter how sophisticated or expensive the cybersecurity investment. An improperly maintained or insufficiently tested piece of equipment could enable backdoor access to malicious parties, putting systems, people and business operations at risk of attack. This risk can be mitigated by working with certified service providers that embed security at the granular level.

The right technologies are those that are deemed secure and fit the requirements of the NIS Directive. In the physical security arena, Secure by Default accreditation, awarded by the Surveillance Camera Commissioner (SCC), Secured by Design, a stamp of approval from the Police Crime Prevention Initiative (PCPI), and Cyber Essentials Plus, a certification awarded by the National Cyber Security Centre, are accolades that provide proof of a manufacturer's security credentials and verification that its products and services are designed and built with security at the forefront.

These credentials play a role in forming the strategic implementation of solid security goals that are aligned with regulation and best practice. It's important that an organisation establishes that the solutions they are considering have appropriate certifications, will operate with other devices or as part of an overarching platform, and to discuss how security is managed and maintained across the ecosystem. Those installing security technologies can benefit from training and education, provided by an approved provider or device manufacturer, which will cover best practice and explore appropriate measures to ensure high levels of security throughout a project.

“**The success of the IoT should not be hampered by weaknesses in physical systems. The potential for its continuing success is too great to be lost to a forgotten IP-flaw.**

The success of the IoT should not be hampered by weaknesses in physical systems. The potential for its continuing success is too great to be lost to a forgotten IP-flaw. The challenge does not lie in how to create the ultimate IoT platform, but in securing it across every touchpoint and unexpected vulnerability. Stakeholders should seek reassurance that those organisations operating with credentials that prove that they take security seriously, have achieved significant standards in security and design, and that they can demonstrate that their products meet the minimum requirements expected in terms of cybersecure surveillance and resilience.



Steven Kenny, Industry Liaison Architecture and Engineering at Axis Communications.

Steven Kenny, Industry Liaison, Architecture & Engineering at Axis Communications.

ISO develops standards on biometrics interoperability

Geneva, Switzerland

Biometric data interchange formats provide the common language that allows for interoperability between different biometric technologies. As the field of applications has grown to give rise to different generations of such formats, so too has the need to ensure they are all compatible with one another. New International Standards have just been published that help to do just that.

A reliable means to verify identities, biometrics is a technology that is increasingly widespread, used in many domains such as border controls using machine-readable passports, healthcare, voter identification and restricted access areas. As the science has evolved, so too has the coding information behind it known as biometric data interchange formats.

In order to ensure interoperability and correct data interchange between different biometric applications and systems, the expert committee on biometrics of ISO and the International Electrotechnical Commission (IEC) has already developed a number of International Standards for a wide variety of applications.

As the technology evolves, however, so do the data elements and formats. Which is why, in order to avoid any future interoperability issues, the experts are developing an additional series of standards that provide the formats capable of being extended in a defined way. The first in this series have just been published and include ISO/IEC 39794-1, Information technology – Extensible biometric data interchange formats – Part 1: Framework; ISO/IEC 39794-4, Information technology – Extensible biometric data interchange formats – Part 4: Finger image data; ISO/IEC 39794-5, Information technology – Extensible biometric data interchange formats – Part 5:



Biometric data interchange formats provide the common language that allows for interoperability between different biometric technologies.

Face image data.

These standards will supersede the corresponding parts of the ISO/IEC 19794 series for data interchange formats, and it is anticipated they will be adopted by the International Civil Aviation Organisation (ICAO) as the basis for their standard 9303 on machine-readable travel documents later this year.

The ISO/IEC 39794 series will be complemented by future additions, including specific parts related to iris, vascular, full body and gait image data.

Patrick Grother, Chair of the ISO/IEC technical committee responsible for the ISO/IEC 39794

series, said it is the latest in a large and comprehensive set of International Standards that support interoperability in biometrics.

“We intend to have internationally agreed standards for all biometric modalities, taking into account the diverse range of applications, the often sensitive nature of the data and the various regulatory and jurisdictional requirements,” he said.

The ISO/IEC 39794 series was developed by joint ISO/IEC technical committee JTC 1, Information technology, subcommittee SC 37, Biometrics, the secretariat of which is held by ANSI, ISO’s member for the USA.

Motorola to acquire Indigovision for £30.4 million

Edinburgh, UK

Motorola has announced that it is to acquire the UK manufacturer of end-to-end video solutions, Indigovision, for a recommended cash sum of GBP £30.4 million (approximately US \$37.2 million), which Motorola will fund through existing cash resources. It is planned that the acquisition will be finalised in May 2020.

According to an Indigovision announcement, the purchase price represents a premium of approximately 116 per cent to the average Closing Price per Indigovision share of 187.6 pence during the 12-month period ended on the Last Practicable Date.

Motorola Solutions, a leading global provider of mission critical communications and analytics, has a strong presence in the large and expanding area of video security. Motorola Solutions’ offerings include high-definition cameras,

advanced video analytics, network video management hardware and software and access control solutions. Motorola Solutions believes that Indigovision’s range of products, global presence and customer base are highly complementary to Motorola Solutions’ existing presence in video security and therefore believes that the acquisition will provide Motorola Solutions with enhanced geographical reach across a wider customer base.

The news of the acquisition comes following the final results

from Indigovision on the 5th March 2020 stating that sales for the financial year ended 31 December 2019 were \$50.2m, representing a 9.2% increase over 2018. In addition, over the last 12 months the company has appointed *Vikki Macleod* to the Board in March 2019, adding expertise in software development, appointed a new Head of Marketing, Vice-President of Product and Engineering, and Head of Customer Care and Operations from outwith the business, and it has strengthened its Senior leadership team. Additionally, Indigovision also acquired Agorasys SA in November 2019 to enhance the company’s software product offering.

Commenting on the acquisition by Motorola, *Pedro Vasco Simoes*, Chief Executive Officer of In-

digovision said: “The access we will now have to Motorola Solutions’ range of innovative technologies will create new opportunities for Indigovision and enable us to bring an exciting proposition to the market that allows us to further deliver on our goal of delivering safety, security and business intelligence.”

Commenting on the acquisition for Motorola Solutions, *John Kedzierski*, Senior Vice President, Video Security Solutions, said: “We share Indigovision’s commitment to providing next-generation, end-to-end video security solutions that enhance safety, security and efficiency. Indigovision’s end-to-end offering, global presence and customer base will complement our existing and growing presence in video security and analytics.”

EU Commission clears Assa Abloy for Agta Record acquisition

Stockholm, Sweden

Assa Abloy has received phase 1 conditional clearance by the EU Commission for Assa Abloy, as a 39% shareholder in the Swiss company Agta Record, to indirectly acquire the 54% shareholding in Agta Record from the shareholders of Agta Finance.

Closing of the acquisition is expected in the second half of 2020 after all remaining closing conditions and the EU Commission requirements have been fulfilled.

"Receiving the EU Commission's approval is an important step towards completing the

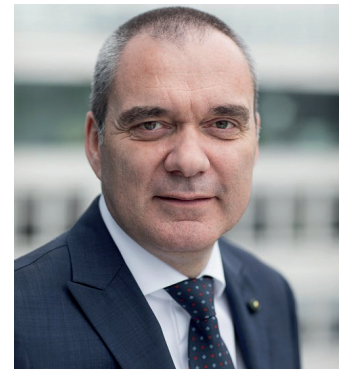
acquisition of Agta Record and we look forward to welcoming the Agta Record people to our Group. This is a strategic addition to the Assa Abloy Group and will bring important competence, products and services to the Group," says *Nico Delvaux*, President and CEO of Assa Abloy.

During the approval process in Europe Assa Abloy has made commitments to address the competition concerns of the EU Commission, including entering into binding agreements for the sale of certain Agta Record and Assa Abloy businesses to third parties.

The commitments include the divestiture of the Agta Record operations in the Netherlands, Austria, Hungary and Slovenia as well as the Assa Abloy automatic

pedestrian door business in France and the UK. In addition, Agta Record's high-speed door business in France will be divested. It is important that the divested businesses get a committed and experienced owner that gives them a new home and creates opportunities for the future. These divestments represent about 20% of total initial added revenue. Despite these divestments, however, the majority of the identified synergies between Assa Abloy and Agta Record will be realised.

After the acquisition Assa Abloy will own approximately 93% of the share capital and voting rights of Agta Record and will shortly thereafter launch a public tender offer for the remaining outstanding shares of Agta Record,



Nico Delvaux, President & CEO, Assa Abloy.

listed on Euronext Paris, at a price of 70 EUR per Agta Record share, subject to the fairness opinion of the independent appraiser to be appointed by Agta Record and to the AMF's clearance decision in the form of image material.

Assa Abloy acquires UK biometrics company

Stockholm, Sweden

Assa Abloy has acquired Biosite, a leading solutions provider of biometric access control to the UK construction industry.

"I am very pleased to welcome Biosite and their employees into the Assa Abloy Group. Biosite is a strategic technological addition to the Assa Abloy Group. The company will rein-

force our current offering within solutions for access control and will provide complementary growth opportunities," says *Nico Delvaux*, President and CEO of Assa Abloy.

"Biosite offers biometric access- and workforce management solutions to the construction sector; maximizing security

and safety whilst providing full visibility to material-, design plans- and people flow on the construction site. Combining hardware, software and services the company is a very good fit with Assa Abloy Global Solutions," says *Christophe Sut*, Executive Vice President and Head of Global Technologies business

unit Global Solutions.

Biosite was founded in 2010, has some 140 employees and the main office is located in Solihull, UK. Sales in 2019 amounted to about GBP 14 million (approx. SEK 175 million) and the acquisition will be dilutive to EPS from start.

Milestone Systems CEO resigns

Copenhagen, Denmark

After 17 years, *Lars Thinggaard*, President and Chief Executive Officer at **Milestone Systems**, has decided to leave the company. As a result, the Board has started an open search to appoint a successor to Lars Thinggaard. During the intervening period, *Lars Larsen*, Milestone Systems' Chief Financial Officer, will serve as Interim CEO.

Following the announcement, *Lau Normann Jørgensen*, Chairman, Milestone Group, said: "I am very grateful to Lars for the energy, vision, and heart that

he has dedicated to Milestone employees and the community partners. Please join me in wishing Lars the absolute best in all his future plans and endeavours."

Lars Larsen, Chief Financial Officer and interim CEO said: "I would like to echo Lau's thanks, Lars has played a crucial role in the development of Milestone. Looking ahead, Milestone is a strong company and well positioned to continue as a leader in the open platform video management software business."

Lars Thinggaard has been

President and CEO of Milestone Systems for 17 years and before this as a member of the non-executive board. For the last six years, since the company's acquisition by Canon Group in 2014, he has led Milestone as a standalone company in the Group. Under his leadership, Milestone has developed into a growth company with a strong team and a great future.

Looking ahead, as investor and non-executive chairman of several companies in the startup community, the company says



Lars Larsen CFO and Interim CEO, and Lars Thinggaard outgoing CEO, Milestone Systems.

that Lars sees that now is the right time to move on and focus on these new initiatives and he would also like the flexibility and time to promote his new book.

