

DETEKTOR



International

Publisher's comment

The industry needs to step up against cyber threats

The Security Technology Market

The global security technology market recovers quickly

Business news

Motorola acquires Ava Security

Product news

New certified cameras for hazardous areas

SPECIAL EDITORIAL FEATURE 1:

ACCESS CONTROL SYSTEMS

–The cloud, mobile solutions and the critical role of identity

SPECIAL EDITORIAL FEATURE 2:

PERIMETER SURVEILLANCE

–About today's technology choices, AI and the threats from drones

What's on in the Security Industry?

– We keep track of what's happening!



www.securityworldmarket.com



**– a world-class information source for
the security industry since 1998**



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: 3F., No. 197, Xinshih 3rd Road
Sec. 2, Tamsui District (251), New Taipei,
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 €25
+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

Printall, 2022



Lennart Alexandrie, Publisher

The industry needs to step up against cyber threats

The brutal war in Ukraine has already had a huge global impact, politically and economically. The concerns over potential escalation and expansion of the war are real, and have relevance. A third world war is the last thing we need.

But in a sense, the conflict has already expanded to a global war, even though it is not being fought on the physical battlefields. While Russian hackers have a long history of state-sponsored cyber attacks, Ukraine has gained support from many white hat hackers and hacktivists since the invasion.

The cyber attacks against Russia or Ukraine are massive and the origins of the attacks are from all over the world. According to a recent report from the IT-security company Atlas VPR, 89% of the cyber attacks worldwide are targeting Russia and Ukraine. According to the same source, cyber criminals launched 70% of cyber attacks on Russia. A total of 5 billion attacks were inbound to Russia on March 5th, writes Atlas VPR.

Atlas VPR refers to data gathered from Imperva Daily Cyber Threat Attack Map statistics and claims that threat actors targeted Ukraine in 19% of cyber attacks. Just a few days before the war outbreak, Russian hackers brought down the websites of the Ukrainian Defense Ministry and the two largest banks in Ukraine with DDoS attacks. Another DDoS attack took down multiple government, military, and bank websites on the 23rd of February.

However, the focus on Russia and Ukraine does not mean that the western countries are safer from cyber attacks. The war just reveals the hacking resources of today, and the vulnerability of our networked based infrastructures. The Russian response to the Western world's sanctions may well be even more hacker attacks on both infrastructure and individual companies. The cyber warfare is here to stay, and it will be used in times of war as well as in times of peace.

Moreover, there is a constant and increasing threat against authorities and companies from cyber criminals. Hackers continue to innovate and find new advanced methods, especially in

ransomware. This global threat needs to be met with increasing awareness and actions, not least the most simple ones, such as patching regularly, segmenting networks and conducting training in IT security. Cyber attacks on corporate networks increased globally by 50 percent during 2021 compared to 2020, according to the IT-security company Checkpoint. Europe had the highest percentage among the continents.

The physical security industry is also a target for hackers. In early 2020 Gunnebo was hit by a ransomware attack where 38,000 documents were stolen from Gunnebo's network and published online. More recent was the sophisticated cyber attack against Axis which caused severe disruption in their systems. The attack was detected at an early stage and forced the company to shut down all systems to limit the impact. Axis reported later that no servers had been found to be encrypted, despite that malware was detected and there were indications that internal directory services were compromised. No customer information was found to be affected in any way.

The importance of cyber security is becoming increasingly more obvious. Every business must look over their cyber security protection and policies. For providers of products and services in the security industry it is even more critical. Security installations should not be a gate for hackers to enter the network of the customer and initiate attacks. That is why requirements for providers of network-based electronic systems for physical security purposes must be raised. There must be an instrument to verify integrator and installer knowledge of material selection and how to install technology for physical security in a cyber-secure way if the industry wants to maintain its credibility. The industry needs standards and norms, which competent and serious security system suppliers can be certified to. Customers must be given the chance to choose safe suppliers, who can verify their expertise in the cyber security area and their routines to prevent cyber threats and damages from cyber attacks.

Actions to establish such European standards and norms cannot wait. It is not just super important for the security industry; but a necessity to protect us all.



3 Publisher's Comment. The industry needs to step up against cyber threats.

6 Security Technology Market. The global security technology market recovers quickly.

10 Theme: Perimeter Surveillance. How do we protect areas from threats on the ground and air?

18 Business News. Motorola acquires Ava Security.

24 Theme: Access Control Systems. The cloud, mobile solutions and the critical role of ID.

30 Product News. New globally certified cameras for hazardous areas.

35 Security Events. Calendar for physical events.

SECURITY TECHNOLOGY MARKET



Security technology Market

Fire alarm & detection market rises.

Page 7



Theme: Perimeter Surveillance

How do we protect areas from threats on the ground and air.

Page 10



Theme: Access Control Systems

The cloud, mobile solutions and the critical role of ID.

Page 24



Business News

Motorola acquires Ava Security.

Page 22



Product News

New globally certified cameras for hazardous areas.

Page 30

Improve security and optimize business performance with Axis solutions.



Network cameras



Network intercoms and access control solutions



Network audio solutions



Wearables



Network video recorders



Video management software



Analytics and more

Along with intelligent solutions, benefit from transparency, open platforms, strong relationships, cybersecurity vigilance, sustainable practices, and an award-winning technical support team from the leader in network video.

The global security technology market recovers quickly

In 2021, sales of physical security products recovered sharply from the previous year, growing to more than \$ 33.8 billion (factory gate prices). In addition, the market will have an average annual growth rate of 7.2 percent until 2026, according to a new report from the market research company Memoori.

The report is called "The Physical Security Business 2021 to 2026" with the subheading "access control, video surveillance & intruder alarms / perimeter protection research".

Now, well into the pandemic, the global physical security market has shown a remarkable degree of resilience, surpassing some other global technology markets and undoubtedly surpassing what Memoori thought was the best case scenario a year ago.

Cloud solutions on the rise

New physical security trends over the past two years have rapidly accelerated cloud adoption. The new report from Memoori explains that for physical security systems the ability to be able to control cameras and access control systems remotely has proven particularly appealing during the pandemic.

Security-as-a-Service

Covid has triggered a need for cloud for remote security, opening up the Security-as-a-Service market for a wide range of buildings. It can unlock a huge range of new services by giving customers greater access and exposure to the cloud ecosystem.

The growth in demand for remote and managed as-a-service models for both access control and video surveillance (ACaaS &



James McHale, the CEO of Memoori, claims that the demand for cloud solutions and cyber security is on the rise.

VSaaS) has outpaced the rest of the market over the course of the pandemic. In addition, according to Memoori, this helped to offset a slight decline in hardware sales over the course of 2020.

"The pandemic is helping to reshape the physical security industry, turbo-charging certain emerging business models, whilst it also continues to make our societies safer; not just from the pandemic but from crime and terrorism," says James McHale, CEO of Memoori.

IoT great driving force

This is the 13th year in a row that Memoori presents a market analysis that brings together all the factors that affect the industry's future. And it is very positive reading. In 2021, the market grew to more than \$ 33.8 billion (factory prices) and Memoori predicts a average annual growth rate of 7.2 percent over the next five years until 2026. In the report, the market is broken down in size in terms of product area, sales in different verticals and geographical regions.

IoT great driving force

The main driving forces behind demand during the period include the growth of IoT and building system integrations, increasing demand for remote control and especially cloud-based ACaaS (Access Control

as a Service) and VSaaS (Video Surveillance as a Service) services, and AI-based video analysis.

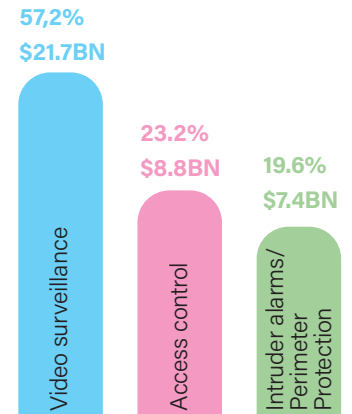
"At the same time, macro-market factors such as crime, persistent terrorist threats, border disputes and refugee crises will continue to push for the adoption of physical security technology," states James McHale.

Big difference between verticals

According to Memoori, the global covid-19 pandemic has created a significant change in demand per vertical over the last two years and some of them will be short-term. Lockdowns, and the economic consequences of them and the public's concerns about the spread of Covid have had a negative effect on sales in several markets, for example in retail, leisure and hotels, while offices have been affected somewhat less negatively. Conversely, investments in healthcare and logistics-related verticals have increased sharply.

Video Surveillance dominates

The market for video surveillance products still accounts for the largest share of sales of physical security with 57 percent of the total market. And it has recovered sharply and increased 14.5 percent compared to the previous year



Video surveillance accounts for the largest share of sales of physical security with 57 percent of the total market in 2021, followed by access control and Intruder Alarms.

and reached 21.65 billion dollars in 2021, which is more than the year before the pandemic, 2019. Over the next five years, Memoori believes that the market for video surveillance products will slow down somewhat and have an average annual growth rate of 7.8 percent and reach \$ 31.5 billion by 2026.

Cyber security more important

Memoori also notes an increased focus on cyber security and believes that if the security companies do not invest in ensuring that their products and systems are not vulnerable to cyber attacks, they can face massive claims and huge reputational harm. One of the critical buying propositions of physical security is now: "what have you done to make this equipment less vulnerable to cyber attack and does it comply with current legislation?"

"The owners and operators of buildings, particularly those with large building estates, need to know that manufacturers and installers fully understand what needs to be done to reduce vulnerabilities," James McHale concludes.

Note: The report "The Physical Security Business 2021 to 2026" is 259 pages long and can be ordered at www.armedia. see under the tab "Reports".

Fire alarm & detection market rises

The global fire alarm and detection market size will reach 56.06 billion dollar by 2030, registering a CAGR of 7.2% from 2022 to 2030, according to a study by Grand View Research, Inc. The market is gaining prominence, more so amidst the Covid-19 pandemic that hit the world economy in 2020, with businesses shifting to remote working models.

Furthermore, the total global fire protection systems market is set to reach \$130 billion by 2030, according to Grand View Research.

Northbrook, IL (USA)

The demand for residential fire safety witnessed a rise, with people spending extended hours working from home. The global demand continues to witness growth over the next seven years. While the pandemic created a few lucrative opportunities for the Original Equipment Manufacturers (OEMs), awareness about the safety and security of assets in the commercial sector also increased.

Technology advancements

As businesses resume operations, the need to safeguard facilities with guidelines and installations promoting fire safety will encourage building owners to either replace old equipment or install new safety devices. In addition, the advancements in fire safety products by leveraging the latest wireless technologies will help OEMs keep up with the competitive rivalry in the industry. Advancements followed by cost-effective products and service & maintenance post installations will go a long way in favouring sales. Vendors aim to launch new products and leverage opportunities in emerging markets by developing a local sales network and closing new business deals.

OEM and replacement sectors strong

All such efforts by OEMs will drive the growth of this market over the next few years. Apart from new equipment sales, the demand

for the replacement market is also on the rise. Ageing infrastructure with outdated fire safety devices will pave the way for new business opportunities over the next seven years. The replacement scenario is likely to create several growth opportunities particularly in the North American and European regional markets, where the market has hit the ceiling, in terms of growth.

Integration with building automation

The growing trend of integrating fire alarm and detection systems with building automation systems offers vast growth opportunities to the market. Connectivity with building automation systems is increasingly becoming a major feature of fire protection systems in commercial, industrial, and residential applications. This can be attributed to the fact that such integration allows for the development of systems that are capable of sharing and gathering data, which can help in alerting individuals about fire safety issues in the premises. A notable rise in investments in smart building automation technologies across several regions is expected to lead to new opportunities for building automation systems in the industrial and commercial sectors.

Other findings

A summary of other findings from the report include the point that



The demand for residential fire safety witnessed a rise, with people spending extended hours working from home.

mandates and guidelines promoting fire safety in residential, commercial, and industrial settings will upkeep the product demand over the forecast period; smoke detectors witnessed a significant demand in 2021; however, heat detectors will register a significant CAGR from 2022 to 2030; regulations governing the commercial sector resulted in the segment dominating the market in 2021; and the market in North America has reached maturity, in terms of demand; however, aging infrastructure will drive replacement sales over the forecast period.

Total fire protection market

Regarding the size of the whole global fire protection system market, Grand View Research expect it to reach 130.37 billion dollar by 2030, based on an expected CAGR of 6.7% from 2022 to 2030. Increasing adoption of wireless technology in fire protection systems, growing human and property loss owing to fire breakouts, and stringent fire safety regulations are projected to fuel the market growth, states Grandview Research.

Increasing implementation of

building safety codes and renovation projects is also anticipated to be a major factor influencing the market growth. The application and usage of fire protection systems are anticipated to increase continuously with the developments of commercial entities and corporations. Furthermore, technological enhancements such as extinguishing technology based on mist and products such as laser optical/infrared smoke detectors, alarms with embedded voice evacuation announcements, hypoxic air fire suppression systems, and wireless fire alarm systems are expected to gain traction in the market globally. Moreover, in 2020, the market will have been hampered due to the Covid-19 crisis, which has interrupted production, impacted demand, and caused supply chain disruption, concludes Grandview Research.

Key players

Key Players operating within the fire alarm and detection market and cited by the analysts in the report include: Johnson Controls, Honeywell, Napco, Nittan, Siemens, Halma, UTC, Bosch and Eaton.

Cloud security market set to reach \$77 billion by 2026

A new report released by Marketsandmarkets on the cloud security market and including a Covid-19 impact analysis predicts that the sector is expected to grow from USD 40.8 billion in 2021 to USD 77.5 billion by 2026, at a CAGR of 13.7% from 2021 to 2026.

Northbrook, IL (USA)

The major growth drivers cited for the market include the increasing number of security breaches and cyber attacks on cloud infrastructure, and strict regulatory compliances toward adoption of cloud services.

Large enterprises lead the way

Large enterprises are classed as those organisations with more than 1,000 employees, and they are investing heavily in advanced technologies for increasing overall productivity and efficiency. Large enterprises are widely opting for cloud security solutions and are expected to invest significantly in advanced cloud security solutions

to provide optimum security to their enterprises' intense competitive environment. Large enterprises have adopted cloud security solutions, as they use a large number of cloud and Internet of Things (IoT)-based applications that are highly susceptible to cyber attacks. Moreover, as they face threats from targeted attacks to disrupt their Information Technology (IT) services, these organisations adopt cloud security solutions to provide effective security.

North America is the geographical strong holding

North America has sustainable and well-established economies, which empower it to invest significantly



Illustration: mohamed Hassan / Pixabay

Large enterprises have adopted cloud security solutions, as they use a large number of cloud and Internet of Things (IoT)-based applications.

in Research and Development (R&D) activities, thereby contributing to the development of new technologies in the cloud security market. The presence of majority of key players in the cloud security market is expected to be the major factor driving the growth of the market in this region. Key players, such as Microsoft, Cisco, McAfee, Palo Alto Networks, Fireeye, and Fortinet, along with several start-ups in the region offer cloud security solutions and services.

Key market players

The major vendors covered in the cloud security market report and not already mentioned above include Amazon Web Services, Checkpoint, Google, IBM, Zscaler, Sophos, Foreseeti, Broadcom, Trend Micro, Tenable, Forcepoint, Netskope, Imperva, Proofpoint, Cloudflare, Aqua Security, Qualys, Ciphercloud, Bitglass, Sitelock, Illumio, Varmour, Avanan, and Cloudpassage.

Security screening market approaches \$10 billion

The estimated market for security screening currently sits at around US\$ 7.8 billion, and according to the latest research, released by Future Market Insights Inc, it is highly likely that this sector could approach revenues worth US\$ 10 billion in the next two years.

Dubai, U.A.E

The ESOMAR-certified research firm suggests that more than half of the total demand for security screening is being accounted for by the developed regional markets. East Asia however is cited as the most lucrative market for investors in security screening systems and solutions.

Rapid growth in the economy, necessitating increasing expenditure on the national and infrastructural security, will continue to push deployment of reliable and advanced technology enabled security screening systems. While analysis identifies an impressive rate of adoption within emerging economies, China, India, and Russia are more likely to

be at the forefront of this growth, in the security screening market.

Airports generate maximum demand

Over 2/5th of the global security screening demand is accounted for by airports, which say the analysts, will remain the dominant application area for security screening systems manufacturers and suppliers. As government buildings are highly vulnerable owing to the voluminous sensitive information that they procure, public recreation areas such as malls are also cited as the next sensitive area for implementation of effective security screening. Border check points are also expected to

emerge lucrative through the coming years, in the security screening market.

Explosive trace detectors, currently accounting for nearly 1/4th share of the total sales of security screening systems, will reportedly witness strong growth in demand through the coming years. According to the report, x-ray screening systems and biometric systems are also highly popular among the end-use application areas in security screening market. The collective market value share of the aforementioned security screening systems is just-under 50% and the report expects attractiveness of the latter to surge - with growing adoption of fingerprint and face recognition technologies.

Smart security screening trends

Looking at the loopholes in current security screening models in terms of efficiency and sustainability, airports have been accelerating the industry's shift to smart security

screening solutions, over the recent past. A combined initiative of Airports Council International (ACI) and the International Air Transport Association (IATA), smart security is emerging as a streamlined solution for airlines, passengers, and their belongings. Recently, Australia's first-ever smart security screening checkpoint was unveiled at the Melbourne Airport.

Key vendor insights

Westminster Group PLC, one of the key players competing in the security screening market, recently completed the acquisition of Keyguard UK Ltd. The latter is a leading company in the security screening space, providing the blend of manned security and the latest technology enabled security screening systems. The former will now offer packages combining technology and guarding - particularly to the infrastructure security domain. This deal is expected to benefit both the business bases, in form of multiple cross-selling opportunities.

Hikvision
AcuSense
Technology

The Easy Upgrade

to

AI



Accurate Alarms
for Humans and
Vehicles



Search Targets
Quickly by Type



Visual and
Auditory Warning



FOCUS
and
ACT

Say "Hello!" to accurate alarms and intelligent security. Hikvision's AcuSense technology uses deep learning algorithms to distinguish people and vehicles from other moving objects in video footage, enabling security personnel to focus and act only when there is real concern.

AcuSense takes **Perimeter Protection** and **Motion Detection** to a whole new level of intelligence. This market-proven technology is now available in more Hikvision products, starting at budget-friendly levels.

Don't miss this great chance to **update and upgrade existing security systems** with affordable deep learning technology. Whether it's a network system or analog, choose Hikvision's products with AcuSense technology to enable easy AI solutions in your next project.

HIKVISION
www.hikvision.com T +86 571 88075998

overseasbusiness@hikvision.com



@HikvisionHQ



@HikvisionHQ



@Hikvision



How do we protect areas from

Perimeter security has moved on from simply triggering after the event when a line has been crossed, to deploying technology that reacts before the intrusion has even happened.

“You want to be proactive and see what happens outside your plot boundary and be able to track objects, that is crucial,” says David Lenot, Critical Infrastructure Practice Leader at Genetec.

“Perimeter security – how do we effectively protect areas from threats on the ground and air?” This was the title of a well-attended panel discussion at Sectech in Stockholm recently, in which the following five industry experts participated:

Jimmy Ek, Nordic Sales Manager, Axis Communications, Mark Cosgrave, Divisional Manager, Western Europe, Optex, Gustav Norvik, Product Manager, Stanley Security, David Lenot, Critical Infrastructure Practice Leader, Genetec and Magnus Cederäng, Business Unit Manager IP-Surveillance, Infralogic.

The market for perimeter security has changed a lot in recent years and the solutions have become more advanced and at the same time more affordable. Jimmy Ek, Nordic Sales Manager at Axis Communications, emphasises that integration is the key when it comes to perimeter security today and that it has been so for a while.

“We see that many people are using security cameras, thermal cameras, radar and so on. It is becoming more common to combine technology, and integration is a clear trend,” he says.

Mixed technology works best

Magnus Cederäng, Business Unit Manager IP-Surveillance, Infralogic, agrees, even though he claims that there are still surprisingly common in the Nordic region to see perimeter surveillance applications utilising just one type of sensor.

“However, I think we are moving away from using one-sensor-type solutions to a combination of several different varieties of sensor and to applications where cameras are used to verify an intrusion,” he says.

Knowledge based decision

The five panelists present at the discussion agreed that there is no single technology that can offer a total perfect solution. Which technology to choose depends on what the customer wants to achieve and the conditions at the site.

Mark Cosgrave, Divisional Manager at Optex, wants to keep it simple. He says that the most important thing is to find a solution that works for the customer. In addition, he advises that integrators should research the technology before making a decision.

“Make sure you understand how it works and its limitations,” comments Mark Cosgrave, who also emphasises that the choice of technology should not be purely based on budget.

“Choose the best solution, not the cheapest, because it may not give you the result you want,” he states, and refers, amongst other things, to the risk of multiple nuisance alarms.

Improved technology

Nuisance alarms are historically a problem in perimeter security applications. For many years the security industry has hyped certain technologies, like video analytics, and made promises to customers that could not be realised. And that still happens. Or as Jimmy Ek from Axis expresses it:

“If a provider of a perimeter surveillance system promises that you will not receive any false alarms, nor will you miss any real alarms and you don’t even have to configure your system, then they simply are not telling the truth.”

However, Jimmy Ek is also keen on explaining the improvements in the technology over the last ten years.

“If you drive a seven-year-old car and then get in a new car, of course the experience will be different. Today, cameras along with AI video analytics are very good. But yes, you need to choose quality hardware with a lot of processing power, you need light sensitivity and you need to plan your installation. If you do this, then you will experience a solution that just generates a few false alarms, but still not zero false alarms,” he says.

Proactive solutions

David Lenot, from Genetec, points out that there are many different types of technologies for perimeter security that have become available due to falling prices.

“In addition to IP-cameras using video analytics and various types of fences and sensors, there are also thermal cameras, radar and Lidar detection systems suitable for perimeter security solutions,” he states

David Lenot also emphasises the difference between “intrusion detection” and systems that track objects.

“Fence alarms, for example, have become much better, and it is also important to be able to track objects with radar or Lidar technology. By tracking the objects both before they reach the fence line and when they have stepped over it, you do not just improve the detection. This is a new paradigm where we try to understand if someone is about to intrude, what happens before that and where is the intruding person heading,” he says.

Lidar technology

Lidar is an abbreviation for “light detection and ranging”. It is a type of laser sensor that measures

distances to objects and maps them via a dot grid which is then read by software.

“Lidar may be new to some people, but it has been used for security applications for more than ten years. Together with cameras and surveillance equipment, it is very effective, not least to create situational awareness. It’s about protecting your plot with several layers,” states Mark Cosgrave, stressing the importance of not just relying on one type of technical solution.

“Don’t do it, because if it doesn’t work, then that’s it. You should have to use several different types of technology within the overall solution,” he says.

Radar technology

Gustav Norvik, from Stanley Security, emphasises that when a camera cannot see far enough, it is more effective to use radar to track the objects and when they get close enough, the camera can focus on them.

“It makes it easier for the operator or end user. With an installed speaker system, they can verbally communicate that they have seen the intrusion and that the offender must leave. In this way, we can use different types of technology together,” he says.

Magnus Cederäng agrees:

“We represent different types of sensors, but I agree with Gustav, the operators need information to act upon and they do not want false alarms. If we can start combining different technologies, I think we can get down to a one percent false alarm rate,” he says.

More proactive in the future

David Lenot believes that it is quality and coverage that are the crucial points, not whether you use cameras, fences, radar or thermal cameras.

“You want to be proactive and see what happens outside your plot boundary and be able to track objects. Being able to position and track objects is crucial,” he states.

threats on the ground and air?

Jimmy Ek believes that the installation and design of the solution is very important.

“Today it takes quite a lot, you have to design correctly, you have to plan, you cannot just mount the camera anywhere and believe that it will not give any false alarms. You have to spend time on it.”

Furthermore, Jimmy Ek also believes that the development of AI will facilitate and make many applications better. He sees the development of deep learning for cameras as something very interesting from a perimeter security perspective.

Drone detection still fresh

Drone detection is becoming an important part of perimeter security.

“Perimeter surveillance is

about about detecting objects on the ground, and on water, but also in the air. The way you design perimeter monitoring needs to be 360 degrees and you should have a system that can position objects,” claims David Lenot.

Gustav Norvik says that he was present when 17 different drone detection systems were tested at a large Nordic airport.

“Most are based on RF or radar. The combination of RF and radar can be good for determining the position of the drone. However, one problem is what to do when an enemy drone is detected. Shooting it down is associated with legal issues, what happens if it hits a person or property when it crashes? This is something that continues to be discussed,” concludes Gustav Norvik.



Perimeter security has gone from being about alarming when the perimeter is broken, to react before an intrusion have been committed.

Intelligent Network Lighting

VARIO2^{iP} PoE

A comprehensive range of Infra-Red, White-Light
and Hybrid LED network illuminators



Fully
Programmable

Real-Time
Response

Remote Set-up
and Maintenance

rayTEC[®]
www.rayteccctv.com



Smarter technology solutions increase perimeter security

Airports, energy facilities and logistics centres are examples of applications where the boundary for where unauthorised persons do not have access should be very clear. Jimmy Ek, Nordic Sales Manager for Axis, believes that the ongoing digitalisation has created completely new conditions for creating strong perimeter protection with IP-based solutions.

Jimmy Ek emphasises that ongoing IoT development has paved the way for achieving effective perimeter monitoring with high precision. Today, security cameras, access control units and digital speakers are connected to IT networks and can receive, analyse and distribute data.

“Smart technologies offer powerful solutions to meet the safety requirements in the perimeters, which provides fast incident management and response,” he says.

Intelligent technology provides better precision

Jimmy Ek believes that the combination of security cameras and software for motion detection has expanded the range and capacity of solutions for perimeter protection, from simple detection to complex intrusion analysis.