Nexus acquired by IN Groupe

Paris, France

IN Groupe (formerly Imprimerie Nationale), a world specialist in identity and secure digital services, has entered into a share purchase agreement, as of February 2020, to acquire Nexus the European leader in enabling trusted digital identities for people and things.

Nexus provides secure solutions that make it easy to issue, manage and make valuable use of trusted identities for both people and things. The company specialises in software that empowers a smooth, automated and governed solution to manage the full life cycle of both physical and digital identities for both people and objects. These solutions include a powerful Public Key Infrastructure (PKI platform), Card Management System (CMS), mobile and desktop-based identity apps (middleware) and a digital access gateway.

With the acquisition of Nexus, IN Groupe is accelerating its growth and confirms its strategic ambition: to be a leading player in identity and secure digital services globally. The integration of these

new digital identity solutions will enable the group to provide clients in France, Europe and globally a consolidated portfolio of differentiated offers, based on cutting edge technologies. The aim is that the combined set of technologies will ensure that IN Groupe's services for governments and corporate customers are more secure, more robust and more competitive than ever.

Consolidating technological capabilities

For 10 years, IN Groupe has demonstrated its unique ability to transform its business in keeping with the digital evolution of the identity sector. Today, the acquisition of Nexus represents a new stage in consolidating IN Groupe's technological capabilities after the

acquisition of SURYS in December 2019.

The acquisition of Nexus gives IN Groupe, a state operator for identity, the ability to lead the transition from physical to digital identity in the European regulatory environment (e.g. e-idas, GDPR).

Furthermore, IN Groupe expands its activities into the field of IoT and the identification of objects on the internet – such as connected cars. Nexus is known for being the world leader when it comes to certificate-based identity services enabling the future of autonomous cars and V2X (vehicle to everything).

International opportunities

IN Groupe will give Nexus access to its world class capability to integrate global legal and digital identity systems. It will also introduce new opportunities with respect to an international complementary customer portfolio.

Didier Trutt, Chairman and CEO of IN Groupe says, "Two months after the integration of



Magnus Malmström, Nexus CEO, and Didier Trutt, Chairman and CEO of IN Groupe.

SURYS, the acquisition of Nexus completes IN Groupe's offer on secure identity in France, Europe and globally. It also gives us, as a public operator, the capacity to master critical technologies at a European level in order to lead the transition from physical to digital identity."

"Today is a very big day for Nexus," Magnus Malmström, Nexus CEO, said. "We share IN Groupe's belief in the power of enabling trusted identities for large enterprises and the public sector. Together, we will be stronger, and we will support our customers even more with secure digital transformation."

Everbridge acquires CNL for \$35.7 million

Burlington, Ma (USA)

Everbridge a global leader in critical event management or CEM, recently filed a 10K SEC document advising the acquisition of both CNL Software and Connexient, a move which will enhance the company's solutions and broaden its support for IoT applications in commercial buildings.

Almost in tandem with this announcement, the company has unveiled new CEM capabilities across the Internet of Things (IoT) for corporate, government and healthcare organisations to protect people, assets, operations, supply chain and brand from critical events such as corona virus (Covid-19).

The first acquisition, New

York based Connexient, which Everbridge acquired for \$20.5 million, is a start up company providing digital wayfinding and indoor navigation solutions for the healthcare sector. There is also a potential contingent payment of up to \$6.0 million that can be earned by the sellers, based on fiscal year 2020 revenue figures.

The second acquisition towards the end of February was CNL Software, a UK based PSIM company founded in 2001, which Everbridge has acquired for a base consideration of approximately \$35.7 million.

"The CNL acquisition enhances Everbridge's enterprise risk management approach and broadens their PSIM portfolio, which was previously enhanced in January 2017 when the company acquired IDV, a US based software solutions provider for powering command centres for \$18.7 million plus add-ons. The CNL transaction will also enhance Everbridge's long-term

growth strategy to expand outside the United States. It is their 5th international acquisition in the last 6 years." commented Daphne Tomlinson, Senior Research Associate at Memoori.

The upgraded Everbridge CEM platform will feature a new IoT extension module that will leverage the intellectual property rights of Connexient and CNL Software, enabling organisations to gather a broader range of situational intelligence and automate targeted responses throughout their entire safety, security, and operational continuum – from across a global footprint to within campuses and facilities.

Business & Product News – Every Day!

www.securityworldmarket.com

HID names new president & CEO

Austin, Tx (USA)

HID Global, a worldwide leader in identity solutions, has named *Björn Lidfelt* as the company's new President and CEO.

Björn joins the company after serving as Chief Commercial Officer (CCO) at HID parent com-

pany Assa Abloy, where he oversaw branding, communications, commercial development and strategy. He also has extensive experience in international sales and marketing, having spent more than nine years in Asia Pacific markets including

China and Malaysia.

Björn Lidfelt succeeds *Stefan Widling*, who led HID Global for over four years.

"I look forward to leading a dedicated and talented global workforce focused on delivering

industry-leading solutions to governments, universities, hospitals, financial institutions and some of the most innovative companies on the planet to create trusted physical and digital places," Björn added.

Acquisition strengthens Securitas in Iberia

Stockholm, Sweden and Madrid, Spain

Securitas has acquired the Spanish company Techco Security at an estimated purchase price €22 million (MSEK230).

Techco Security offers a integrated security services including installation, maintenance and remote guarding services as well as access control, electronic alarm surveillance and fire protection,

and supports clients through two operations centres in Madrid and Barcelona. The company has approximately 520 employees with a strong footprint across Spain and Portugal. Techco Security's annual sales was MEUR \$50 million (MSEK 520) in 2018.

"The acquisition represents an important milestone in the

transformation of our company. We will have an even stronger position in delivering quality electronic security services to our clients and we will continue growing the business together with the team", says Jorge Couto, Divisional President, Security Services Ibero-America.

In the full year of 2018

security solutions and electronic security sales represented 20 percent, or approximately BSEK 20, of total Securitas Group sales. Securitas ambition for its security solutions and electronic security business is to double the size from approximately BSEK 20 in 2018 to approximately BSEK 40 in 2023.

Bosch develops a code of ethics for AI

Stuttgart, Germany

Bosch has established ethical "red lines" for the use of artificial intelligence (AI). The company has now issued guidelines governing the use of AI in its intelligent products.

Bosch's AI code of ethics is based on the following maxim: Humans should be the ultimate arbiter of any AI-based decisions. "Artificial intelligence should serve people. Our AI code of ethics provides our associates with clear guidance regarding the development of intelligent products," Bosch CEO Volkmar Denner said at the opening of Bosch Connectedworld (BCW), the company's annual IoT conference in Berlin. "Our goal is that people should trust our AI-based products."

AI is a technology of vital importance for Bosch. By 2025, the aim is for all Bosch products to either contain AI or have been developed or manufactured with its help. The company wants its AI-based products to be safe, robust, and explainable. "If AI is a black box, then people won't trust it. In a connected world, however, trust will be essential,"

said Michael Bolle, the Bosch CDO and CTO. Bosch is aiming to produce AI-based products that are trustworthy. The code of ethics is based on Bosch's "Invented for life" ethos, which combines a quest for innovation with a sense of social responsibility.

Over the next two years, Bosch plans to train 20,000 of its associates in the use of AI. Bosch's AI code of ethics governing the responsible use of this technology will be part of this training programme.

AI offers major potential

Artificial intelligence is a global engine of progress and growth. The management consultants PwC, for example, project that between now and 2030, AI will boost GDP in China by 26 percent, by 14 percent in North America, and by around 10 percent in Europe. This technology can help overcome

challenges such as the need for climate action and optimise outcomes in a host of areas such as transportation, medicine, and agriculture. By analysing huge volumes of data, algorithms are able to reason and make decisions. Well in advance of the introduction of binding EU standards, Bosch has therefore taken the decision to actively engage with the ethical questions that the use of this technology raises. The moral foundation for this process is provided by the values enshrined in the Universal Declaration of Human Rights.

Humans should retain control

Bosch's AI code of ethics stipulates that artificial intelligence should not make any decisions about humans without this process being subject to some form of human oversight. Instead, artificial intelligence should serve people as a tool. Three possible approaches are described. All have the following in common: in AI-based products developed by Bosch, humans should retain control over any decisions the technology makes.



Bosch has established ethical "red lines" for the use of artificial intelligence (AI).

The importance of trust

Bosch also hopes its AI code of ethics will contribute to public debate on artificial intelligence. "AI will change every aspect of our lives," Denner said. "For this reason, such a debate is vital." It will take more than just technical know-how to establish trust in intelligent systems – there is also a need for close dialogue among policymakers, the scientific community, and the general public. This is why Bosch has signed up to the High-Level Expert Group on Artificial Intelligence, a body appointed by the European Commission to examine issues such as the ethical dimension of AI.



The card that never sleeps

Micron® Industrial microSD Cards 32GB-1TB

- 3 years 24x7 recording
- 2M hours MTTF
- Lifetime health monitor
- Up to 960 TBW
- Frame capture optimization
- Card lock/unlock for data security

Edge storage
for surveillance
IP cameras





Memoori's 2019 world report on the physical security industry shows that video surveillance product sales reached \$19.15Bn in 2019 and could reach \$35.82Bn by 2024.

AI video analytics ready to take off – before the Covid-19 pandemic outbreak

Memoori's 2019 world report on the physical security industry shows that video surveillance product sales reached \$19.15Bn in 2019 and could reach \$35.82Bn by 2024.

However, the report was released at the end of 2019, before the corona crisis hit the world so viciously, so figures regarding the future growth and similar predictions are no longer relevant until we know how the pandemic will affect the market.

By Henrik Söderlund

In the report the Memoori forecast showed the highest growth ever, and explained that it is being driven by a number of factors – but particularly the sales of AI video analytics software now entering the commercial market.

Analysts found also that the VSaaS market was growing at around 15% per annum and the impact of the IoT has yet to be fully realised. IP video cameras could become one of the most powerful sensors in commercial and industrial buildings.

AI video analytics provides the boost

So before the Covid-19 pandemic Memoori suggested that the AI video analytics contribution would boost video surveillance sales, on its own contributing some \$3.5Bn to 2024. The company predicted that AI video would be the main game changer over the next 10 years, and that China will take more than 50% of the world market for AI video analytics software by 2024, but privacy issues in Western markets could hold back the rate of growth. The traditional

video surveillance companies naturally see AI video analytics as a feature to run off their existing products offering a way to differentiate themselves.

Cameras with embedded video analytics, such as motion, face, and

“IP video cameras could become one of the most powerful sensors in commercial and industrial buildings”.

object detection, analyse image data at the point of capture and can effectively eliminate the need to transmit video and data to a central server. This enables very efficient use of both transmission and recording bandwidth.