“By utilising the power of AI, modern camera technology, which can already distinguish between a vehicle and a person approaching a place, is moving fast,” Jimmy Ek emphasises.

“Based on new and improved algorithms, which are based on a lot of monitoring data, it is possible to determine a vehicle category or type, or a person’s gender, age profile and hair colour, all of which serve to improve correct identification.”

Thermal cameras and speakers

By combining visual data from cameras with other sources – such as images from thermal cameras – the detection capacity can be further improved.

“Thanks to the power of the

optics they use, Axis thermal cameras offer the possibility of locating activity over considerable distances, which may be needed at, for example, an airport with a fence at the extremes that are several hundred metres long,” states Jimmy Ek.

A thermal imager can detect someone trying to access the location and automatically trigger Axis PTZ cameras to target the exact location based on geo coordinates. The addition of integrated IP horn speakers allows pre-recorded alerts to be issued to deter potential intruders, or real-time voice alerts that can be communicated from a central location. Edge-based analysis, advances in image quality, the use of AI and in-depth learning opportunities require increased processing power. This is where on-board analysis and edge-based processing comes in. Today’s smart camera technology can analyse and process video data in the cameras themselves without having to upload or download over a network to a central server.

“In addition to the fact that it means significant energy savings over time, you avoid the risk that it would entail with putting the intelligence in a centralised server that in the event of a malfunction puts the intelligence of the cameras out of play. Instead, the edge units make local decisions from unit to unit,” says Jimmy Ek.

“Axis’ own Axis Perimeter Defender solution includes edge-based analysis of intrusion detection and optional PTZ auto-tracking, along with a design tool to enable smooth and careful planning of



Today, security cameras, access control units and digital speakers are connected to IT networks and can receive, analyse, and distribute data, says Jimmy Ek, Nordic Sales Manager for Axis.

camera installations in an area, maximizing their efficiency.”

Benefit – smarter security

Jimmy Ek emphasises that there are really no limits to the number of actions that can be automated. A security camera that triggers an alarm, a pre-recorded audible warning, or a live video that is sent to a team when they go out to investigate an incident, are all examples of automated actions.

Perimeter monitoring in an outdoor environment involves many challenges. It places high demands on installation, product, and technology choices. The occurrence of repeated false alarms otherwise results in problems for the operators who have to handle incoming alarms. This can lead to actions in case of sharp alarms being delayed. But with the right technology, alarm events can be verified with precision.

“With today’s significantly improved images and video analysis, operators now have the opportunity to carefully assess a situation before deciding on action measures,” comments Jimmy Ek.

Access control with network video

Jimmy Ek also believes in access control systems with video

surveillance as a complementary factor for authentication in the entry and exit points of perimeter protection. Friction-free access control technologies offer a streamlined and secure access process where a QR code presented with a mobile phone is backed up by a network camera that confirms the identity before access is granted.

Improved service via access control

Jimmy also believes that automatic access control can also improve both service and customer experience, for example by activating a welcome message and any instructions to the visitor via network speakers while an automatically triggered email or call is sent to the person who will receive the visitor.

Jimmy Ek sees that scalable and future-proof security and surveillance technology has become available to an ever-widening spectrum of industries and companies.

“To embrace these solutions and take full advantage of the many opportunities offered to reduce threats and also improve the visitors’ experience, leads to the creation of a smarter and safer world,” Jimmy Ek concludes.

See where unified security can take you.

93% of organizations that moved to a unified platform saw a decrease in compatibility issues across their security system. This is why our Security Center platform excels. It delivers a cohesive operating picture through modules that were built as one system. So, whether you're securing an airport, a parking structure, a multi-site enterprise, public transit, or an entire city, you can access all the information you need in one place.

To learn about the benefits of unifying your security operations visit genetec.com

Genetec™



© 2021 Genetec Inc. Genetec and the Genetec logo are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.



Long range detection with REDSCAN PRO

The award-winning OPTEX REDSCAN LiDAR series just went one better, with a new detector featuring its longest range yet. The REDSCAN PRO can accurately detect intruders and moving objects up to 50 x 100m away – making it particularly well suited for those responsible for protecting the highest security sites. And by creating rectangular, high resolution detection patterns, there are no 'gaps', so everything from facades to fences, ceilings to roofs can be covered. For the installer, the sensor's intelligent multiple zones logic means each detection zone can be independently configured, while its camera module brings visual assistance for configuration and post-alarm analysis. The alarms and video stream can all be configured via ONVIF.



www.optex-europe.com

ONVIF® | 
ONVIF is a trademark of Onvif, Inc.

INTRUSION DETECTION | VISUAL VERIFICATION
TAILGATING DETECTION | VEHICLE DETECTION
PEOPLE COUNTING



Intelligent security system helped automotive repair business to expand

Business success drove the Australia-based mechanical repair specialist Florida Automotive to a large new facility. With expensive equipment and client assets on-site 24 hours per day, and the new workshop positioned in a quiet industrial area, the automotive repairer chose an advanced security solution from Hikvision.

Florida Automotive in Melbourne's Craigieburn satellite suburb is a Victorian Automotive Chamber of Commerce, or VACC, certified automobile services business. The repairer has become well-known in for their high quality work on all makes and models of vehicles.

The business had grown recent times requiring the move to new and bigger premises. The new premise, located in an industrial area of Craigieburn, gave them the space needed to work on multiple vehicles at once, and store clients' cars overnight for diagnoses and repairs. Nevertheless, as it's a rather un-busy area, especially at night, the company recognised the need for an upgraded and advanced security system to protect a range of expensive, specialist equipment while providing high-level vehicle services.

The owner of Florida Automotive, Nilanga Lakshan Kirulapana, began to look for a security system that would protect his premises and the assets within it, and help the company maintain compliance with regulations and security insurance guidelines. The system had to be reliable, accurate and cost-effective, while having the capability to act automatically in the event of a security incident, warding off potential intruders.

"Our new facility required greater security, but we also needed a better way to control and monitor that system. With Hikvision and our trusted partners, we have designed the ideal solution for our needs," states Nilanga.

Powerful perimeter security

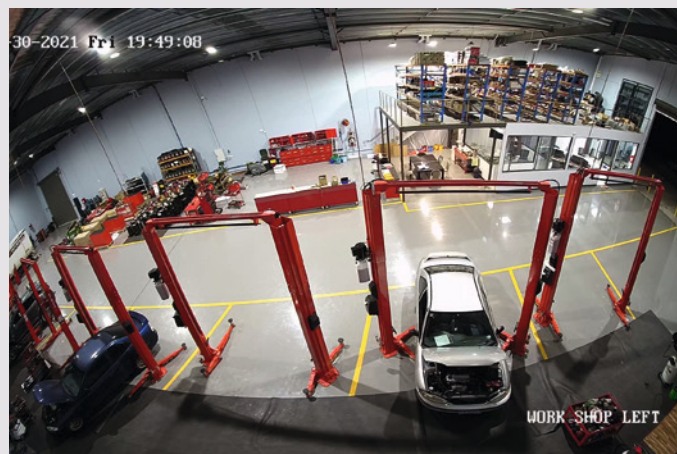
Working with the installer and

Hikvision representative, Nilanga deployed a sophisticated, converged solution built around Hikvision cameras, NVR, indoor stations, and centralised management software.

Ten 4K-resolution Acusense Live Guard cameras were installed around the property, providing complete 360-degree coverage of the perimeter. These are coupled with Smart Event technology (intrusion detection and line crossing) which triggers a built-in siren and strobe light in the event of someone crossing into a specific area once the system is turned on. Three 4K EasyIP 3.0 cameras were installed at the entry and exit points of the premises, providing extra security and continual monitoring of anyone entering and exiting the building. Three Super Wide Angle Fixed Bullet Network Cameras were installed internally due to their ability to capture a 180-degree range of movement.

The 32-channel Network Video Recorder (NVR) provides Florida Automotive with a minimum of two months' recording. RAID6 acts as a backup, in the unlikely event of a hard drive failure.

The Intercom Door Station was deployed at the main gate, capturing a wide field of view as individuals and vehicles approach. It also provides remote control to the main gate of the repair shop for after hours access. A two-way audio was set up at the front gate as well, allowing for easy communication between the reception or manager's office, and whoever happens to be at the gate. A KH8 Series Indoor Station was deployed in the reception area to control access to the main gate.



Through the Hik-Connect software it is easy to view, arm, and disarm everything in the security system with a single touch.

All the security devices are linked to the Hikvision Hik-Connect software, therefore giving the business owner the flexibility to view, arm, and disarm everything in the security system with a single touch.

Besides, two control points for the security system were created, one at the reception area, which combines with the front gate system for easy and convenient operation, and another in the manager's office, which includes four 50-inch monitors for full and clear observation and monitoring.

Avoiding false alarms

With this security Florida Automotive has a large warehouse space fully monitored both inside and at the perimeter. The setup features video and two-way audio communication from the front gate to the offices inside, and line-crossing alerts set up to be triggered at night in the event of an intrusion.

The vehicle repairer can manage the entire security system from the Hik-Connect App on a phone or tablet. It allows them to check in on any element of the security system from wherever they happen to be, whether it is the alarm system, outdoor intrusion, detection, video intercom, or cameras. The staff will receive automated alerts pushed to the application in the event of



Ten 4K-resolution Acusense Live Guard cameras are installed around the property.

any intrusion. The accuracy of the alerts is ensured by the Liveguard solution, which is calibrated by Hikvision's representative so as to avoid unnecessary activations.

"We are very happy with our system design and infrastructure, especially the fact that we are able to check and control the system remotely. This means that we are able to avoid most of the false alarms by checking the live view and activating it from wherever we happen to be," says Florida Automotive's Nilanga. "It's quite a relief that such a large area containing expensive customer vehicles is adequately safeguarded, and we are fully compliant with security regulations and insurance guidelines."



Raytec:

Things to consider when specifying lighting for perimeter security applications

Raytec is the world leader in LED lighting for safety and security, and the company behind the VARIO2 range of award-winning LED illuminators, designed to enhance the performance of any security system.

In this article, their experts point out important elements to consider when it comes to using LED illuminators in perimeter security applications.

These are the five important things to consider when specifying lighting for perimeter security applications, according to the experts from Raytec.

1. Types of Light

Infrared (IR) illumination is the most common type of light used around a perimeter fence line. IR omits zero light pollution, but crucially, it allows the camera to capture night-time images covertly, without alerting potential intruders or giving them light to work by. Once the camera has detected an intruder, the site may choose to raise an alarm. This is where white-light is often deployed; automatically triggered as a flashing deterrent to ward off an intruder or used to provide accurate positive identification of the intruder. Only using white-light when it's needed ensures light pollution is kept to a minimum while still providing optimum levels of security. In some instances, white-light may still be chosen to illuminate the entire perimeter, but due to light pollution, and the fact that the camera is more receptive to IR, means white-light is often preferred as a deterrent.

Another option that specifiers should consider is the use of hybrid illuminators. Hybrid illuminators provide an all-in-one solution, combining both IR and white-light into a single unit. This means one illuminator can be used for both covert surveillance, and as a white-light deterrent. Hybrid allows the user to control the

wavelength and switch seamlessly between IR and white-light.

2. Quality and Distance

Perimeter fence lines often cover large areas, so distance and coverage of an illuminator are two of the main things for a specifier to consider. It is also equally important to consider how the illuminator will assist the camera in obtaining the highest quality images. Illuminators able to deliver longer distances may allow cost savings by reducing the total number of illuminators across the site. It may also reduce costs in terms of the numbers of cameras, lighting columns, cabling and other ancillary equipment needed as part of the installation.

Using illuminators that reduces hot spots and provide an even image across the entire scene is also a way to ensure high image quality. Raytec's Vario2 range uses Hot-Spot Reduction Technology (HRT) to deliver a highly diffused, elliptical beam shape, which targets the light where it's needed. This supports longer distances, minimises light wastage, and ensures even distribution of light throughout the scene. The HRT system also prevents overexposure of foreground objects; light uniformity is crucial in ensuring hot spots are minimised.

3. Hardware Integration

Hardware integration is an important factor to consider as modern perimeter surveillance systems often consist of several IP enabled devices, intended to work together



Perimeter fence lines often cover large areas, so distance and coverage of an illuminator are two of the main things for a specifier to consider.

to provide high levels of security. Typically, these include IP cameras, passive infrared sensors (PIR), laser detectors and fibre optic fence sensors. For applications using these kinds of devices, specifying an IP enabled illuminator capable of providing an automated lighting response, is essential. For example, if a PIR sensor detects movement from an intruder, an alarm could be raised to automatically turn on the white-light (so the intruder can be positively identified) or put the lamps into deterrent mode (to ward off the intruder).

4. Software Integration

In terms of specifying an illuminator, it's important to choose one which can be integrated with the Video Management Software (VMS) used by the site. For example, if a site is using Milestone's Xprotect platform, the chosen illuminator should be capable of being integrated into that system, so it can be controlled easily and lighting responses set-up to be triggered by other detection devices. If the lighting system cannot be integrated with the VMS used on site, it could have a detrimental impact on the efficiency of the security system.

5. Camera Analytics

Using video analytics is an effective



Vario2 range uses Hot-Spot Reduction Technology to deliver a highly diffused, elliptical beam shape.

way to determine if unwanted or suspicious behaviour is occurring in a camera's field of view. However, camera analytics are only as effective as their ability to provide a consistent, clear image. This is where lighting plays an important role. Using analytics requires often increased light levels compared to standard applications. Darkness will seriously affect the performance of the used video analytics and create false alarms. In terms of specifying an illuminator, it's important to choose one which can be integrated with the security management platform in use by the site. For example, if a site is using Milestone's Xprotect platform, the chosen illuminator should be capable of being integrated into that system, so it can be controlled easily and lighting responses set up to be triggered by other detection devices.



Optex:

Protecting perimeters and entrances with intelligent Lidar detection

Many facilities require their perimeter to be secured as it provides a first line of defence preventing intruders from accessing the boundary of the site. However, it is challenging, especially when considering the highest security sites and critical infrastructure environments. Mark Cosgrave, Optex Divisional Manager for Western Europe, outlines the challenges and explains how intelligent Lidar detection can make a difference.

The main objective of a security system at the perimeter is to be alerted of any breach or potential threat. There is a risk of false alarm activations, however, which can incur a high cost and disrupt an effective response. Security professionals consequently search for solutions which can work reliably in an ever-changing environment and can deliver a stable performance in different weather, temperature and variable lighting conditions. That is where Lidar technology can make a big difference, according to Mark Cosgrave:

"Lidar-based intrusion detection is increasingly becoming a preferred choice for perimeter security due to its proven reliability in variable lighting conditions including complete darkness and in extreme weather conditions," he explains.

Mark Cosgrave says that the target can also be customised: "Small to medium sized animals can be ignored, keeping the focus of detection on the real potential threats, whether it's humans, or vehicles. When integrated with good quality cameras and high-performing video management systems, Lidar enhances the security system with accurate detection which can mitigate false alarms and allows to locate real threats and intruders," he adds.

Adaptable system needed

Within high security sites and critical infrastructure there are often

areas which are vital to the good operation of the site. In an airport, for instance, if there is a perimeter breach near a runway there is an immediate danger which would disrupt and shut down completely the airport's operations. Taking the example of an oil refinery, a breach near the oil storage could present a serious threat. Mark Cosgrave believes these scenarios serve as good examples of the benefits of intelligent Lidar technology: "The security system needs to be able to adapt to the different threat levels and locations in order to protect highly restricted areas," he continues. "It is something that the next generation Lidar Redscan Pro can achieve by creating different zones with different sensitivity levels and outputs. An area can therefore be set as pre-warning alert and a different area as immediate security alert."

Virtual fenceless protection

Due to the nature of Lidar technology, an invisible laser wall or plane can be created around buildings and facilities to trigger an alert if anyone trespasses into a highly restricted area. Thanks to its advanced detection logic, Redscan Pro, for example, can use different judgement rules to determine what constitutes a real threat and what can be ignored. For instance, it can be set to raise the alert if different detection zones are crossed by an intruder as he approaches a high restricted zone, or if a vehicle



In addition to horizontal and vertical modes, Redscan sensors allow up to a 45-degree angled detection which can be used on the perimeter as an alert before the target reaches the fence line.

of an unusual or unexpected size approaches a certain area.

Point detection

Locating exactly where the security breach is taking place is pivotal in highly restricted areas as it enables the security staff to know exactly where the threat is coming from. It also makes the visual verification process significantly quicker as cameras do not need to search an entire zone, but instead can look precisely to the point where the intruders are and track them through the detection area. "Point location is one of the key features of Redscan Pro Lidar which can facilitate the exact X,Y coordinates when integrated with high performance VMS," Mark Cosgrave says.

Pre-alert in sensitive areas

In addition to horizontal and vertical modes, Redscan sensors allow up to a 45-degree angled detection which can be used on the perimeter as an alert before the target reaches the fence line. The target object can be defined by size and speed of movement, and it is therefore easy to ignore most wildlife, birds, rodents and cats which could be a major cause of false alarms for other technologies. This pre-alert is an extra layer of

security giving advanced notice of potential security breaches.

Securing entrance points

Sites have to allow access to vehicles and people coming in and out of their facilities in order to run their operation and it is critical to protect those entry and exit points. The credentials are managed via access control management systems which are becoming ever more sophisticated to ensure only authorised vehicles and individuals are allowed in. However as soon as a gate opens, the perimeter isn't closed anymore and it could lead to potential intrusions, such as a person tailgating a legitimate vehicle. Redscan Lidars are deployed to secure gates when they are operating and activate an alert if an intruder is entering the site while the gate is closing or through blind spots while vehicles drive in and out.

Mark Cosgrave is convinced that the use of Lidar detection technology will continue to increase, due to the demand for early effective detection and minimal numbers of false alarms:

"With its advanced flexibility and customisation, Redscan Pro Lidar is set to be a game changer for a wide range of perimeter security applications," he concludes.



Erik Nord, Genetec:

An open platform gathering event data provides the best perimeter protection

How can we optimise perimeter protection and prevent intrusions? According to Erik Nord, Nordic Business Development Manager at Genetec, the answer is to use a mix of technologies via an open platform.

“With a combination of systems for video surveillance, access control, intrusion alarms and automatic license plate recognition, we increase the capability to protect and manage the perimeter,” he says.

In large operations such as airports and critical infrastructure, perimeter security becomes more complicated due to the large areas. And when an organisation has limited awareness of throughout its perimeter, the risk of physical security breaches and cyber attacks increases.

Multiple layers

“With a traditional perimeter monitoring system, operators are only alerted if there is a potential intrusion into areas where unauthorised persons do not have access and this does not hold today,” says Erik Nord, who emphasises that many facilities now have several, overlapping perimeters where everyone has their own rights to access, risk profile and operational requirements.

“Therefore, it is not possible to rely exclusively on a sensor or analysis to detect intrusion, but instead perimeter security must be built in several layers, which means that a combination of sensor technologies are used,” he says.

Erik Nord believes that new technology has meant an opportunity to look beyond the fence and become more specific in terms of what is to be monitored and how. He claims, by using several different types of technology, for example heatmaps, sensors for intrusion detection such as radar, lidar, lasers and fence sensors as well as video analysis, cameras, access control and other stand-alone systems, it will be possible to detect potential unauthorised intrusions outside the perimeter.

The security platform holds gather the information

When an organization does not combine its security systems and technologies on a single platform, but instead relies on vendor integration, it can create information gaps or an incomplete picture of the perimeter. But a unified physical security platform helps combine the data collected by these different systems to provide the situational awareness required to keep facilities and people safe, states Erik Nord.

“Our Security Center platform is integrated with more and more devices, such as radar and laser-based solutions to help detect potential threats over large areas. Moving targets are tracked automatically on geographical maps and displayed intuitively so that security personnel can assess and respond to threats faster,” says Erik Nord.

Faster and better decisions

By presenting all the information about intrusion, threats and potential intrusion together, the unified system enables operators to quickly make important decisions, according to Erik Nord.

Furthermore he claims that high-resolution PTZ cameras with long range are a good complement to perimeter security, for example if the system is configured so that the cameras automatically start looking for visual verification in an area if the perimeter protection indicates intrusion. The pictures are sent directly to those responsible



who can see what is happening and take actions.

Early detection and other benefits

“Detecting potential threats early is crucial. Therefore, for example, lidar technology and seismic sensors can be a way to get alarms even before the perimeter has been broken,” states Erik Nord.

With the help of filtering functions, the security team can also filter objects (for example, so you can distinguish between humans and animals) in different zones to reduce unnecessary alarms. It is also possible to use ANPR readers to scan vehicles and thus obtain better information about who moves around the perimeter.

Physical Identity and Access Management Systems (PIAMS) add another layer to the process by linking access control to business systems, including HR. The interconnection allows organisations to automatically assign or remove access to restricted areas based on company policy. When employees quit or change roles, their access to sensitive areas can be adjusted automatically.

Streamlines event management

A unified security system with automated alerts, standardised procedures for how operators should handle and respond to incidents

A unified security system with automated alerts, standardised procedures for how operators should handle and respond to incidents step by step can help ensure that potential threats are identified, investigated, and resolved quickly and consistently.

step by step can help ensure that potential threats are identified, investigated, and resolved quickly and consistently.

“In some cases, a potential security threat can be difficult for a person to detect. For example an operator may not be able to make the connection between a contractor who unexpectedly enters a restricted area and a device that goes offline. But a unified security system can easily connect these events and quickly flag them,” comments Erik Nord.

Data management it's a big deal

The ability to merge event data is also important for good perimeter protection. A unified security system provides greater awareness of situations that have arisen for operators by aggregating reports and alerts from all modules currently running on the platform. “This is crucial because it makes it possible to see a new situation from all parts of the system as a single event rather than a series of separate incidents. An open platform that holds event data together therefore provides the best perimeter protection,” Erik Nord concludes.

FSN Capital acquires Swedish IAM-company

Stockholm, Sweden

FSN Capital has signed an agreement to acquire a majority stake in Seriline, a Swedish provider of Identity and Access Management (IAM) solutions.

Headquartered in Stockholm, Sweden, Seriline is a fast-growing provider of physical access management solutions, such as physical

credentials, card readers, and on-line identity management systems. The company is owned by the senior management team, Freddie and Pierre Parrman, who will retain a sizable stake in the company. Seriline has 29 employees and had 84 million Swedish kronor sales in 2021.

Seriline is expected to be the initial platform for a buy-and-build strategy to create a Nordic cybersecurity leader within IAM, with the company having a pipeline of potential M&A targets in the fragmented market. Today, Seriline has a broad and long-term

customer base, including large blue-chip corporations, as well as universities, hospitals, and other public sector institutions. For many, cyber security concerns and growing GDPR requirements are driving a focus on physical IAM processes and solutions.

Simon Larsson, Investment Director at FSN Capital Partners, is very satisfied with the agreement.

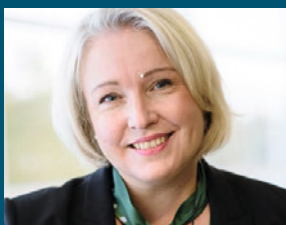
"Seriline has a strong position in the rapidly growing Identity and Access Management space where it is well-positioned to drive further consolidation in the market. We

are very excited to partner up with Freddie Parrman and his experienced team to build a challenger in the European cybersecurity market," he says.

Also Freddie Parrman, CEO at Seriline, is happy with the arrangement.

"To have this strong partnership will be crucial in the next stage of rapid growth for Seriline. To be an early mover in this market is an advantage that will help us create value and continue to lead the way in serving the evolving security needs of our customers," he concludes.

BUSINESS PEOPLE



Erja Sankari has been appointed as Executive Vice President and Chief Operating Officer.

New executive VP and COO at Iloq

Espoo, Finland

Erja Sankari has been appointed as Executive Vice President and Chief Operating Officer as of 1st February, 2022. Erja will also become a member of Iloq's Management Team. Before joining Iloq, Sankari has been working as Vice President of Global Supply Chain at Nokia. She will replace Esa Myllylä who will be retiring in 2022.

Erja will be responsible for the comprehensive management and development of Iloq's global operations, internal practices and way of working and driving forward management systems.

"I am looking forward to bringing my own expertise into the mix and helping to cement Iloq's position as a leading player in software platforms and cloud-based services," says Erja Sankari.

"I look forward to working with Erja and the seamless transfer of responsibilities to ensure the ongoing fulfillment of our company strategies," Heikki Hiltunen, Iloq President and CEO.

Esa Myllylä has been a member of Iloq's Executive Board since 2014. He will step out during spring 2022.

Bosch set to acquire home automation company

Grasbrunn, Germany

Bosch Building Technologies plans to acquire Hoerburger AG, headquartered in Waltenhofen, Bavaria, Germany. Bosch and the owners of Hoerburger AG have already signed corresponding agreements at the end of 2021

Hoerburger offers a comprehensive portfolio of products and solutions focusing on building automation and energy management. The company has 45 years of experience in planning and implementing projects and providing services in this area. A major focus of its activities is the efficient and sustainable operation of buildings. The solutions are used in numerous sectors, for example in large industrial companies, healthcare facilities, and retail

chains. Hoerburger has more than 200 employees at six locations in Germany and one location in Romania and generated sales of 33 million euros in 2020.

Designing intelligent building solutions as a team

"Digitalisation, connectivity, and artificial intelligence are opening up ever more opportunities for us to transform commercial buildings into smart living and working environments that provide people with increased security, safety, and comfort, and ensure greater sustainability. Hoerburger's many years of experience will further strengthen our current portfolio in the areas of building security, safety, energy services, and



Hoerburger focuses on building automation and energy management.

building automation," comments Thomas Quante, president of Bosch Building Technologies.

The acquisition is subject to the approval of the relevant antitrust authorities. It has been agreed that the purchase price will not be disclosed.