Cloud services gain credibility

According to the report, there is much evidence in 2019 that in the physical security business, that cloud services, specifically VSaaS, has broken off its niche market shackles and its capability and performance value are no longer doubted. Demand was growing significantly this year and

Memoori forecasted that over the next 5 years it will deliver a CAGR of no less than 12%.

The report also pointed out that in the next few years – as the Building Internet of Things (BIoT) becomes a reality – IP cameras will be directly connected with these systems and that will present a myriad of opportunities for them to contribute to solving other problems not necessarily associated with security.

Integration within physical security is now a common requirement and IT convergence is almost a given in the enterprise market. The BIoT will connect services in the building, minimizing duplication, reducing hardware and software costs and IP cameras will

become an important factor acting as sensors in buildings. This, say the researchers, will change the routes to market and introduce new players into the business.

More innovative products

The research found that background economics and trading conditions have remained fairly static in the last year but more innovative products that have delivered better performing systems have more than compensated for this and quality brands have increased their share of the business as a result. Memoori had expected for the last 2 years that merger and acquisition by non-Chinese

companies would have delivered some help in building up scale but found nothing of any great consequence has happened through acquisition.

Geographical changes

Over the last eight years there has been a major change in the geographic distribution of video surveillance product sales. Asia has delivered the highest rate of growth, increasing its market share every year and there is still a massive latent demand waiting to be exploited. The main driver of this growth is China where the penetration is still less than a half of that in North America and well before this latent business has been mined, the Chinese market will be more than twice the size of North America.

The Covid-19 impact

In an article on page 10 in this magazine, the CEO of Memoori, James McHale, make comments on how sees the impact of the Covid-19 on the global markets for intruder alarm, access control and video surveillance. He forecast a general decline of 5% for the first quarter, caused by reduced demand and further declines for the next three quarters to follow.

But regarding some video surveillance areas he can see a possible growth. AI video analytics is an example. McHale states that AI video analytics “could very likely to be required to play an important role in keeping order on our streets, while law enforcement departments are being stretched to cover new responsibilities.

Cloud solutions will streamline the video surveillance market

Cloud solutions for video surveillance eliminates the need of cumbersome on-site storage. In addition, SD cards now can store much more than before, enabling storage at the edge. However, cloud solutions have not had as big a breakthrough in the physical security industry as in many other industries. Yet.

Detektor and securityworldmarket.com have interviewed some representatives for leading video surveillance companies about the development of cloud solutions on the market.

By Lennart Alexandrie

Cloud based video surveillance allows users to remotely store, manage, record, play, and monitor surveillance footage entirely on the cloud. The advantages include cost efficiency, remote access to data, secure data storage, and high reliability, among many others.

"The market is ready"

Rishi Lodhia is Managing Director for Eagle Eye Networks, an American company that offers cloud-based video surveillance. He believes that the major benefits of the cloud are that end users do not need to have large hard drives in on site, and do not have to manage video surveillance themselves, or update software since everything is managed centrally.

Rishi Lodhia says: "We get a lot of inquiries from retail but also from others. We offer the services both to small companies and to large organisations such as hospitals and to companies operating in thousands of different locations"

He believes that the market is ready for cloud services and that a shift is underway right now. The IT industry has already made the shift and video surveillance and access control are two of few technologies that have not fully taken the step towards the cloud.

"End customers are driving demand for cloud services in video surveillance and are already used to paying a monthly fee for various services. Retailers and integrators also see the benefits of this business model with recurring

revenues", says Rishi Lodhia.

Håkan Johansson, Axis Communications' Sales Manager for Northern Europe, is also very positive about cloud services. He says: "With hosted cloud solutions you avoid some start-up costs, and since someone else is managing it for you, there is no need to think about cost for services, upgrades and so on. Paying a monthly fee seems to be very popular for many and especially for small end customers."

“End customers are driving demand for cloud services in video surveillance and are already used to paying a monthly fee for various services”.

Storage at the edge

Cloud solutions are not the only way to avoid local network video recorders and centralised storage. For example, Micron Senior Director of Segment Marketing, Amit Gattani, stresses their latest 1TB micro SD card enables users of video surveillance systems to capture and store more than three months of high-quality video footage at the edge. This makes it cheaper for small- to medium-sized deployments to have primary storage in the camera compared to a centralised storage architecture.

Has lagged behind

Josh Woodhouse, principal analyst of video surveillance technology at IHS Markit, thinks video



More cloud solutions mean cyber security becomes even more important.

surveillance has lagged behind the wider IT industry in adopting the cloud and the reason why is the amount of data it generates. He says: "That means that the cost of bandwidth is still quite high and can put quite a lot of people off from a cost point of view. The data that has been required to be restored has generated a huge external storage market for video

still from storage point of view"

Vanderbilt President David Sullivan has a clear opinion in the matter of why cloud solutions have not been more widely adopted. He says: "The problem is that the installers are sometimes reluctant to make the change and I think that is because they do not know how to deal with some of the obstacles they encounter".

Cyber security

More cloud solutions mean cyber security becomes even more important. Håkan Johansson, Sales Director for Northern Europe at Axis Communications, says even though the industry has been working with network products and IoT for a long time, cyber security issues have caught the industry by surprise. However, he believes products are safer today compared to a couple of years ago. He says: "But at the same time, the threats are evolving all the time, you need to keep up the good work at all times".

Mobotix CEO Thomas Lausten argues cyber security is a trend that has started in some markets but has now moved into other areas. He says: "And therefore we believe we will see a much stronger trend towards cyber security in an everyday business aspect. It will be as important as it is today to have a high-resolution camera."



Zipstream – the story behind the invention of a revolutionary compression technology

Years ago, the bitrate consumed by cameras was holding the industry back, a technical obstacle on the path of innovation. A group of Axis engineers set out with the ambition to improve the bitrate by perhaps 10–15%. When they finally held the new technology in their hands, the results were much better with an improvement of up to 95 percent, without losing important details in the footage.

Now the Zipstream technology is in place in almost every Axis camera from that point on.

Before Zipstream, video surveillance was wasting lots of bitrate on recording details that were not important – such as a plain, unmoving wall. As such, it was affecting the bandwidth and storage of video footage. In 2014, at the HQ of Axis Communications in Lund, Sweden, a diverse group of engineers began working on a solution to change bitrate and remove these obstacles.

“I remember the first time we tried the algorithm outside,” says Viktor Edpalm, Senior Engineer in the Core Technologies Media department of Axis.

“We still didn’t know exactly how efficient it would be outside the ideal condition of the lab. There was a flock of crows in our frame, just flying around, must have been three hundred of them, but when we decompressed the footage...you could still see every single bird. It was simply incredible.”

A revolutionary compression technology

Viktor was one of the minds behind the invention of Zipstream, a revolutionary compression technology which doesn’t simply reduce bitrate, but is also able to identify crucial forensic information through the use of three different algorithms, ensuring it’s recorded and sent in full resolution and at full frame rate. Along with Expert Engineer Stefan Lundberg and Project Manager Xing Danielsson Fan (at the time an engineer herself), Viktor and the team developed the technology in 2014.

A winning innovation

Axis now includes Zipstream in most of its cameras, since it can be applied to virtually any type of installation. Zipstream has also been awarded multiple times, acquiring trophies such as the Detektor International Award (first prize) for best video surveillance product 2015, “New Product of the Year” award in 2015 for Advanced Imaging Technologies and the “Government Security Award” in 2016 for Video Surveillance Data Storage, both from Security Today Magazine.

Finding a new edge

In 2014 hard disk storage was still the most popular choice; cloud storage was making its first steps into a larger audience, but the bitrate was still a major obstacle. So, when the team was first put together, they had a goal: being able to compress video footage for storage without losing details. However, they didn’t yet have a solution.

“We knew there was untapped potential in compression software and we were determined to create something that could benefit both on-site storage and cloud users,” says Stefan “But we could have never imagined where the journey would bring us.”

Sensational result

They started with the idea of optimising bitrate by 10%, maybe 15% at best, but at the end of the process they had improved it by up to 95% without losing important details in the footage. The eureka moment finally came



The team behind the invention of Zipstream compression technology, from left: Xing Danielsson Fan, Viktor Edpalm and Stefan Lundberg.

after months of experimenting and brainstorming, when Viktor showed his colleagues two supposedly identical pieces of footage, one recorded with the usual bitrate, and the other using the new compression technology. A heatmap of the video highlighting the areas of reduced bitrate showed it was possible to maintain every detail while reducing the overall bitrate.

“When we saw it”, recalls Xing, “We understood we had something great and unique.”

A game changer

Of course, the process was not without its challenges. The greatest involved low light conditions, but the team was impressed and surprised to see how well the technology handled it, not just at night time but also in bad weather conditions like a snow storm. The results were almost even better than in daylight.

As for how they did it, the team believes that it was their diversity that made the difference and helped them overcome every challenge. People of different ages, cultural and professional background put their minds together and managed to think out of the box, accomplishing even better results than they expected in the first place.

“We thought cloud users would adopt it straight away,” recalls Stefan, “But the people using on-site storage loved it! They were the first to embrace it.”

Banks also saw a great potential in the technology, for its capabilities of maintaining forensic details.



Before Zipstream, video surveillance was wasting lots of bitrate on recording details that were not important.

A large banking group became Axis’ client for the first time thanks to Zipstream; by integrating the software to the cameras in their branches, they managed to save and store more surveillance footage in one centralised database, without losing video quality.

The job is never done

The development of Zipstream is not finished. Axis still strives to improve it every year, by constant development and challenging of their standards.

“In order to stay innovative and carry on, you need to find what the real problems are,” says Xing “

You need to listen to your customers and understand the challenges they face with the equipment. Often engineers lose sight of how their product works, and they focus on issues that seem major to them, but actually don’t affect the customer experience of the technology. You need to keep your mind open, increase your knowledge and make an effort to find new combinations of solutions in order to solve a problem.”

The world's first 1TB industrial-grade microSD card for cloud-managed video surveillance

Micron Technology, Inc. has launched the world's highest-capacity industrial microSD card – micron i300 1TB3 microSDXC UHS-I – to address the edge storage needs of the video surveillance market and other industrial applications.

The new Micron i300 1TB microSD card is based on Micron's advanced 96-layer 3D quad-level cell (QLC) NAND technology, now making it cheaper for small-to medium-sized deployments to have primary storage in the camera compared to a centralised storage architecture. The i300 microSD card enables users of video surveillance systems to capture and store more than three months of high-quality video footage on-device and at the edge.

"Micron's i300 industrial-grade microSD cards for edge storage open the possibility for a broad range of video surveillance as a service deployments that no longer require local network video recorders," said Amit Gattani, senior director of Segment Marketing in Micron's Embedded Business Unit. "Micron's 96-layer 3D QLC NAND is instrumental in helping us deliver 1TB of storage in a microSD form factor and at a breakthrough price point to accelerate edge storage and cloud-based service models."