Assa Abloy to acquire Vigil in Canada

Stockholm, Sweden and Victoria, Canada

Assa Abloy has entered into an agreement to acquire Vigil Health Solutions Inc., a leader in innovative call systems and resident monitoring solutions for senior living.

Vigil develops and markets a proprietary technology platform combining software and hardware to provide alarm systems and solutions that guide care of and monitor seniors living in senior living communities.

Headquartered in Victoria, Canada, Vigil was established in 1998 and has some 30 employees. The company is listed on the TSX Venture Exchange.

Sales for 2020 amounted to about MCAD 6 (approx. MSEK 40). According to the statement from



Nico Delvaux, President and CEO, Assa Abloy.

Assa Abloy, the acquisition will be accretive to EPS from the start, and is expected to close during the first quarter of 2022.

"The company will reinforce our current offering within Senior Care and will provide complementary growth opportunities," says Nico Delvaux, President and CEO of Assa Abloy.

Changes at the top as Milestone Systems aligns for growth

Copenhagen, Denmark

Milestone Systems has announced that Malou Toft will transition from Vice President (VP) of Europe, Middle East, and Africa (EMEA) to VP of Asia-Pacific (APAC), effective April 1.

Also, effective April 1, Benjamin Low will assume responsibility for a newly established role leading Global Partners of APAC, while Jos Beernink will lead EMEA as the regional VP, a position he has held in the interim while Malou was on maternity leave. "To continue Milestone's strategic journey and to meet our massive growth ambition, I'm pleased

to announce three, new exciting changes to our team," says Thomas Jensen, CEO of Milestone Systems A/S. "Malou will relocate from Copenhagen to Singapore to lead our APAC organisation, Benjamin will focus on helping us grow and reinforce our strategic relationships with global partners in Asia, and Jos will head our EMEA region on a permanent basis. I look forward to working with all three of them in their new roles." Malou, who has been with Milestone Systems A/S since 2018, has vast experience leading large organisations, and a strong background in sales. She has been an inspiration to the entire EMEA team over the years with a strong track-record. Her primary responsibilities as VP for APAC will

include leadership of Milestone's APAC organisation and mentoring of the APAC team for continuous growth and scale. Benjamin Low has been with Milestone Systems A/S since 2015. As current VP for APAC, he has been the catalyst for establishing Milestone across the APAC region. Once Benjamin moves into his new role, he will help reinforce Milestone's efforts with Global Partners, an important priority to grow and scale the business. Jos Beernink has been with Milestone Systems A/S since 2019. He will now formally take over the role as VP of EMEA, a position he has held since October 2020. Jos is a charismatic leader that will drive organisational growth by devising innovative business development



Malou Toft, Benjamin Low and Jos Beernink take up their new roles at Milestone Systems.

initiatives, forming important partnerships, and building strong business relationships.

Business & Product News - Every Day!

www.securityworldmarket.com

HID Global acquires Invotech Systems

Austin, Tx and Woodland Hills, Ca (USA)

HID Global has acquired Invotech Systems, Inc. The acquisition enhances HID's advanced textile inventory management systems offering for uniforms, linens, and laundry operations and adds to HID Global's industry-leading RFID portfolio.

The acquisition advances HID's stature within this growing market, as Invotech provides technology and services to clients across hundreds of properties across the globe, including many of the largest players in the hotel, resort, theme park, and cruise industries.

"Bringing Invotech into the HID family exemplifies our commitment to extending our leadership in textile and laundry inventory management applications by providing a comprehensive suite

of technology and services to customers around the world," said Björn Lidfelt, EVP and Head of HID Global. "This acquisition, as well as HID's recent acquisition of the Textile Services business from Invengo, positions us to expand both our technology portfolio and geographic footprint as we become the global leader in uniform, laundry and linen management applications."

Invotech's real-time inventory management platform combines software, RFID tags, equipment and services to efficiently identify, track and monitor uniforms, linen and textile assets. Invotech enables the real-time visibility of textile assets via three core software solutions, including Invotech Uniform System that manages the lifecycle of employee uniforms from purchasing through daily use to final discard; Invotech Linen System, which automates linen inventory management operations using RFID tags for automatic identification, counting, tracking and more; and, Invotech Laundry



Björn Lidfelt Executive Vice President and Head of HID Global.

System, a solution to automatically track and manage laundry activity for customer-owned and rental uniforms and linens for industrial laundries, hotels and hospitals

Founded in 1993, and based in Woodland Hills, California, Invotech Systems is now part of HID's Identification Technologies Business Area led by Marc Biemann, Senior Vice President and Head of Identification Technologies. The Invotech offering will merge into HID Textile Services and benefit from HID's expertise in laundry RFID tags and readers to support their solution offering.

BUSINESS PEOPLE



Dr. JihFen Lei is promoted to Executive Vice President at Teledyne Flir Defense.

New Executive VP of Teledyne Flir's Defense division

Espoo, Finland

Teledyne Technologies Incorporated has promoted Dr. JihFen Lei to Executive Vice President of Teledyne Flir Defense, one of the leading providers of thermal imaging, unmanned systems, and intelligent sensing solutions to global security and public safety markets. The newly named organisation is a rebranding of the company's Defense Technologies Segment, comprising two businesses - Surveillance, and Unmanned and Integrated Solutions (UIS).

With the new role, Dr. Lei will also continue to serve as General Manager of Surveillance, reporting to Edwin Roks, Executive Vice President of Teledyne and Segment President, Teledyne Digital Imaging.

Dr. Lei rejoined Teledyne in 2021 after serving in the U.S. Department of Defense, including as Acting Deputy Under Secretary of Research & Engineering, where she led the Science and Technology Enterprise. Her career also includes service as director of NASA's John Glenn Research Center.

Mobotix acquires AI specialist Vaxtor

Langmeil, Germany

Mobotix has signed an agreement to acquire Vaxtor Group (Vaxtor), Tres Cantos, Spain, a leading artificial intelligence (AI) based video analytics provider, specialising in optical character recognition (OCR) and deep learning technologies.

Vaxtor's OCR analytics technology, and in particular their automatic license plate recognition (ALPR) products, provide a wide range of solutions for numerous vertical market segments. With 100% in-house development, their technical vision, expertise, continuous R&D investment and product quality have secured year-on-year growth and healthy operating profits. Vaxtor has a broad global customer base, in 50 Countries, and partners with most of the relevant players in the industry, delivering both camera agnostic and at the edge video analytics in various sectors.

Their analytics technology, used in combination with cameras, allows the automated capture of

e.g., letters, numbers or other machine and human readable data and enables such information to be recorded and processed cost-effectively at high speed and trigger any related processes.

This is both a facilitator and accelerator for Mobotix's vertical market strategy as the use of these technologies can be applied in e.g., government, retail and transportation sectors but also, for example, in the tracking of containers, vehicles and aircraft the logistics and manufacturing areas. Market intelligence estimates that the global market for ALPR solutions alone will increase from \$2.3 Billion to \$3.8 Billion by 2025, a CAGR of 10%.

In addition, Vaxtor's products

are tailor made for the Mobotix 7 high performance camera platform and have the competitive advantage that their analytics apps can be run decentralised on board the camera, removing the need for expensive peripheral hardware. They are also integrated into the Mobotix Hub video management software.

With all these factors taken into consideration, the acquisition offers extensive commercial and development possibilities and synergy effects, in particular the opportunity for close development collaboration between Vaxtor and the recently formed Mobotix Development Office in Madrid, all of which will allow both companies to address emerging growth markets or future requirements more effectively.

Mobotix CEO Thomas Lausten commented: "This acquisition is a significant step in our strategy of strengthening our artificial intelligence and deep



Thomas Lausten, CEO Mobotix.

learning capabilities and, whilst Vaxtor will continue to operate as a stand-alone company, is based on compelling commercial and development synergies and clear strategic benefits for both parties."

Both companies agreed not to disclose any financial details. The corporate bodies have approved the takeover. Completion is still subject to the approval of the relevant authorities, and the acquisition is expected to close in Q1/2022.

New stadium in Finland ensures security with contactless access

Tampere, Finland and Stockholm, Sweden

A fully-integrated access management solution from Abloy will ensure smooth, secure and safe access for customers and staff at the newly-opened Nokia Arena in Tampere, Finland.

With a capacity of 15,000 people, the visually-striking Nokia Arena also includes a restaurant, hotel and casino. To ensure the easy passage of its anticipated 1 million customers per year, plus 600 permanent staff and numerous temporary workers during events, it is essential to separate public areas from premises accessible only to employees or hotel guests.

The carefully-tailored solution implemented by Abloy combines the assets of Abloy OS access control, including overall management and access rights to smart devices, electromechanical Protec2 Cliq locking products and keys, wireless Aperio door handles and Abloy Exit push bars.

In the arena, the doors are opened with access rights stored on mobile devices and wristbands. "For example, an ice hockey team training in the rink does not have to worry about losing or returning keys to the right place when their access rights expire at the end of the session," says Jani Helenius, Property and Security Manager at Nokia Arena. When granting access, it is also possible to determine which premises can be accessed and at what times.

"The locks are integrated into the work shift system of the arena's restaurants," says Mikael Ermala, Key Account Manager, Abloy. "For example, when a waiter arrives at the beginning of his or her shift,



In the arena, the doors are opened with access rights stored on mobile devices and wristbands.

the access rights granted to the person immediately take effect in the necessary premises."

Directing an audience of 15,000 to safety in case of emergencies is essential. That's why the locks on the arena doors are integrated with the fire safety system. Smooth evacuation is ensured by Abloy push bars, so that the doors open quickly and easily when

needed.

"Nokia Arena is a striking example of security trends, where access rights are becoming digital and door environments are touchless," says Jari Perälä, Vice President, Domestic Sales and Marketing, Abloy Oy. "In this development, various human resources, space and access management systems are integrated."

Photo: Credit: Tomorrow AB, Studio Lleskind, Ahho Arkkiendi.

Securitas reports highest margins in a decade

Stockholm, Sweden

The latest year end financial results for Securitas AB demonstrate a strong and transformative year for the organisation, with record level operating results and the highest operating margin in more than a decade.

Commenting on these latest figures, the company's President and CEO, Magnus Ahlqvist, said, "Our strategy, investments and actions are starting to pay off and resulting in increasing profitability in all business segments." He believes that the strong cash flow generation has contributed to reduced leverage and a solid financial position at the year end, preparing the company for the closure of the Stanley Security acquisition.

Real sales growth

The company has finalised two transformation programmes and has achieved cost saving targets in key areas and good benefit realisation in North America towards the end of the year, all of which, Ahlqvist suggests, positions the company with a stronger foundation to enhance client value and drive operating margin improvement.

"We finished the year with 4 percent organic sales growth in the quarter and full year. The conditions in the business environment improved gradually during the year, with good commercial activity across all business segments while growth was hampered in North America due to reduced corona-related extra sales and the previously announced contract losses.

Sales of security solutions and electronic security showed real sales growth of 8 percent in 2021, representing 22 percent of Group sales. We saw improved growth in the fourth quarter despite challenges related to component shortages," commented Magnus Ahlqvist.

"The operating result for the Group, adjusted for changes in exchange rates, increased by 15 percent in the fourth quarter and by 28



President and CEO of Securitas AB, Magnus Ahlqvist comments on the company's year end results.

percent for the full year. The operating margin improved to 5.9 percent in the quarter and to 5.6 percent for 2021," he confirmed.

Transformational acquisition for leadership position

At the end of 2021, Securitas took a significant step in its strategy to pursue growth through technology with the agreement to acquire Stanley Security. "This is a transformative acquisition, which we expect will lead to significant added commercial growth and a substantial operating margin improvement over time," said Ahlqvist.

Building a "new Securitas"

Going into 2022, the company is preparing to close the acquisition of Stanley Security. The integration has started and is well on track, according to Ahlqvist. "We are continuing to execute on our transformation programmes in Europe and Ibero-America, which are developing according to plan. The transformation programme in North America was successfully finalised in 2021 and we see positive impacts on our operations and the operating margin at the end of 2021 with further opportunity going into 2022."

"When Stanley is integrated and the transformation programs are fully implemented, we will have built a new Securitas – a modern, digitised and innovative security solutions partner for our clients with a structurally higher margin profile" concluded Magnus Ahlqvist in his closing statement.

HID chosen to design new E-passport for Barbados

Austin, Tx (USA)

HID Global has – through its partner Secure Issuance & Citizen ID Solutions – been selected to supply a newly designed passport to Barbados.

HID Global moved quickly to ensure that from the moment Barbados became a republic, the passports issued reflect this historic change. Barbados is considered to have the Caribbean region's most powerful passport, according to the Henley Passport Index.

"We look forward to working with HID to

finalise the new book design and implement the disaster recovery site," said Hon. Wilfred Abrahams, Barbados Minister of Home Affairs.

The new design is part of a three-year supply agreement that includes the creation of a disaster recovery site at the airport to ensure business continuity should the main passport issuance centre be compromised. This is composed of technology upgrades as well as support for the main issuance site.

ASSA ABLOY

Opening Solutions

Incedo™

Business Cloud

Take control of your buildings security from anywhere



Download a free introductory guide

campaigns.
assaabloyopeningsolutions.eu/incedo-business-cloud

Experience a safer and more open world

Motorola acquires Ava Security

London, UK

Motorola Solutions has acquired London-based Ava Security Ltd, a global provider of cloud-native video security and analytics.

This acquisition means that the Group strengthens its global dominance in the video surveillance industry, especially in the area of video analytics. The video security companies Avigilon, Pelco, IndigoVision and the mobil access control provider Openpath (are already part of the group.

The terms of the transaction were not revealed in the press release from Motorola Solutions, but according to the American online publication IPVM, it is said among many professionals in the security industry that it is about 400 million dollars.

Impressive growth

Earlier this month Ava's latest financials revealed another year of triple digit growth for 2021. Overall the figures show that video revenue grew globally by over 300%, ARR grew by 500% and the number of cameras connected to the Ava Aware Cloud continues to double every three months. The company continued to make sig-

nificant investments across R&D, sales, marketing and leadership throughout the year.

Innovative development

On the innovation front, during the year, Ava introduced two new cloud cameras (the Ava Compact Dome and the Ava Bullet), launched Ava Cloud Storage, delivered a unified dashboard for hybrid deployments and developed native integrations with IP Video's Halo sensors and Disruptive Technologies' environmental sensors. Ava also launched software-driven LPR (License Plate Recognition), enabling the technology on both Ava and third party cameras and not requiring separate dedicated LPR hardware.

"2021 was a great year for us, with our growth rate boosted by new enterprise customers – five Fortune 1000 customers in Q4 alone. But we're not stopping there, as we're projecting similar growth numbers for 2022," comments Tormod Ree, CEO & Co-Founder of Ava Security.

Intelligent video surveillance

Ava Security's scalable, secure and flexible cloud solution provides enterprises with real-time visibility and powerful analytics to optimise their operations and detect anoma-

lies and threats. The platform offers organisations the benefit of an enterprise-grade video security solution while minimizing the physical footprint of their security infrastructure.

"Our acquisition of Ava highlights our continued commitment to advancing cloud-based video security technologies," states Greg Brown, chairman and CEO, Motorola Solutions.

"With Ava, we're well-positioned to support our customers' evolving security needs by expanding our portfolio of intelligent video solutions that help to enhance safety and streamline operations."

In addition to allowing organisations to easily access, search and manage their entire system from a centralised dashboard, its self-learning algorithms also enhance enterprise security by detecting abnormal behaviour and alerting operators to events in real-time.

Merger created a hybrid

Ava Security was formed through a merger between Jazz Networks, a cyber security insider threat detection and response company, and Vaion, an end-to-end video security provider. Together, they would meet the market's needs against both physical threats and cyber security threats by making companies



"Our acquisition of Ava highlights our continued commitment to advancing cloud-based video security technologies," states Greg Brown, CEO of Motorola Solutions.

and other organisations to monitor, understand and act on threats in real time to protect people, assets and data. Both companies were privately owned by Ubon Partners and employees.

Now, this merger creation has become a part of Motorola Solutions.

"I would like to thank Ubon Partners for their backing and believing in our vision. We look forward to building upon Motorola Solutions' industry-leading video security and access control portfolio, providing customers with advanced ways to protect their people and enhance their operational insights," comments Tormod Ree, CEO, Ava Security.

Johnson Controls acquires Envision

Manchester, UK and Armagh, Northern Ireland

Johnson Controls acquires Envision Intelligent Solutions, a business, specialising in technology-enabled remote monitoring and perimeter protection services.

Headquartered in Armagh, Northern Ireland, Envision's expert team of security engineers, installers and managers design and deploy security technologies across the UK. Its in-house accredited alarm and remote video response centre will continue to provide around-

the-clock customer support.

"Envision's expert team and its innovative security solutions will enhance the connected security solutions we can offer our customers and provide fantastic opportunities to realise increased security alongside the benefits that holistic digital transformation strategies provide," comments Richard Jones, general manager at Fire & Security, Johnson Controls UK&I.

Dormakaba acquires Atiqx

Rümlang, Switzerland

Dormakaba has acquired Atiqx Holding B.V, a provider of electronic access control and workforce management in the Netherlands.

Atiqx' offering includes cloud-based solutions with a 24/7 services model, with a attractive recurring Software-as-a-Service (SaaS) income. The company is based in Utrecht/Dordrecht and has around 70 employees. Atiqx generated mid-single-digit million sales

in Swiss Francs in financial year 2021.

"Atiqx is one of the key players in the Netherlands and has a profound know-how of the local electronic access control market. They serve a well-established customer base with a passionate team of highly skilled employees. By joining forces, we can extend our scale and market access in our core business as well as in services," comments Dormakaba CEO Jim-Heng Lee.

Telekom, Hitachi and Securitas form Alliance against blackouts

Barcelona, Spain

In a unified recognition that the energy sector has become the top target for hackers, together, Telekom, Hitachi Energy and Securitas have formed an Alliance against blackouts, in an effort to protect energy suppliers against attacks. The companies made the announcement ahead of the Mobile World Congress in Barcelona.

“Critical infrastructures are being attacked more and more frequently. The latest example in Portugal unfortunately shows how cyber attacks can affect networked technology,” states Telekom Security CEO Thomas Fetten.

“Electricity is particularly important. A successful, precise attack on this area of critical infrastructure would cripple life as we know it. The economy, too. That’s why we’re pooling our expertise in fighting physical attacks, just as we do against attacks from virtual space,” adds Thomas Fetten.

“The future is electric but uncertain”

Pierre-Alain Graf, Head of Global Security Business Hitachi Energy, makes a similar conclusion.

“We have a saying: the future is uncertain but electric. We are addressing climate change with renewable energy from the sun, water and wind. And are generating electricity in an increasingly decentralised way. This inevitably makes us more vulnerable to attack. The partnership therefore extends the umbrella of protection to produc-

tion technology.”

Anders Gustavsson, Head of Remote Video Solutions Securitas Services Europe, emphasizes that “building a Fort Knox around solar farms and substations is not enough..Attackers shy away from robustly secured facilities. They move into cyber space.”

“Together, no one can fend off attacks on company networks, operating technology and sites alone. That’s why we’re pooling our expertise,” he states further.

Cut off power to 700,000 households

Attacks on the energy sector target society as a whole. Attackers include state-backed hacker groups. The German domestic intelligence services cite the intelligence services of Russia, China and Iran as the source of cyber attacks against German plants. In 2015 and 2016, hackers had sabotaged power supplies in Ukraine, highlighting the impact of such attacks for the first time. More than 700,000 households were without power for hours.

The energy industry represents



Photo: Pixabay

Hitachi Energy and Securitas have formed an Alliance against blackouts, in an effort to protect energy suppliers against attacks.

the most critical of infrastructure. Targeted attacks on pipelines, power plants or substations are on the rise. Examples include Colonial Pipeline in the USA and the Danish wind turbine manufacturer Vestas. In Brazil, hackers targeted the nuclear branch of Eletrobras.

Top three attack targets

The sector is one of the top-three targets for cyber criminals worldwide. That’s because the industry is now highly digital. Beyond corporate IT, smart operating computers with sensors control electricity. Digitally networked, they are also targets for attackers. Physical security is needed for plants in the energy sector. This is especially true for remote distribution stations, pumping stations and high-voltage

pylons. If a hacker gets his hands on a control cabinet, he attacks from the inside. Even the best network firewall cannot protect against this. Here, for example, networked video cameras keep watch over the site.

Overarching protective shield

Securing critical infrastructures requires an overarching understanding of OT, IT and physical security. A team of experts from Telekom Security, Hitachi Energy and Securitas has developed an overarching approach in recent years. This combines physical protection with enterprise network and digital operational technology security. The three companies claim that it enables critical infrastructures to meet protection and regulatory challenges.

Johnson Controls acquires smart buildings company Foghorn

Cork, Ireland and Sunnyvale, Ca (USA)

Johnson Controls has completed the acquisition of Foghorn, the leading developer of Edge AI software for the industrial and commercial Internet of Things (IoT) solutions.

“Value is increasingly being created by applying intelligence at the edge-device level to create real-time, secure, actionable insights,” said Johnson Controls CTO Vijay Sankaran. “By pervasively integrating Foghorn’s world class Edge AI throughout our

Openblue solution portfolio, we are accelerating the pace towards our vision of smart, autonomous buildings that continuously learn, adapt and automatically respond to the needs of the environment and people.”

As the number of sensors and amount of data in buildings continues to grow exponentially, the value of processing data and applying intelligence at the edge, without having to send data to the cloud, becomes increasingly

pronounced.

Sastry Malladi, who served as Chief Technology Officer at Foghorn, will join Johnson Controls, reporting to Sankaran as Vice President, Openblue Artificial Intelligence.

“We are thrilled to bring the Foghorn team and edge AI capabilities to Johnson Controls and Openblue,” said Sastry Malladi, Foghorn’s Chief Technology Officer. “By combining our respective strengths, Johnson Controls can

make an even bigger impact on continuing to address some of the world’s most pressing challenges of decarbonisation, sustainability and energy efficiency, indoor air quality and smart, secure buildings.”

Financial terms of the transaction were not disclosed. Foghorn’s technical team will be integrated into the Openblue Solutions organisation. Foghorn’s headquarters in Sunnyvale, California will function as an ‘AI Hub’ for Johnson Controls.



Panel discussion

The cloud, mobile solutions and the

The access control market is becoming less proprietary and more global. Domestic access control brands have been dominating many of the EU-markets, but the increasing demand for open platform systems will increase the competition in all markets.

A panel discussion about access control trends was held at the Sectech event in Stockholm in October 2021. This article gives a summary of the views on those trends, as expressed by the panelists.

The panelists in the discussion were Simon Wallén, Director Nordic Sales at Nexus Group, Robert Jansson, Director of sales at Stid Security, Nordics and Eastern Europe, Magnus Olsson, Head Of Business Development at Seriline, and Tore Brænna, Lead, Business Development EAD, Scanbalt Dormakaba.

A grey zone

Robert Jansson, from Stid Security, is convinced that we will see a more international access control market. Even Sweden, the home of the global market leader Assa Abloy, will be affected. The increasing import of access control products will also contribute to more open systems.

"The entire market in Sweden has been proprietary for a long time. The customers around the world that we serve, they are global and interested in having a platform that they can smoothly run anywhere: in Sweden, Denmark, Norway, Germany, USA and so on. We will see lots of this when the larger international companies are consolidated," Robert Jansson says.

Simon Wallén at Nexus adds that the standards must also be open for that to happen.

"It's a question of levels, it will never be completely open or completely closed. A 40 percent transparency would result in large cost gains and gains in the ecosystem as such. It is never the case

that it is completely proprietary or completely open, but there will be different layers, there will be different situations, different users, and equipment for it," says Simon Wallén.

Robert Jansson states that manufacturers have their driving forces, and buyers and end users have their driving forces. Sometimes they agree, sometimes not.

"There are two fairly clear ways to go, proprietary or open. I think the open will win in the long run," he says

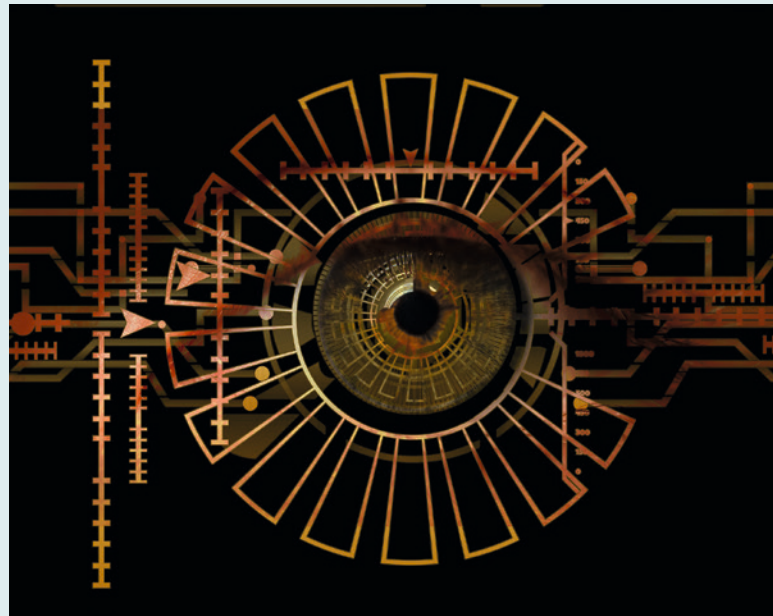
Identity of everything

Simon Wallén claims that one of the strongest trends in the market for access control is increased focus on identity.

"I think we are starting to see an awareness of how to secure the identity of the first link in the chain, we talk quite a lot about card technologies, about how to protect an identity and so on. But if one cannot be sure that the specific credential is used by the specific person it is intended for, then the protecting technology doesn't matter anymore."

Simon Wallén compares it to a passport: it is not worth anything for the technology itself, but because everyone knows that the police and a number of authorities guarantee that the person is what the passport shows.