Intelligence at the edge

VSaaS systems are increasingly integrating artificial intelligence-based and higher-resolution cameras that require more storage at the edge. The Micron i300 1TB microSDXC card allows 24/7 continuous capture and storage of up to 1TB of high-quality video in the camera. Users of video surveillance systems can now store large amounts of video footage on-device, opening a broader set of uses for cloud-managed solutions.

"Demand for commercial surveillance cameras continues to grow at a rapid pace," said Jeff Janukowicz, research vice president at International Data Corporation (IDC). "Smart cameras, artificial intelligence, machine learning and threat detection are being driven to the edge for real-time responsiveness, making Micron's 1TB microSD card an invaluable solution for differentiation and innovation."

Lowering the TCO

The VSaaS market is projected to reach \$6 billion in 2022, according to MarketsandMarkets, corresponding to a growth of 22% compound annual growth rate

„Demand for commercial surveillance cameras continues to grow at a rapid pace.“

between 2017 and 2022. The rising adoption of VSaaS by small to medium businesses and enterprises is attributed to lower overhead costs achieved through ease of installation and elimination of the need for on-site NVRs and DVRs. The ability to store large video footage files in the camera and at the edge reduces the demand for network bandwidth and expenditure associated with continuous cloud storage. These savings contribute to lowering the overall cost of ownership for businesses while bringing flexibility and scalability associated with cloud-based implementation models.



The new Micron i300 1TB microSD card is an important contribution to edge-based storage in VSaaS applications.

"The video surveillance market is quickly shifting toward hybrid cloud architectures that store video footage on-camera, allowing secure access via cloud-based software," said Raj Misra, director of Hardware Engineering at Verkada. "Enterprise customers are choosing hybrid cloud offerings to

in a 24/7, 30 frames per second (FPS) recording environment, offering twice the reliability of hard disk drives at 2 million hours mean time to failure. The card features a smart tool for monitoring the health of devices.

"Vivotek has launched a series of edge-computing network cameras and successfully deployed Micron's high-quality industrial-grade micro SD cards," said Shengfu Cheng, director of Marketing and Product Development Division, Vivotek Inc. "Micron's portfolio of industrial microSD cards up to 1TB equips us to deliver greater flexibility, scalability and maintenance efficiency to our customers, all of which contribute to a better return on investment."

Availability

The Micron i300 microSDXC UHS-I card is offered in 128GB to 1TB capacities and the entire industrial-grade portfolio includes capacities ranging from 32GB to 1TB.

For more information, visit <http://www.micron.com/surveillance>

Strong reliability

Micron's industrial-grade microSD portfolio is designed to endure the harsh environments in which surveillance systems are deployed. The Micron i300 1TB microSDXC card minimizes frame drops

reduce operational costs, simplify installation and management, and gain from powerful video analytics. Micron extending its range of reliable industrial-grade microSD cards to 1TB enables us to provide our customers with industry-leading data retention, security and video resolution options at very cost-effective price points."



Ad by IDB (Industry Development Bureau), MOEA, Taiwan.

IoT Cybersecurity: Taiwan Plans Ahead With Overt Outcome

Since the end of 2017, the Taiwan government has brought together the know-how and resources from the industrial elite, specialists in cyber security, and scholars in the field to work on “The IoT Cyber Security Standards and Testing Specification”, which was officially announced in mid-2018.

Today, its proposition for IP Cameras is certified as being the national standard (CNS 16120: IP Cameras), while regulations on other network-connectable devices are still pending in application. These standards and regulations are made to help Taiwan-based manufacturers to design in discreet cyber security mechanisms within their IP Cameras, NVRs and DVRs.

Having not only contributed an outstanding performance to the fight against the Covid-19 corona virus epidemic, Taiwan has

also worked to create an improved performance in the prevention of hacking of networkable video surveillance devices and systems.

The standards for Video Surveillance System Series (TA-ICS TS0014-1 v2.0—for IP Cameras, TAICS TS-0014-3—for DVR, and TAICS TS-0014-4 v1.0—for NVR) are said to be 72% compliant to the requirements of UL2900, according to III (The Institution for Information Industry), a think tank and R&D organisation for, the Digital Economy, Industrialisation and Talent Cultivation. The standards

and regulations will be reviewed and updated under the supervision of III when any industrial feedback or market complaints are raised.

Based on the latest standards, in working with TAF¹-certified testing labs, TSSIA² Industrial Association has got the governmental project to offer counseling service since 2018. To date, there are Twenty-two (22) Taiwan-based manufacturers (as shown below) received the service in improving the cyber security in design to their IP Cameras (benefit to 200 models+). Among them,

11 companies have successfully passed their products through the strict Lab testing in compliance to the nation's IoT Cyber Security Standards & Regulations.

As the number of cyber-attacks world-wide on IoT devices and consequently on video systems has been much more frequent and is growing at an unprecedented rate, and, bearing in mind, that the continually growing number of IP cameras shipped from Taiwan has reached a figure of 35% – 40% of the total number installed globally. The Taiwan government acknowl-



edged the phenomenon and thus released the IoT cyber security standards and regulations. According to the regulations, there are eight professional testing labs being assessed and certified by TAF to assist customers (including governmental agencies) in supervision, ensure that networkable devices incorporate effective cyber protection and/or meet the nation's standards and regulations.

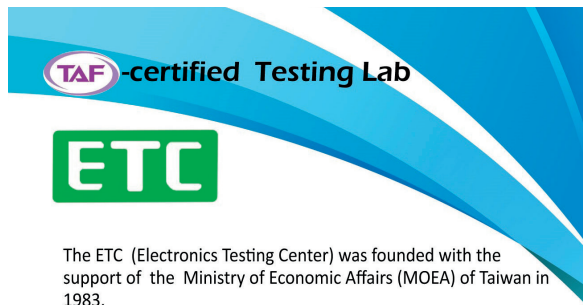
With the experience, the TSSIA will, in working with selected TAF-certified testing Labs, TAICS, and III, as a service

window would like to extend the consultation and testing programme to companies overseas, to help enhance inspection of cyber security performance of products that are assigned for production in Taiwan.

Cyber security in IP Surveillance has been highlighted and recognised as a serious issue throughout the world, the policy will give impetus to the IP surveillance industry in Taiwan, enabling it to enhance its export business to the rest of the globe and also build a 'safe and reliable digital land' in the nation of Taiwan.

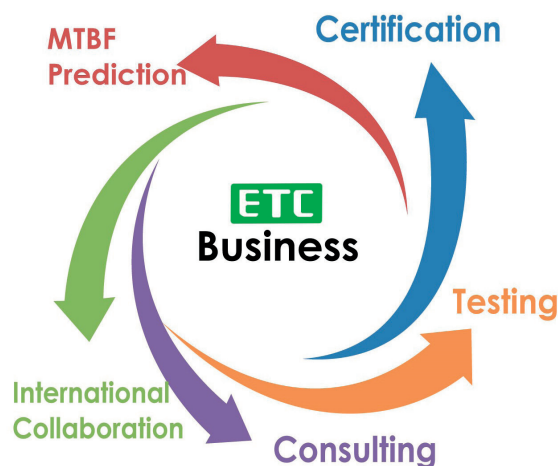
TAF¹, The Taiwan Accreditation Foundation, is the only body in Taiwan recognised by the Government for the accreditation of conformity assessment against international standards. TAF is a full member of ILAC-MRA. The ILAC Mutual Recognition Arrangement (ILAC MRA) provides significant technical underpinning to the calibration, testing, medical testing and inspection results of the accredited conformity assessment bodies and in turn delivers confidence in the acceptance of results.

TSSIA² Taiwan Safety and Security Industry Association(TSSIA) was established since Jan. 2005 with supported by the Industrial Development Bureau (IDB) MOEA in Taiwan, being a bridge between the Government bureau and the industry for cross-domain integration in the Taiwan safety and security industry.



The ETC (Electronics Testing Center) was founded with the support of the Ministry of Economic Affairs (MOEA) of Taiwan in 1983.

The Lab is accredited as a certification body by BSMI, NCC (National Communications Commission) and Taiwan EPA. ETC is also the first non-governmental RPC Certification Body in Taiwan. It is also a designated laboratory for safety and EMC testing.



Test and Improve

**Network-connecting
Cyber Security**

within Your IP Surveillance products/systems



With the Taiwanese governmental projects' support, TSSIA in associate with ETC (TAF-certified testing Lab) offer the testing and consulting service on the IoT Surveillance devices from Taiwan.

International brands and manufacturers, wish to undertake OEM or OBM manufacturing in Taiwan, they will also be able to use the service to get an impartial testing report from us, the certified 3rd party, to assure the cyber security performance of their OEM/OBM products before being shipped, on sales, or applying to projects.

The service will be mainly executed based on the "The IoT Cyber Security Standards and Testing Specification" (for IP Cameras and for NVR/DVR) of Taiwan that are almost 72% compliant to the requirements of UL2900; please scan the QR code (above) to learn more.



Service Window:



**Taiwan Safety & Security
Industry Association
(TSSIA)**

TEL: +(886-2) 2629 1800

Email: tssia.tw@gmail.com

<http://www.tssia.org.tw/en/>



Axis releases anti-ligature corner mount camera

Lund, Sweden

Axis Communications is launching the *Axis Q9216-SLV* network camera, a compact and robust corner-mount camera designed to provide a wide field-of-view and ensure no area is left uncovered.

Available in white and in stainless-steel, this new camera is designed to deliver sharp 4 MP video quality and features wide dynamic range (WDR) for clarity even when there's both dark and

light areas in the scene.

This vandal-resistant IK10+/IP66 rated camera is ideal for high-security installations such as in prisons and psychiatric wards, where it can help prevent self-harm. It features 940nm invisible IR illumination and polygonal privacy masking for flexible coverage and to help ensure occupant privacy is respected. Additionally, for ease of maintenance, the stainless-steel

casing is IP66- and IP6k9k-rated to allow cleaning with high pressure, high temperate water jets. And, the abrasion-resistant two-part front cover is easily removed for more thorough cleaning.

This product offers Axis Zip-stream technology with support for both H.264 and H.265 which significantly reduces bandwidth and storage requirements. Furthermore, signed firmware and a Trusted



This camera is ideal for high-security installations such as in prisons and psychiatric wards.

Platform Module (TPM, FIPS 140-2 level 2 certified) help prevent unauthorised access and safeguard the system. 

POS tool helps retailers detect theft

Montreal, Canada

The new **Genetec** Security Center Transaction Finder, correlates POS data with corresponding video, with the ability to bring in additional sources such as analytics, as an added feature. It eliminates the need to jump between different platforms, and helps investigators filter through large volumes of transactions to quickly detect suspicious activities that might warrant further investigation.

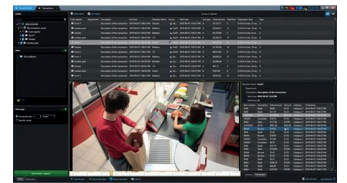
Retail shrink is increasing, and theft tactics are becoming more complex, strategic and internal. According to the National Retail Federation (NRF) 2019 national retail security survey, theft, fraud and losses from other retail "shrink"

continues to rise (totaling \$50.6 billion in 2018, up from \$46.8 billion the year before). To identify theft trends and combat loss, retailers are increasingly turning to technology to put in place effective ways to work smarter and automate their processes to reduce losses and preserve valuable margin.

"Working with a variety of tools and applications to reduce retail loss is a critical aspect of any retail investigator's job. However, the enormous volume of POS transactions to review, combined with the amount of time it takes to manually find the security video associated with potentially fraudulent activity makes this a daunting task.

"With Transaction Finder, we solve that problem by using a single tool that makes it easy to detect theft trends, identify suspicious transactions and locate video of interest," explains Rob Borsch, Practice Leader – Retail and Banking at Genetec, Inc.

Using the Transaction Finder task in Security Center, investigators simply enter relevant search criteria like date and time, employee name, SKUs involved in the transaction, void transactions, or whether motion was detected on the customer side of the register, etc. Transaction Finder will scan the POS database for activities that meet the selected criteria along



Transaction Finder will scan the POS database for activities that meet the selected criteria along with the associated video and the transaction details.

with the associated video and the transaction details. Using customisable dashboards, investigators can quickly identify suspicious transactions, immediately review the associated video for more context, and flag transactions for further investigation. 

Dahua launches Wizsense night-time colour camera series

Hangzhou, China

The new camera series incorporates a large aperture lens featuring an F1.0 super large aperture that collects 2.5 times the amount of light compared with an F1.6 aperture, in turn this creates brighter images. The high-performance sensor offers 30% photosensitive capacity increase through its larger sensor size; and the advanced ISP, *Dahua ISP 4.0*, greatly improves signal-to-noise ratio (SNR) and colour reproduction. Another feature is warm light - the weighted radiance of blue light is 40% below European Union standards, which presents lower light pollu-

tion and less harm to human eyes.

These technological advancements make this series ideal for highly effective performance at night. It achieves 24/7 monitoring by capturing vivid details and presenting coloured images in low light conditions.

At the same time, it provides warm and smart auxiliary light to offer guaranteed image clarity and quality even in total darkness. Built-in AI functions additionally provide higher monitoring accuracy at night, according to Dahua.

With this this new product **Dahua** claims a world first, as it

combines SMD and full-colour for night surveillance, delivering both technologies' advantages to its customers. On the one hand, SMD can easily process visual information collected by the full-colour camera. And on the other hand, the full-colour camera significantly increases the accuracy of SMD at night. In addition, Dahua SMD has the ability to effectively filter false alarms triggered by pets, leaves, branches, raindrops, lights and other irrelevant objects, and only focus on real threats - human and vehicle.

Utilising the two advanced



Dahua Technology's latest solution for smart night surveillance - the Wizsense full-colour series network camera.

technologies, Dahua Wizsense full-colour camera can accommodate a wide range of application scenarios, such as museums, cinemas, factories, villas, schools, etc. Users no longer need to worry about the high cost of patrolling or leaving their property unguarded at night. This solution is fully capable of meeting the demands of ordinary users, delivering a safer and cost-effective solution for night surveillance. 



LET'S WORK TOGETHER FOR A SAFER TOMORROW

Most people dream of a safer society. People like you work on creating one. Skydd, the largest trade fair for Security, Fire & Rescue in the Nordic region, is the meeting place for you and your company. Here you'll take part of exciting news, interesting lectures and the latest technology in cooperation with all of the industry's major players. One thing is for sure: to be a part of a safer tomorrow, this is where your company should exhibit.

OCT 20-22 2020



Latest facial recognition works even with masks

Barcelona, Spain

The company had been working on the issue of partial occlusions for some time and, following the worldwide outbreak of Corona virus (COVID19), development has been accelerated to launch a version of the software that helps provide an accurate identification under these conditions.

Based on deep learning technology, **Herta's** algorithms provide very high identification rates, especially in identity verification tasks and their reliability is very high, even when people hide a large part

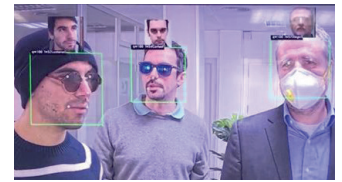
of their face. It is important to remember that the most differential part of the human face is in the eye area.

The launch of this software is key for the identification in automatic passenger control systems with documentation, such as border control with the passport. This way it will not be necessary for the person to remove the mask, avoiding possible contagion or long waiting times. Its application, in general, extends to any type of access control or identity

verification system.

Herta expects that the impact of this new technology in the market will be very important worldwide and that it will be used massively in environments such as transportation, health, government, events, sports stadiums or in the gaming sector.

Herta specialises in the analysis of crowded environments, which allows to detect and identify multiple subjects at the same time through IP cameras. The company's software is designed to be



Herta, has just this week launched a new version of its facial recognition algorithms that can correctly identify people who wear facial masks.

fully scalable and compatible with any IP camera, becoming an easy-to-use and accessible tool for any business organisation.

Eagle Eye releases new anti-tamper analytic

Austin, Tx (USA)



Eagle Eye anti-tamper analytics can be added to existing cameras

Eagle Eye Networks, a global leader in cloud video surveillance, has announced a camera tampering analytic that automatically detects and notifies users if a camera is tampered with.

While camera tamper notifications are not new to the industry, Eagle Eye Networks AI-based approach serves as a differentiator, delivering enhanced accuracy, reliability, and a reduction of false alarms to Eagle Eye Cloud customers.

Common examples of camera tampering include a sudden change to focus, a covered lens or an intentional redirection of the camera's view by physically moving the camera. Without real-time tampering notifications, reaction times to a criminal act may be

delayed, or in a more benign case, accidental camera movements, like employees cleaning, may prevent the camera from capturing later events.

"Eagle Eye Networks is more than a video surveillance platform, it's a business intelligence platform aimed at helping customers improve operational efficiencies while keeping their businesses safe and secure. Eagle Eye Analytics instantly transforms standard analogue and IP cameras into powerful AI solutions, without any additional on-site hardware," said

Dean Drako, CEO of Eagle Eye Networks.

In addition to camera tampering, Eagle Eye Networks offers the following analytics: Line Crossing; People Counting; Intrusion Detection; Object Counting; and Loitering.

The camera tampering analytic is immediately available globally and can be enabled within the Eagle Eye Dashboard on a camera-by-camera basis. Customers do not need to replace their existing cameras to use the Eagle Eye Cloud VMS camera tampering analytic. 

Hanwha releases Wisenet Retail Insight

Chertsey, Surrey (UK)

Hanwha Techwin has introduced a business intelligence application which enables retailers to gain a greater understanding of customer behaviour and buying patterns.

Wisenet Retail Insight utilises people counting, heat mapping and queue management applications running on board selected Wisenet Q and Wisenet X fixed lens and fish-eye cameras to display statistical analytics on a centralised dashboard, along with other practical information such as weather reports.

Accessed from anywhere on the network, Retail Insight is a web based application which consolidates the data captured by the three

analytics applications running on up to 500 Wisenet Q or X series cameras and presents it on a customisable dashboard.

Retailers are able to take advantage of the captured data to measure the impact of advertising, on-line promotions and other marketing activities on the number of people who enter their stores, as well as making best use of human resources in order to manage the peaks and troughs of customer flow at checkouts.

"With revenues and profitability under threat, retailers are understandably looking at ways to improve productivity," said *Uri Guterman*, Head of Product &

Marketing for Hanwha Techwin Europe. "In terms of the business intelligence which could be made available to operations, marketing, merchandising and store management, the metadata traditionally extracted from Electronic Point of Sale (EPOS) systems is unlikely to be sufficient for retailers to identify opportunities to increase productivity or improve the customer experience."

Retail Insight generates reports in a variety of formats including PDF, Excel, CSV or HTML, whilst with the help of five customisable tabbed screens, users are able to view real-time updates on a wide range of activity, including the



Hanwha Techwin has introduced a business intelligence application which enables retailers to gain a greater understanding of customer behaviour and buying patterns.

number of store visitors for any particular time of day or accumulatively over a specified period of time, as well as data on queue congestion times and heat mapping information showing the busiest areas of a store. 

Motorola brings facial recognition to VMS

Chicago, IL (USA)

The video management software *Avigilon Control Center (ACC) 7.6* – the newest addition to the **Motorola** video security and analytics portfolio. It enables enterprise customers to better monitor their facilities through new AI-powered facial recognition features and analytics. The new video management capabilities include robust controls to govern the retention and accessibility of watch list data, the ability to create and manage multiple watch lists from within ACC and the option to upload reference images to a watch list. These features are built into the solution natively, meaning that the technology is developed and owned by Motorola Solutions as opposed to a third-party vendor.

In addition, the new facial recognition capabilities do not make consequential decisions or initiate actions on their own. The data that are entered and saved in the watch lists are managed and maintained by the enterprise customers employing the technology.

ACC 7.6 features also “Unusual Activity Detection” analytics that provide site-wide



ACC 7.6. enables enterprise customers to better monitor their facilities through new AI-powered facial recognition features and analytics.

intelligence with the ability to recognise out-of-ordinary activity such as unusual speed of movement or location of people or vehicles. This edge-based intelligence distinguishes between typical and abnormal events by continuously learning what usual activity might be for a scene over time. For example, if there is an individual running through a crowded mall, a security guard could be alerted in Focus of Attention to locate where the individual is and take measures to understand the situation.

Axis enters body worn camera market

Lund, Sweden

Axis Communications has launched a body worn camera solution, designed on an open system architecture, which enables integration with a broad range of video management systems (VMS) and evidence management systems (EMS).

The scalable Axis body worn solution can be used with a third-party VMS and EMS, on-premise or in the cloud, allowing for integration with other video surveillance data. It can also be delivered as an end-to-end solution, using Axis Camera Station, the company's own VMS software.

The new Axis body worn camera system features a camera, a docking station (8-bay or 1-bay); and a system controller.

The camera captures video up to 1080p @30fps and audio through dual microphones for noise suppression capabilities. Wide dynamic range technology is employed to guarantee image quality in even the most challenging light conditions, while Axis Zipstream reduces the



The new Axis body worn camera captures video up to 1080p @30fps and audio through dual microphones.

demands for storage. Battery power is designed to cover 12 hours of normal usage and the capability for charging in-car or from a power bank.

All data is encrypted both at rest and in transfer using AES256 and TLS. In addition, video data can be fully end-to-end encrypted with specific integrations. 

ASSA ABLOY
Opening Solutions

eCLIQ:

The key to
electronic
locking



eCLIQ is a durable and secure electronic locking system utilizing web-based software

campaigns.
assaabloyopeningsolutions.eu/cliq

Experience a safer
and more open world

Smart thermal design tool aids camera selection

Hoofddorp, The Netherlands

Hikvision has launched a new online thermal design tool to help distributors, integrators and end users to find the right thermal camera for the right position in their solution.