Robert Jansson agrees that the issuance of identities for people



Domestic access control brands have been dominating many of the EU-markets, but the increasing demand for open system platforms will increase the competition on all markets.

and things will be more and more important.

"We have to have an identity in almost everything, from light bulbs to cars and access control and readers," he says.

Magnus Olsson at the IAM-company Seriline emphasises the importance of identity management from another perspective.

"When we talk about identity, it is important to make sure that you only have one identity in your system, not several. It makes it much easier when a company needs to remove a user from their IAM-system, for example, when someone leaves their employment and should no longer have access to the facilities of the company," he says.

Simon Wallén stresses that identity management is linked to the IoT.

"It is already a part of it, when you look at smart buildings and flexible access to a safe entry into buildings. IoT is a pursuit of automation, intelligence, and big data, then the access to the

information collected by different systems must be protected. There the access control system with its extension is important", he says.

Another trend is that standards are becoming more important, and the introduction of GDPR was for sure a game changer.

"Standardisation will help end customers, and also installers who will help end customers to be safe when the identity is forced over from the card carrier via the reader into the system. Also for mobile ID, these trends are very clear," states Robert Jansson.

Outdated technologies still linger on

The panelists were also in agreement that the choice of card technology sometimes reveals lack of knowledge and security awareness. It still happens in public procurements that consultants request Mifare Classic, which was hacked already in 2007, according to Robert Jansson.

"Many have transferred over to Mifare Desfire but we continue to

critical role of ID

see, that some of the old technologies installed in the late 1990s still remain. We would have liked the development towards safer card technology to be faster,” comments Magnus Olsson.

Simon Wallén thinks that digitalisation in access control isn't really going smoothly.

“For obvious reasons, it takes a long time to replace a complete ecosystem to find more modern and user-friendly alternatives. There is always a trade-off between whether it is for sure, what it costs and how easy it is to replace it. And it is also a matter of whether the customers are aware that the existing systems need to be replaced,” he says.

Tore Brænna at Dormakaba thinks one should be careful about switching from short to mobile solutions.

“In any event, customers should be aware of the standards relating to the use of mobile phone solutions, and in particular, companies that feel there could be a security risk.”

More and more apps

Robert Jansson is positive about mobile solutions and believes that there is always a balance between convenience and security.

“People often want a convenient system rather than a secure system. If you can obtain both a comfortable and secure system, then you should of course have it. However, we use the phone for everything in our lives today, we send bank transactions and sign with both qualified and unqualified certificates, we email, and read sensitive details from the tax authority – the technology is there to build a comfortable and safe solution, but you have to be very clear about what you are doing.”

Robert Jansson also points out that Apple “blocks” the use of NFC and therefore many are more or less forced to run with

Bluetooth or BLE to be able to have a mix of both iPhones and other phones.

Magnus Olsson believes that solutions for using the mobile phone as a credential in an access control system are often proprietary.

“In that way, it becomes a step back: if you go to one company, you get a solution, you go to another you get another solution and that means that there will be many apps in the phone”.

Simon Wallén believes that NFC is a factor of uncertainty because Apple is big enough to do what they want.

“On the other hand, I believe it will be more standardised in the future: which carrier we will use. Whether it is Bluetooth or not, we will focus on identity and how we protect it, regardless of whether it is a card or a mobile phone that is used,” he says.

Biometrics too slow

Biometrics is something that has been discussed for a very long time in access control. Here, too, a balance is struck between conveni-

“If you go to one company, you get a solution, you go to another you get another solution and that means that there will be many apps in the phone”

Magnus Olsson, Sereline.

ence on the one hand and safety on the other.

“You can make it very safe and not allow access to someone who has a dirty thumb, for example, or you can do it more conveniently. Most people come to a compromise somewhere in the middle. GDPR is a sensitive point here, you must not store biometric data anywhere, anytime or anywhere,” claims Robert Jansson.

For day to day applications,



Simon Wallén, Director Nordic Sales at Nexus Group.



Robert Jansson, Director of sales at STId Security, Nordics and Eastern Europe.



Magnus Olsson, Head Of Business Development at Sereline.



Tore Brænna, Lead, Business Development EAD, Scanbalt Dormakaba.

many companies find that PIN codes are too slow to combine with cards and even for biometric solutions, time is a factor.

“We sell biometrics equipment, but due to convenience and speed, biometrics has become less of a success than the market thought it would be,” says Tore Brænna.

access control as a service is a growing part of the industry.

“Some have an old PC with an operating system that is no longer sold, and it is clear that you avoid the problems there if you have a cloud service that is updated automatically ‘on the fly’, but at the same time, there are some high-security customers who do not want data to be in a cloud service and want it on-site.”

Simon Wallén states that while an access control system should prevent unauthorised persons from entering, companies today, should primarily want to protect information.

“Honestly, it’s not what is in the premises, but what the company owns in the form of information, that is important. I don’t think many people have trade secrets physically printed in binders anymore, they are stored somewhere else, for example in the cloud. We meet companies that are opposed to having their access control system in the cloud, but at the same time, they might have all their business-critical information already in the cloud,” he concludes.

Cloud solutions are growing

Magnus Olsson thinks that the industry has been quite slow in moving towards cloud solutions, but that it has gained some momentum and is ongoing right now.

“It’s clear that cloud-based solutions offer great benefits, as well as there being other benefits to having them “on-site”.

Tore Brænna emphasises the benefits of cloud services and

Robert Jansson, Stid Security:

“Secured access control of vehicles and people must be given higher priority”

When we talk about electronic perimeter surveillance, we often think of fences, alarm systems, radar and cameras, including thermal cameras. Secure access control at the entry and exit points is rarely discussed. It is taken for granted.

“The quality of the authorisation check of vehicles with drivers is very variable. Sometimes it is secured, but then often inflexible. If it is flexible, it is usually based on one-factor authentication,” states Robert Jansson at Stid Security who sees the solution in a new multi-technology reader.

In any perimeter protection area, there is always one or more gate for entry and exit. Perhaps there are staff present in connection with these gates to control people and vehicles, or there is a remote operator who checks the authorisation and decides whether the person or the vehicle / driver should have access.

But what is controlled and how is it controlled? This is the crucial issue that Stid’s sales manager for the Nordic and the Eastern Europe, Robert Jansson, is passionate about.

“All perimeter protection aims to steer both vehicles and people to controlled points. And there you have to have control, which vehicles and which people go through it”, he says.

One-factor authentication

Robert Jansson, emphasises how the control of vehicles and drivers can vary.

“There is usually a tag on the vehicle that is detected by a reader to determine if access should be allowed. It only detects the vehicle,” he says.

Robert Jansson points out that the vehicle’s measurable dimensions and registration number can also be identity parameters to ensure that it is the right vehicle, before access is granted.

“But notice, we are talking about ensuring the identity of the vehicle, not the drivers right to access in this case. Too often the

driver is excluded from control or both the vehicle and the person behind the wheel have a UHF badge, which means that both use one-factor authentication.”

Robert Jansson admits that it happens that the driver is forced to leave the vehicle to go to a reader, swipe his card and enter his PIN code, which is two-factor authentication.

“But then they have departed from the very purpose of long-distance reading, namely that the transports should be agile,” he says.

Two-factor authentication

But it is actually possible to use two-factor authentication without the driver having to step out of the car.

“If you use virtual cards via the mobile phone, you can have both one-factor and two-factor authentication in the hand of the driver. Then you can ensure that the person is the authorised driver and shall be admitted access. It is not someone else’s ID carrier that they use. That is important,” comments Robert Jansson.

Two-factor authentication means that the driver’s mobile is detected, but only when the PIN code alternatively fingerprint or face reading have opened the mobile phone, the signature of the virtual card is sent to the reader. Thus, no unauthorised person can use the ID carrier and gain passage into the area.



With Specter Nano, access control systems can thus apply a so-called “two-man rule”, ie access is only granted if both the vehicle and the driver are authorised.

Safe and flexible vehicle passage

As sales manager for Stid in northern and central Europe, it is easy for Robert Jansson to propagate for two-factor authentication and smooth access control for vehicles and drivers. With the multi-technology reader Specter Nano, Stid has developed a unique solution for reading vehicles and people quickly, smoothly and safely. It detects over long distances and checks the vehicle’s and driver’s identity and right to access simultaneously. The reader can handle several vehicles and people at the same time.

“In addition to reading the mobile’s virtual card for two-factor authentication of people, Specter Nano reads all types of windshield tags, cards, key fobs or other things that have UHF or Blue-tooth,” says Robert Jansson.

“The reading distances can be adjusted with both Bluetooth and UHF and the fast reading means that the driver hardly needs to slow down, which contributes to user-friendliness without reducing safety,” he adds.

Sets a new standard

Robert Jansson believes that Specter Nano sets a new standard for access control and enables both fast and secure access controls for vehicles and people.

“It’s time, for safe access control

of vehicles and people must be given higher priority. Being able to identify the vehicle and the driver simultaneously is important for the access control to work properly. The risk of criminals entering an area via a stolen authorised vehicle is eliminated with this solution,” he says.

“Now you do not have to choose to quickly and safely detect either vehicles or drivers, but you get the best of both worlds. The vehicle approaches the reader and is detected by the encrypted UHF tag and the driver can then already be detected via his virtual card in the phone.”

The only legal way in Norway

With Specter Nano, access control systems can thus apply a so-called “two-man rule”, ie access is only granted if both the vehicle and the driver are authorised. This feature arouses special upheaval in Norway, where there is a law on two-factor authentication if a transaction is to be logged in an access control system.

“If you provide one-factor authentication on a person, only the vehicle can be logged, not the person. Specter Nano is the first solution where you can legally – via one single reader – have a transaction of the drivers and the vehicle in an access control system,” states Robert Jansson finally.



How do you benefit from access control integration?

ASSA ABLOY
Opening Solutions

Get the insights
Download the white paper



Experience a safer
and more open world

New report about integrated solutions:

Access Control – the foundation for smarter buildings and efficient workflows

Access control systems are often viewed as the starting point for a building to shift from operating in siloes, towards a more functional, connected and 'integrated' building management system, according to a report from Ifsec Global and Assa Abloy Opening Solutions.

"To reap the benefits of connected security, businesses need technologies which are primed and ready to work seamlessly with each other," comments Thomas Schulz, EMEA Product Marketing Director, Assa Abloy Opening Solutions. In a recent survey of security professionals – published in "The Wireless Access Control Report 2021" by Assa Abloy Solutions – over 90 percent of the responders noted the critical importance of integration across building management functions. But what exactly are the benefits – and how can organisations deploy effective strategies to realise them, even with a limited budget? An 18-page white paper, "Boosting efficiency and streamlining security with an integrated access control solution", from experts at Ifsec Global and Assa Abloy Opening Solutions, responds to these questions, providing the detailed background which key decision-makers need before launching an integration project.

Education sector

Thomas Schulz explains that the report examines the growing role for integration within and beyond building security. It highlights the benefits – in cost control, employee and energy efficiency, security and more – for businesses with integrated security systems and process.

"The concrete benefits an organisation can expect vary from case to case. The white paper studies

real-world hardware integrations in the healthcare and higher education sectors in two European countries. It considers the cost and efficiency impact on the organisations which integrated access control effectively," he states and continues with an example from the report.

"At the Inholland University of Applied Sciences, a Nedap AEOS system integrated with Aperio wireless devices is able to control access for seven different campuses from a single, integrated point. A new university site in Amsterdam will be developed as a 'smart building', incorporating many of the same interoperable technologies integrated with an intelligent building system."

Health care sector

Thomas Schulz also mentions an example from the healthcare sector.

"At Centre Hospitalier Métropole Savoie in France, a single ARD system integrates Aperio locks for building access and security with an internal HR management system and the French government's electronic Health Professional Card. Having a single credential for multiple uses increased efficiency for both security administrators and medical staff."

Long-term and short-term benefits

The paper examines how integrated solutions reward businesses in both the short and the long



Looking further ahead, integration helps businesses to retool their building management for the challenges of the 2020s.

term. It states that "in the short run, integrated security can make employee workflows more efficient, as those real-world cases show. When facilities staff only consult or update a single interface, rather than multiple systems, they save time and reduce manual errors."

Looking further ahead, integration helps businesses to retool their building management for the challenges of the 2020s. The smart building is integrated, automated and future-proofed.

"Whereas security has mostly been a reactive profession prior to now, integrated solutions allow data to be transformed into knowledge," explains Danny Laurier at Securitas, in an exclusive interview for the white paper.

"And, when you have knowledge, you can move from a reactive to predictive risk management approach."

How to deploy security integration

What information must company decision-makers digest to assess their specific case for greater security integration? How can they choose the best off-the-shelf inte-

grated or integratable solutions?

Of immediate practical use, the report examines different types of integration and the technologies required to make each work. It explains how deployments can be made even when faced with tight budgets and a demand for concrete returns on investment, including for high-demand access control integrations such as visitor management and video surveillance.

Look over interoperability

Ensuring an organisation buys and plans for interoperability in both hardware and software is critical.