The free tool streamlines the process of designing a solution and preparing a quote. Use of online GIS map data gives accurate data that provides the correct scale, so frustrating scale issues are avoided. Importantly, it saves time because there's no need to use a map manually and adjust field of view to make the right calculation. *The Thermal Design Tool* automates all of this. If map data is not yet avail-

able for a site, the tool will still be able to provide a 2D version.

The tool creates a professional report quickly, which makes a technical solution very clear and easy to reference. This also means it can be used to present to a customer. Adjustment of plans can be done quickly to meet the customer's needs, and the impact of any change is easy to see immediately.

This will come into its own for solutions involving perimeter protection. It is also useful in scenarios which warrant cameras with fire detection (for example forest fires) and fire prevention with



The free tool streamlines the process of designing a solution and preparing a quote.

temperature measurement.

"Our new Thermal Design Tool takes the hassle out of designing a thermal solution, making it quicker and simpler to build a solution and to quote", says Franck

Carette, Thermal Product Manager for Hikvision Europe. "Because the tool is now online, there's no need to install or update anything. This will make it a handy tool for installers and end users alike." **swm**

Vanderbilt agrees new integration partnership

Indianapolis, In (USA) and Wiesbaden, Germany

Vanderbilt has entered into a new partnership with Dutch-based company, Logitime International, a provider of a complete and integrated solution for access control, time and attendance, and shop floor data collection.

The Vanderbilt partnership centres around the integration of Vanderbilt's VR40 OSDP Readers with Logitime's Time and Attendance (T&A), Access Control, and Shop Floor Data Collection software solution.

Logitime solutions' primary function is to deliver a fully customisable and interactive access control product to their customers. As such, Vanderbilt's VR40 Readers, which are supported by OSDP, fit perfectly into this customer-first model.

Logitime's T&A software is designed to be a fully integrated programme. This enables Logi-



The Vanderbilt partnership centres around the integration of Vanderbilt's VR40 OSDP Readers with Logitime's software solution.

time to provide a tailored solution for each unique customer. Vanderbilt's VR40 Readers fit into this mix by complementing Logitime's goal of being interactive and customisable. This is because the VR40 Readers come with a display screen that allows Logitime to integrate and customise the messaging being displayed to their intended audiences on a customer-by-customer basis.

Speaking on the integration, *Alexandre Prinsen*, Senior

Consultant at Logitime, explains: "At Logitime, our interactive technology is a crucial component for us. Therefore, being able to work with Vanderbilt's VR40 OSDP Readers and customise our messaging in their display screens is, of course, an excellent match for us."

"The Vanderbilt VR Readers are very suitable for highly technological environments that need or want the feedback within their access control systems. We can even use them as T&A readers," Prinsen concludes.

Commenting on the partnership from Vanderbilt was *Nick Pegtol*, Country Manager for Benelux at the company. "As well as being attractive and robust, Vanderbilt's VR40 OSDP Readers introduce dynamic features and an OLED display to simplify installation and in-service func-

tionality. Our VR40 readers have three indicator LEDs and a multi-tone buzzer for audio verification. A multi-colour light frame enforces access status information. This can be configured to follow the indicator LEDs or any number of different options. Display brilliance is set automatically by an inbuilt light sensor."

"Aesthetics aside, one of the key features of our VR40 Readers is the inclusion of the highly secure OSDP (Open Supervised Device Protocol) to help combat people hacking communications. OSDP ensures that sniffing devices cannot be installed behind the reader or along the communications path, which we also believe strongly aligns with Logitime's goal of producing customer-orientated solutions," Pegtol summarises. **swm**

New cost effective I-Pro from Panasonic

Rolling Meadows, IL (USA)

The latest *Panasonic I-Pro Sensing Solutions* offer a new option of economically priced U-Series network cameras. Designed for SMB, schools, and numerous other applications, the new U-Series cameras have many of the features found in the company's flagship

I-Pro Extreme Series cameras at economical price points.

The U-Series includes thirteen models in indoor and outdoor dome and bullet camera configurations with fixed or varifocal lenses, 2MP and 4MP models. Features include: H.265 compression and

smart coding to increase bandwidth efficiency and reduce storage requirements; colour night vision for use in low-light conditions; and IA (Intelligent Auto) and Super Dynamic functions for enhanced dynamic range in scenes with varying lighting conditions. Ad-

ditionally, U-Series cameras are bundled with I-Pro Video Insight 7.6 VMS software and feature a five-year warranty, which positions them to aggressively compete in a price-sensitive market category when it comes to total cost of ownership. **swm**

New U-series cameras from Panasonic I-Pro.



Cliq Web Manager can now control more than access

London, UK

No matter what the nature of a business, the Cliq Web Manager is designed to help manage its access control quickly and efficiently. Now businesses can also integrate its powerful access management features with their existing business process software. Thanks to the Cliq Web Manager's open architecture, a single interface can now be created to control everything.

Cliq Web Manager can help streamline everyday operations, while also managing a Cliq key access control system to its full potential. Integration works in two distinct ways, the Cliq Web Manager can plug directly into an existing platform, making access control one node in a current control panel. And, there is an SDK, so if they wish businesses can add Cliq Connect remote access control manage-

ment to a company app.

Alternatively, Cliq Web Manager can be the hub for multiple business processes. Businesses can manage HR, support ticketing, financial reporting and more alongside daily access control tasks like validating and revalidating credentials, cancelling lost keys and ordering automated audit trails for locks or users.

With Cliq Web Manager web services, a comprehensive, cus-

tomised integration with existing software can be built to help the business operate more efficiently.

Time- and cost-saving measures are baked into every Cliq Web Manager integration. Cutting back data double-entry reduces database errors and minimizes tedious data entry. Internal workflows in security and beyond are streamlined when one interface enables an answer multiple questions.

Plus, businesses can choose a customised solution with a format that best suits the business when integrating the Cliq Web Manager with existing software.

If a Cliq Web Manager Software as a Service (SaaS) package is selected further economies can be made on IT. Security infrastructure budgeting becomes more predictable and data enjoys complete



The Cliq Web Manager is designed to help manage its access control quickly and efficiently.

redundancy. Additionally, the Cliq software is always, automatically up to date – a bonus for cyber-security resilience.

Cliq Web Manager enables a wide range of controlled security workflows, including real-time access control management. Now it integrates easily with all kinds of business software, helping businesses to work smarter, too.

vario2 HYBRID ONE PRODUCT TWO ILLUMINATORS



Outstanding
Performance

Combined White-Light
and Infra-Red

IP Enabled

rayTEC[®]
www.rayteccctv.com



Perimeter security: The m

Perimeter security continues to be something that is widely talked about in the physical security industry and the market is expected to continue to grow at almost eight percent per year until 2025. Detektor International has met up with a number of experts to discuss the market, technology and the future.

The customer requirements: reliability, integration and low prices

The solutions for perimeter security must be reliable and be able to be integrated with video surveillance.

“A couple of years ago we saw just a fence alarm or just a camera with video analytics in it, today it is a combination of technologies”, says Erik Nord, Sales Engineer at Genetec.

By Henrik Söderlund

According to market research company Research and Markets, the global market for perimeter security will reach 29.6 billion dollars by 2025. This represents an annual growth rate (CAGR) of 7.7 percent.

A changing market

Kertil Stenberg, CEO for Stanley Security in the Nordics, believes that the market for perimeter security has changed a lot in recent years.

“We have moved more and more towards high technology solutions, radar has developed a lot as well as video surveillance”, he says.

Kertil Stenberg also points out that video analytics has been used for a long time for perimeter security, but previously there were major problems with false alarms. In recent times, there have been new developments in video analytics and accuracy has improved significantly.

“Having said that, you do not want to take 100 per cent of false alarms away because then you risk taking away some of the real ones too”, he says.

Jimmy Ek, Nordic Sales Manager at Axis Communications, stresses that a larger variety of products and sensors for perimeter security are being integrated today. Radar, thermal cameras, laser detectors and drones in collaboration with security guards are some examples. And there is more focus on solutions rather than on individual products.

Higher quality and lower price

Mark Cosgrave, Division Manager for Western Europe at Optex, also believes the market has changed, and that goes both for the sensors and end user requirements.

He says: “They want reliability, they want to protect what they have and that we can provide”.

Nicolas Jdanoff, Business Development Manager for Europe and Northern Africa at the Italian perimeter security manufacturer Cias, stresses that IP solutions is a must have and that everything needs to be completely integrated with third party systems like video management systems.

“The market is always calling for higher quality, sometimes at lower prices, which is a paradox. We are trying to bring detection performance and lower the rate of false alarms by improving the quality of the algorithms,” he says.

Björn Bäck, Pre-Sales Engineer at Hikvision, thinks that the biggest changes in the market are that the price has decreased and the technology is more accessible and the security cameras are so efficient now that they are good solutions both during day and night and also during winter time without creating false alarms.

Johan Elliott, Business Development Manager at Bosch Building Technologies, says that high quality video analytics is dominating the market and that the customers have more confidence in it than in more traditional



The solutions for perimeter security must be reliable and be able to be integrated with video surveillance.

perimeter security technology such as fence alarms.

The customers and the demand

Jimmy Ek thinks that industry applications, factories and logistic centres are the three most common examples of businesses that require perimeter security.

“But then there is perimeter without any hard fence, like schools for example”, he says.

High security facilities such as power stations and other critical infrastructure, as well as airports, military bases and prisons are some other examples where perimeter security is important. Often, it is about monitoring the outer perimeter. Public transport with train stations and metro is another example, where it is about detecting whether someone enters the train tracks or gets pushed down on to a track.

But there can be a great variation in customers and applications for perimeter security. Imagine an airport: it has many different types of areas that require different levels of security. Everything from car parks outside the airport, to runways and areas where unauthorised people should definitely not have access, to the terminals themselves which more or less function as

shopping centres.

“What customers demand in the first place is reliability. Early warning is the other thing as well. It is desirable to detect somebody when they are on the outside, of course, that is what people really want”, says Mark Cosgrave from Optex.

Early detection is crucial

Björn Bäck from Hikvision believes that customers primarily demand efficient technology that detects and reports what is happening. Johan Elliott believes that a typical customer, such as a logistics centre, often has problems with intruders trying to steal things at night.

“Customers want to detect people that come close to the fence, they want to see them, and they want to receive an alarm”, he says.

Early detection is very important since it makes it possible to react before an intrusion takes place and thus completely avoid any damage.

Jimmy Ek says: “End customers want to keep people outside the premises, they want to control who is coming in. Perimeter is important for many companies. They understand how much value is at risk if someone breaks in and steals things or causes a downtime.”

arket and the technology

Will cameras take over the market for perimeter security?

How will perimeter security look in the future? Most of the experts that Detektor and securityworldmarket.com met up with believe that cameras will not take over completely, but there are exceptions.

By Henrik Söderlund

Video surveillance is the segment within perimeter security that the market research company Research and Markets believes will grow most in the next five years.

Ketil Stenberg, CEO for Stanley Security in the Nordics, says: "Video technology and video analytics are developing with a kind of artificial intelligence and radar is another technology that is growing and drones are becoming more common too. There are several different kinds of technology, but none of them is a silver bullet."

He also says he is 100 per cent sure that security cameras will not totally take over the market for perimeter security, although they will play an increasing role with more machine learning/ artificial intelligence.

"But only to a certain extent, because even though if you have fantastic analytics around, the systems can be deceived one way or another. I think radar is interesting, it was developed during World War II and the technology itself has not developed that much since then, but now radar is really coming back. Radar was not as big in the private security industry ten years ago as it is today – some things that you think might decline are actually coming back", he says.

Layer on layer

Perimeter security is often described as layer on layer, much like an onion. And different layers may require different technical solutions.

Jimmy Ek, Nordic Sales Manager at Axis Communications, stresses there is no single solution or product that can solve all of the end customer needs for perimeter security.

He says: "We see the biggest growth in the big area inside the

outer perimeter. You might want thermal cameras to monitor the outer perimeter and inside you may want radar. And you want these different technologies to work together."

Erik Nord, Sales Engineer at Genetec agrees:

"Just like with everything else, we have to ask what the customer wants to achieve – what is the problem and how can we raise the security level", he says.

Tailored solutions

Mark Cosgrave, Division Manager for Western Europe at Optex, wishes there was one solution for all perimeter security, but he says there is not.

"We have over 2,000 different types of sensing solutions, and the reason we do that is so we can customise our solution to the end user's requirements and give them the very best solution", he says.

Nicolas Jdanoff, Cias' Business Development Manager for Europe and Northern Africa, believes that perimeter security must combine qualitative sensors that provide reliable information and that a video surveillance system then can verify/

„We are only at the beginning of AI and it will develop a lot in the future.“

confirm what is happening.

He says: "There is not one solution that fits all sites or all constraints. A typical perimeter security solution needs to be engineered and designed depending on constraints on each and every site. There might be harsh weather conditions, sandstorms or physical human industry or activity next to it."

Nicolas Jdanoff sees no reason why only video surveillance should be used for perimeter protection,



Mark Cosgrave, Optex.



Nicolas Jdanoff, Cias.



Ketil Stenberg, Stanley Security.



Jimmy Ek, Axis.

now or in the future. He says: "It is hard to believe that cameras will be able to replace efficient perimeter security solutions especially in very large sites and in difficult environments."

Improved video analytics

Johan Elliott, Business Development Manager at Bosch Building Technologies, has a greater belief than the other industry professionals that Detektor International talked to, that video surveillance

and video analytics will take over the market.

He says: "There will always be special customers with certain environments, but you always need to be able to verify what kind of intrusion is happening. So, yes, I think cameras will take over."

Johan Elliott believes that one can rely on video analytics for perimeter security but that there are some special conditions when it does not work as well.

"Outdoors, thermal cameras are the best option for avoiding shadows from cars and anything else that passes by. But regular security cameras work well today compared to a few years ago", he says.

Technology and people

Jimmy Ek at Axis is more sceptical and thinks video analytics sometimes is overestimated. He says: "Many companies are talking about AI and deep learning, and yes, video analytics can do more today than it could do before, but much of it is about teaching the analytic to trigger on certain things and not on others. We are only at the beginning of AI and it will develop a lot in the future."

Ketil Stenberg believes that technology itself is never enough – security guards are also required. He says: "Security guards and technology do not compete with each other, good technology sends the security guards to where they are needed, and this also applies to police and military – good security technology can show where they are going and what is waiting for them there", he says.

A nimble and reassured perimeter surveillance solution

Compared to conventional sensor-based alarm systems, a surveillance system that utilises cameras has several advantages: The ability to watch events in real-time, obtaining key data around those events, and providing solid and accurate evidence for law enforcement. Hikvision Acusense technology provides just that!

Empowered by deep learning algorithms, Acusense technology distinguishes people and vehicles from other moving objects. The result is a striking reduction in false alarms – now with an accuracy approaching 98%. In this way, security personnel can focus on genuine security issues and take action.

There are many application scenarios where Acusense technology helps create that “sense of safety”.

Residences

Whether people choose to keep an eye on their houses themselves or hire professional service providers to do it, there are two functions they can rely on with Acusense:

Prompt notification via smartphone – it’s always good to have first-hand information to check on the safety of properties. When applied with AcuSense, they’ll get a notification on the App or via SMS when an alarm is triggered.

Light and sound intruder deterrence – cameras with Acusense can be set to react to intrusion events with a flashing light and customisable siren, alerting any would-be intruder that they are

being monitored and have already been spotted.

Restricted areas

Restricted areas or dangerous areas usually have signage to warn about danger. However, people ignore these signs from time to time, resulting in serious consequences, trespassing in high-security zones. With an Acusense camera, property owners or administrators can customise an audio message to be sent when the camera detects someone attempting to enter the area.

Factories

Factories and warehouses store high-value raw materials or commodities. Security here is crucial. However, using manpower for 24 hours patrolling is no easy task. With Acusense technology, those facilities are able to:

Replace security patrols with camera monitoring – Acusense technology greatly improves perimeter monitoring efficiency and ensures that limited human resources can be deployed only where most needed.

Have accurate trespassing alarm for human targets – factories and warehouses mostly deal



with human intrusion events, which might turn into burglary or vandalism. Accordingly, Acusense devices can be configured to send alerts only upon the detection of a human intrusion.

The latest generation of Hikvision Acusense products deliver:

- Improved alarm accuracy, now approaching 98% powered by an upgraded deep learning algorithm to analyse live video streams and label them as “human,” “vehicle,” or “other events.”
- Enhanced motion detection with human / vehicle classification. Products are designed to integrate human and vehicle classifications with motion detection, so customers can enjoy the same

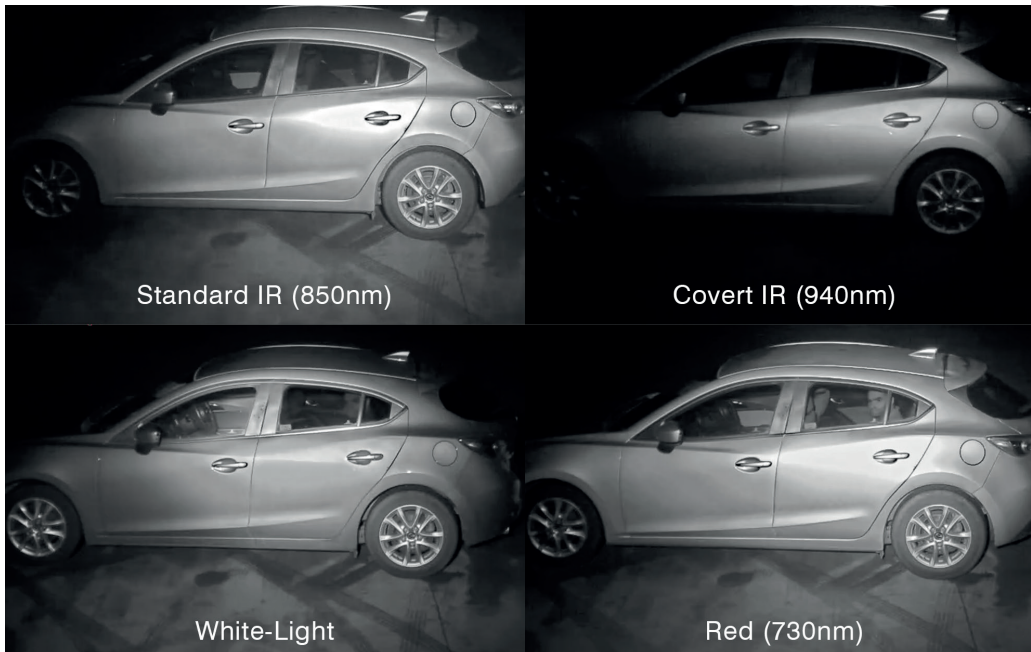
level of alarm accuracy afforded by Hikvision’s Acusense technology.

- Flashing light and two-way voice conversation. Security personnel can communicate with the person who triggered the alarm to confirm their authorisation, thanks to the built-in speaker and microphone in the camera.

- Better performance in low-light environments. The latest Acusense camera lenses are equipped with an aperture reaching up to F1.4, allowing more light to enter the lens for optimised image brightness.

- Larger detection area. The new generation of Acusense products extends target classification distances to 20, 25, or 30 metres, depending on the model.

“Hikvision introduced its cutting-edge Acusense technology in its EasyIP product line in 2018, with the idea of making intelligent alarms and services available to small businesses and residential customers for the first time,” says Frank Zhang, President of International Product and Solution Centre at Hikvision. “In a nutshell, Acusense technology enables security personnel to focus on human and vehicle events rather than insignificant objects, so they can act more efficiently which helps save time and costs, while end users can get full control of their security system anytime, from anywhere.”



Passenger recognition test with different wavelength illumination on a tinted rear window – 730nm provides the best result.



The driver recognition test revealed that three out of four wavelength examples delivered fairly good level of details inside the vehicle. However, the Covert IR (940nm) delivered significantly worse images.



When zooming for a closer look, 730nm provided the greatest level of detail.

730nm – a new solution for driver recognition results

An increasing number of transport applications around the world are trying to identify drivers and passengers inside a vehicle. In this article, Callum Ryder, Marketing Manager at Raytec explore the difficulties of seeing through the windscreen, and discuss how different wavelengths of light could help to overcome the issues.

Modern windscreens block out certain wavelengths of light to protect the occupants of the vehicle from ultraviolet (UV) rays and to keep the cabin cool by blocking infrared (IR). However, the filters do not block all IR rays which means IR can still be used for these applications.

One option is to use more power, but this can be expensive and uneconomical.

Overcoming the challenges

In a series of night-time tests using a high-performance camera, we tested four different wavelengths of light (all using the same power) to see how well they performed. The wavelengths tested were standard IR (850nm) Covert IR (940nm), White-Light and Red (730nm).

Looking at the images above,

we can see that each type of light achieves different results. Although the power of each illuminator is the same, the different wavelength of each means varying levels of light are able to pass through the windscreen. Let's summarise the results;

- With standard IR (850nm), the image shows a fairly good level of detail inside the vehicle, helped by the fact the camera is highly sensitive to this wavelength.

- Aside from the Covert IR (940nm), which delivers significantly worse images, at first glance, the other images do not appear to show a huge difference.

- However, when we zoom further in, we can see that 730nm does provide a greater level of detail.

In more challenging applica-

tions, perhaps when the car is moving at speed, the difference in quality is likely to be more pronounced.

Tinting is an additional challenge as it blocks even more light. In the UK, 75% of light must be able to pass through the windscreen, although other countries have more lenient laws. However, darker tints can generally be used on rear windows, which makes identifying passengers through rear windows particularly difficult. Let's look at the results of our different wavelength illuminators on a tinted rear window.

Here, the results are more obvious as the 730nm wavelength provides the best results. We can summarise that; while image clarity can be improved by increasing the quantity of light, using a more appropriate wavelength can also impact the quality of an image. However, we also need to consider the impact of light on the driver.

Other considerations

Ideally, the quality of images produced using 730nm could be achieved using an illuminator

which gives off no visible light. In reality, as we move further down the spectrum, more light becomes visible to the driver.

Covert IR (940nm) gives off no visible light, but the images are poor. With standard IR (850nm) the quality of the images are good, but there is a visible red glow. Lastly, 730nm achieves excellent quality images with detail of the individual in the car, but there is a very obvious red glow.

Product development

The deployment of driver and passenger recognition is a hot topic, and the uptake of these systems is very much application and country specific. While it is premature to claim that using 730nm illuminators will provide the best results for all driver and passenger recognition scenarios (more testing across a wider range of conditions is required to prove its effectiveness), the idea of using different wavelengths of light to provide improved results is certainly a topic for further exploration.

Callum Ryder,
Marketing Manager at Raytec

Security Center for Airports — perimeter surveillance and much more

The Genetec Security Center for Airports is a new solution designed to help airports of all sizes manage and optimise their security and airport terminal operations. It enables security managers, control room operators, terminal and ground handling staff as well as passenger experience managers to work together using a single unified product tailored to their unique needs.

Security Center for Airports has been designed to empower customers to create a safer environment, improve airport operations, enhance passenger experience, while reducing the overall costs of operations and increasing non-aviation revenues.

David Lenot, Airport Practice Leader at Genetec, points out that airports traditionally would have to work with a multitude of single-purpose products that don't interconnect to build their global security operations centres.

"This would often create a very complex operating environment

leading to slow security response time. But with the growing volume of passengers, airports need help to guarantee safe travel, and many airport security teams are rethinking their security technology strategy," states David Lenot.

"With Security Center for Airports, control room operators, terminal operations, and ground handling can all work in sync to ensure their airport runs like clockwork."

Daniel St-Pierre, Deputy Director, Operations & IT Security at Aéroports de Montréal, knows all about the demands on an airport.



Security Center for Airports is a new solution designed to help airports of all sizes manage and optimise their security and airport terminal operations.

"From parking, shopping and dining to check-in and take off, our airport, like any other, must provide a safe and efficient experience for travellers," he states.

"The Genetec unified platform helps us make the passenger journey seamless while also improving operations and making the airport a safer environment for everyone that passes through our doors."

An "all inclusive" solution

In addition to video management

(Security Center Omnicast), access control (Security Center Synergis) and Automatic License Plate recognition capabilities (Security Center Autovu), Security Center for Airports features a number of airport-specific capabilities including Security Center Flight Business Logic, Security Center Boarding Route Management, Security Center Restricted Area Surveillance and Security Center Passenger Analytics.



Keep yourself informed about the global security technology market

Now it is available:

"The Physical Security Business 2019 to 2024"

This report from the market research company Memoori offers an insight into the global market for Access Control, Intruder Alarm/ Perimeter Protection & Video Surveillance.

How big are the various sub-sectors in the electronic security system market?

What are the trends? What impact do business acquisitions, AI and the development of IoT have on the market? These are just examples of questions this 350 pages report covers.

● Order the report online:

www.armedia.se (click on "Reports") or info@armedia.se

armedia
...we are security

AR Media International AB, Västberga Allé 32, 126 30 Hägersten, Sweden, www.armedia.se



📍 Villas

💬 "I instantly get alerts and can check with my phone when someone walks into my yard."

Intrusion Detection and Deterrence for Home Security

FOCUS *and* ACT

Now, pay attention
only to what matters

HUMAN and
VEHICLE events



Accurate Trespass Alarm, 24 Hours a Day

📍 Factories

💬 "Now I get notified when people are entering the premises, not when a cat runs into the area."



📍 Restricted Areas

💬 "It's great that I can use my security camera to verbally warn anyone who approaches the area."

Customizable Visual and Auditory Warning

Now, with
AcuSense Technology,
network cameras, NVRs, and DVRs:

- Vastly reduce false alarms through human & vehicle classification
- Search targets quickly using sorted human & vehicle video clips
- Perform real-time deterrence using flashing light and custom auditory warning



For more information,
please visit our
AcuSense page.

HIKVISION®
www.hikvision.com

Security Events Calendar

May

 **7-9 May**
Secutech India – Bombay, India
Venue: Bombay Exhibition Center, Mumbai
Organiser: Messe Frankfurt New Era Business Media (MFNE)
Tel: +886 2 8729 1099 ext 531
Email: Israel.gogol@newera.messefrankfurt.com
Website: www.secutechindia.co.int
w.ifsec.events/international/

June

 **30 June – 1 July**
Securix West Africa 2020 – Lagos, Nigeria
Venue: Landmark Centre
Organiser: Montgomery Group
Tel: +44 (0) 20 7886 3048
Email: ben.dale@montex.co.uk
Website: www.securixwestafrica.com/

July

 **20-20 July**
ISC West 2020 – Las Vegas, United States
Venue: : Sands Expo
Organiser: Reed Exhibitions
Tel: +1 203.840.5602
Email: inquiry@isc.reedexpo.com
Website: www.iscwest.com

August

 **20-22 August**
Secutech Vietnam – Saigon, Viet Nam
Venue: Saigon Exhibition & Convention Center (SECC), Ho Chi Minh City
Organiser: Messe Frankfurt New Era Business Media (MFNE)
Tel: +886 2 8729 1099 ext 531
Email: Israel.gogol@newera.messefrankfurt.com
Website: www.secutechvietnam.com

September

 **8-10 September**
Ifsec – London, United Kingdom
Venue: ExCel London
Organiser: UBM
Tel: +44 (0)20 7921 8166

Email: ifsecustomerservice@ubm.com
Website: www.ifsec.events/international/

 **22-23 September**
The Security Event – Birmingham, United Kingdom
Venue: NEC Birmingham
Organiser: Nineteen Group
Tel: +44(0)203 790 7370
Email: tristan@thesecurityevent.co.uk
Website: www.thesecurityevent.co.uk

 **22-25 September**
Security Essen – Essen, Germany
Venue: Essen Fair venue
Organiser: Messe Essen
Tel: +49 (0)201 72 44-524
Email: julia.jacob@messe-essen.de
Website: www.security-essen.de/impetus_provider/

 **27 September – 2 October**
Intersec Building – Frankfurt, Germany
Venue: Frankfurt am Main
Organiser: Messe Frankfurt Exhibition GmbH
Tel: +49 697575-0
Email: intersec-building@messefrankfurt.com
Website: www.intersec-building.com

October

 **12-14 October**
OFSEC EXPO 2020 – Muscat, Oman
Venue: Oman Convention and Exhibition Centre
Organiser: Muscat Expo LLC
Tel: +968 24 788 476
Email: info@muscat-expo.com
Website: www.muscat-expo.com/ofsec/

 **21-22 October**
Sicherheits Expo – München, Germany
Venue: MOC Munich
Organiser: NETCOMM GmbH
Tel: +49 (0)89-88 94 93 70
Email: info@netcomm-gmbh.de
Website: www.sicherheitsexpo.de

 **20-22 October**
Skydd – Stockholm, Sweden
Venue: Stockholm Fair ground (Stockholmsmässan)
Organiser: Stockholm Fair
Tel: +46 8 749 4100
Email: info@stockholmsmassan.se

Website: www.skydd.net
Visit AR Media at Skydd

November

 **10-12 November**
PSecurexpo East Africa – Nairobi, Kenya
Venue: Sarit Exhibition Center
Organiser: Montgomery Group
Tel: +44 (0)20 7886 3039
Email: Gemma.Hore@montgomerygroup.com
Website: www.securexpoeastafrica.com/

 **18-20 November**
Securix Pozna – Pozna, Poland
Venue: Poznan International Fair
Organiser: Poznan International Fair Ltd.
Tel: +48 (0)61 8692000
Email: karolina.greiner@grupamtp.pl
Website: www.securexpl/en

 **25-27 November**
Secutech Thailand – Bangkok, Thailand
Venue: Bangkok International Trade & Exhibition Center (BITEC), Bangkok
Organiser: Messe Frankfurt New Era Business Media (MFNE)
Tel: +886 2 8729 1099 ext 531
Email: Israel.gogol@newera.messefrankfurt.com
Website: www.secutechthailand.com

December

 **1-2 December**
Sectech Denmark – Copenhagen, Denmark
Venue: Bella Center
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Email: deniz.baykal@armedia.se
Website: www.sectech.nu
Visit AR Media at Sectech Denmark

January 2021

 **12-14 January**
Eliaden – Lillestrøm, Norway
Venue: Norges Varemesse
Organiser: Eliaden
Tel: +47 23087700
Email: post@eliaden.no
Website: https://eliaden.no/

Classified Ads

Access Control



Touchless Biometric Systems AG

Rietbrunnen 2, Pfaffikon SZ,
 CH 8808, Switzerland
 Tel +41 (0)55 533 20 00
 tbs@tbs-biometrics.com
 www.tbs-biometrics.com

Perimeter Protection



Manufacturer of perimeter protection systems

Forteza, JSC
 Tilzes str. 38, 91112 Klaipeda
 Lithuania
 Phone +370 46 441195
 forteza@forteza.com
 www.forteza.com

Perimeter Protection



TAKEX Europe Ltd.

Aviary Court, Wade Rd, Basingstoke,
 Hampshire RG24 8PE, UK
 Tel +44 1256 475555
 Fax +44 1256 466268
 sales@takex.com • www.takex.com

Security Trade Press



Do business in Denmark



SECTECH
EXPO & SEMINARS/DENMARK
COPENHAGEN 1-2 DECEMBER 2020

The Sectech 2020 event – featuring exhibition and seminars – will take place in Copenhagen on the 1st–2nd of December at the newly renovated premises of Bella Center.

At this compact event over two days security professionals from all over Denmark will gather to see the latest innovations within security technology presented by exhibitors whether it is intruder alarms, video surveillance, access control and integrated security solutions.

As usual, the exhibition space is limited to about 30 exhibitors who will receive about 1,000 high quality professional visitors over two days. As a security solution provider of importance, you should book your booth now – before it is too late.

Book your stand now!

For reservation please contact:

Deniz Baykal, Mobile: +46 73 987 53 33, deniz.baykal@armedia.se

www.Sectech.dk

Arrangeres af:

armedia
...we are security



Stockholmsmässan

Mediapartnere:

DETEKTOR
SOLICARD

security
WORLDMARKET.COM

Entrance sponsor:

seriline

AR Media International, Västberga Allé 32, 126 30 Hägersten, Sweden, Tel +46 8 556 306 80, www.armedia.se, www.sectech.dk



THERMAL DEEP LEARNING TURRET CAMERA BEFORE IT EVER HAPPENS



Temperature exception alarm
with visualised smart warning



Vigilant smoking detection
helps to detect smoking
behaviours in the first place



Video Content Analytics
with deep learning algorithms
to filter out false alarm



Picture-in-picture preview saves
efforts on switching between
optical and thermal channels