"As well as being more flexible, solutions developed to compatible, shared standards are better future-proofed," explains Russell Wagstaff, EMEA Platform Director at Assa Abloy Opening Solutions.

"Standards ensure investments can be made today with confidence that hardware and firmware can be built on seamlessly in the future. Compatible solutions, ready to integrate with multiple different systems, offer greater peace of mind than proprietary technologies which 'lock you in' for the long term."



Download a free copy of the white paper

Reading the white paper "Boosting efficiency and streamlining security with an integrated access control solution" will help any size or type of business plan its next steps with integration.

Download a free copy today at: <https://campaigns.assaabloyopeningsolutions.eu/das-integration-whitepaper>

Get a free copy of the: "The Wireless Access Control Report 2021" at: <https://campaigns.assaabloyopeningsolutions.eu/wacreport2021>

I AM A BEAUTY...



... BUT MORE IMPORTANTLY I'M THE FASTEST AND MOST SECURE WAY TO ACCESS YOUR CAR-PARK

With my combination of UHF and Bluetooth® technologies, I recognize your visitors, employees, their vehicles or even both at a glance. I will comply with your security policy.

Together, we will manage all of your access points. Your security will be under control from end to end, even in the most challenging situations.

My compatibility with the STid Mobile ID® ecosystem enables the use of smartphones and virtual cards to access all of your organization's critical infrastructures.

My ability to support hands-free identification will provide you with a smooth access control experience without compromising on security.

WE'VE GOT YOUR BACK



Videx launches new video monitor

London, UK

Videx has launched a new premium video monitor for its flagship door entry system the VX2200 and its 2-wire video VX2300 range.

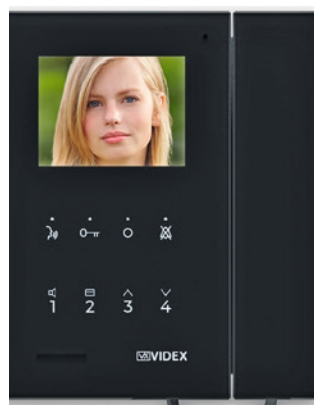
The video monitor, coupled with the 6-wire VX2200 or 2-wire VX2300, is offered as an ideal entry solution for smaller installations, such as apartments and houses, as well as multi-story apartment or office blocks.

The video monitor boasts a 3.5" TFT LCD monitor and eight soft-touch controls, four of which are programmable for features such as activating additional

outputs or intercommunicating with other devices in the same apartment or other apartments.

There are several different formats of the video monitor available such as hands free and those with a handset. The handset version includes hands free as well. A desk mount kit is also available for the handset version while the hands-free version can optionally be flush mounted.

Available in a polished white or polished black finish with backlit touch controls, the monitors have an elegant and sophisticated look and feel and include a wide



The video monitor boasts a 3.5" TFT LCD monitor and eight soft-touch controls.

range of enhanced features such as timed privacy, door recall and local doorbell and alarm inputs.

The new range of video monitors are easy to use and enable intuitive entry management across a wide range of properties and buildings making them an attractive choice for door entry, both for small and larger installations," he concluded.

Up to 10 monitors can be installed in the same apartment on the VX2200 system while the VX2300 supports up to four per apartment.

swm

TBS launches new 3D access on the fly

Pfaffikon, Switzerland

The newest addition to the **TBS** portfolio of biometric readers and solutions is the *3D Fly*. An innovative sensor offering on-the-fly user identification, meaning users do not have to physically stop at the device.

TBS 3D Fly is a touchless scanning terminal using our fingerprints. The AI-assisted hand recognition technology significantly increases user throughput without compromising on security.

The 3D Fly sensor captures a high-resolution picture of the entire hand and extracts the biometric features of up to four fingers,

resulting in superior recognition performance. This superior sensor technology – combined with fast data processing – identifies a person within a second. The process has been designed to be so fast that users can present their hands whilst walking towards 3D Fly and through the speed gate with no stopping no slowing down.

The high sensor precision is reflected by the large storage capacity of templates of over 10,000 users in identification (1:N) mode. In addition, biometrics can be combined with a PIN code to create a two-step authentication process

(1:1) for high-security sites and increase user count to 100,000.

The 3D Fly is designed for access control in high throughput environments, namely on-the-fly applications such as speed gates, turnstiles, sliding doors – any access point where security, convenience, and speed are critical. From financial institutions to government bodies, corporations, or critical infrastructures such as energy, healthcare, data, and logistic centres, the 3D Fly will be one of the most integral parts of access control – starting at the main entrance of such premises.



The new 3D Fly touchless biometrics access system from TBS.

The 3D Fly provides users with a secure authentication with a friendly user experience, requiring explicit user consent and cooperation every time they present their hand to the sensor. All the while being legally compliant without raising the ethical concerns related to passive surveillance capabilities of traditional face recognition technologies.

swm

New globally certified cameras for hazardous areas

Lund, Sweden

Two new explosion-protected cameras from **Axis Communications** are designed to monitor vast areas and send an alert whenever fire or smoke is detected. Ideal for Health, Safety, Environment (HSE) applications within potentially combustible areas, they offer worldwide Ex certification.

The Axis *XPQ1785* is a PTZ camera that offers total situational awareness, with 1080p with 32x optical zoom and continuous 360° pan and tilt at up to 200°/sec.

Whilst the Axis *XFQ1798* is a

fixed camera featuring a powerful, extremely light-sensitive 4/3" image sensor, with superior 4K resolution at 30 fps.

Both models have 5 years warranty and are globally certified Class I/II/III Div 1 and Zone 1,21, IIC, IIIC stainless steel (316L) cameras for use in hazardous areas (according to NEC, CEC, IECEx, ATEX, and more).

Featuring built-in smoke alert analytics, they constantly monitor for signs of smoke or fire in potentially combustible environments and send an alert if

fire or smoke is detected, helping to protect personnel and reduce hazards. Temperature range is specified at -60°C to 60°C (-76°F to 140°F).

These robust, explosion-protected cameras help to safeguard production processes from a distance, helping ensure personnel are only sent into restricted, potentially explosive environments when necessary. With mains power (110-230 VAC) and network (Ethernet + SFP port for fibre/coax) connected directly to the camera, there is no need for



Featuring built-in smoke alert analytics, the two new cameras monitor for signs of smoke or fire in potentially combustible environments.

an additional power supply.

The cameras are set to be available through Axis distribution channels in Q3/Q4 of this year.

swm

The Physical Security Business 2021–2026



This year's most important report

Don't miss out on this definitive report about the global markets for access control, video surveillance, intruder alarm and perimeter protection.

What is the status of these markets today and what can we expect until 2026?

The Physical Security Business 2021 to 2026 is a useful tool for all professionals engaged in managing, operating and investing in security technology companies – in particular for those with the intention to acquire, merge or sell companies.

For more information about the report: www.armediaint.com – click "reports"

armedia

AR Media International AB, Västberga Allé 32, 126 30 Hägersten, Sweden
Phone: +46 8 556 306 80, info@armedia.se, www.armediaint.com

Assa Abloy unveils new suite of Ecliq key options

London, UK

Assa Abloy has released a powerful new suite of programmable Ecliq keys, designed to provide even more robust, longer-lasting performance. An IP67 rating against water and dust ensures new Ecliq Basic, Ecliq Professional and Ecliq Connect keys can handle any weather.

Durability is ensured with up to a 10-year lifetime from a single, standard battery for the Basic and Professional keys. All three new keys are compatible with new and existing Ecliq wireless access control systems — and can be used alongside existing Ecliq keys.

Easy to update

By deploying new *Ecliq keys*, facility managers gain the flexibility to operate access control exactly how they choose. Both Ecliq Basic and Ecliq Professional keys can be updated at the desktop,

via wall readers or with mobile programmer. The Professional key adds acoustic feedback to the Ecliq Basic's LED key feedback.

A third new member of the family, the new Ecliq Connect key will be released soon and may also be paired with a smartphone app to update access rights from anywhere. A security administrator simply updates the system; the keyholder transmits new access permissions from phone to key via an encrypted Bluetooth connection. A key battery typically lasts two years or up to 2,000 connections.



All three new Ecliq programmable keys are IP67-rated with a long battery life

Allround cylinder

A fully electronic extension of Assa Abloy's award-winning Cliq access control system, Ecliq is built around precision-engineered wireless locks and high-end microelectronics. A standard battery inside each programmable electronic key powers the Ecliq cylinder or padlock — and encrypts data transfer between lock, key and system.

The Ecliq cylinder range brings almost any opening into an access control system. Robust,

durable Ecliq locks can secure lifts, machines, mailboxes, cabinets and more, with the same control as sensitive doors. Available in multiple sizes and formats — Ecliq cylinders help maintain security across an organisation.

Easy management

Managing Ecliq is fast and flexible. Existing keys are programmed with the same easy-to-use software and hardware as the three new Ecliq keys. Security managers have a choice between a local software installation (Cliq Local Manager) or cloud-based Cliq Web Manager.

Because Ecliq keys are powered by standard batteries, they can extend powerful electronic access control anywhere — far beyond the reach of electric cabling. Cylinders and padlocks operate safely between -25°C and 85°C, indoors and outdoors.



Hanwha adds 3 intrinsically safe cameras to line-up

Chertsey, Surrey (UK)

The long-range IR illuminator built into the *TNO-6322ER* and *TNU-6322ER* models allows night-time surveillance at a distance of up to 200m.

Hanwha Techwin, a global supplier of security solutions, has announced the launch of three NDAA compliant explosion-proof camera models (*TNU-6322E*, *6322ER*, *TNO-6322ER*) designed to operate safely even in industrial locations with highly volatile atmospheres.

The intrinsically safe cameras are contained within IECEx and ATEX certified stainless steel

housings, which have the ability to prevent any sparks generated by the camera escaping the device and igniting gases or other ignition sources in the environment.

TNU-6322E/6322ER models feature 360° endless panning and 180° tilting, and, combined with powerful 32x (4.44 - 142.6mm) optical zoom lenses, these cameras will reach into every corner of a large industrial site.

2MP high-quality resolution guarantees sharp and clear image capture and Hanwha's wide dynamic range (WDR) technology improves the accuracy of images

in scenes containing a challenging mix of dark and bright areas by compensating differences in brightness.

For external installations an onboard defog function ensures clear images can be achieved in all weathers, whilst the long-range IR illuminator built into the *TNO-6322ER* and *TNU-6322ER* models allows night-time surveillance at a distance of up to 200m. There is also a gyro sensor, which drastically reduces motion blur caused by vibration, and therefore ensures stable images even in the most challenging environments.



The long-range IR illuminator.

Embedded WisestreamII compression technology effectively reduces data size, whilst still maintaining optimum image quality, thereby minimising bandwidth requirements. In addition, the cameras are IP67 certified water and dust resistant and IK10 certified vandal-proof.



Mirasys adds new LPR plug in for VMS

Espoo, Finland

Mirasys, a provider of open platform video management software, has launched the company's latest plugin - *Mirasys Easy LPR*.

The Mirasys License Plate Recognition (LPR) plugin is a VMS Spotter add-on product that provides camera based vehicle identification that automates

processes based on recognising license plates.

Key benefits of the new add-on include the ability to track and regulate access and to trigger alarms based on access control. It also enables the system to optimise and eliminate manual processes whilst it is designed to

additionally support a wide range of different application scenarios.

Key features offer real-time vehicle monitoring, multiple license plate search criteria with a single camera. Users are also able to manage number plate lists, for example authorised white lists and unauthorised or warning for

black listed numbers. Number plates can be imported and exported, and number plate lists can be uploaded to the cameras.

In addition there are options for alarm triggering such as other plate detected; black list plate detected; white list plate detected.

Hikvision launches LPR cameras

City of Industry, Ca (USA)

Powered by Hikvision's Deep Learning algorithm, the new Deepinview LPR G3 cameras offer the ability to provide detailed wide-area surveillance with the added benefit of on-board analytics.

Deepinview LPR G3 cameras are designed with the ability to learn license plate information and recognise a broader range of vehicle plates than conventional LPR systems. Their powerful analyt-

ics also analyse vehicle attributes, including colour, to enhance the efficiency of video searches to ensure highly accurate vehicle identification. The combined performance and intelligence of the new Deepinview LPR G3 cameras can help reduce false alarms by as much as 95 percent by accurately classifying vehicles and human attributes, while ignoring innocuous motion events, such as blowing tree limbs or roaming animals.

Unlike traditional surveillance cameras, Deepinview LPR G3 cameras' unique design enables clear viewing angles without the cumbersome position adjustments

common to other systems. Another advantage of the new Deepinview LPR G3 cameras is their ability to produce clear images in dark environments using high light compensation (HLC). This technology reduces glare and enables the cameras to capture precise visual data, even with strong overexposure or backlighting.

Additional features include a 4 MP image sensor for high-resolution images with an automatic iris to maintain quality images in changing lighting conditions, and H.265+ compression to reduce bandwidth and storage requirements. Deepinview LPR G3 cam-



Deepinview LPR G3 cameras are designed with the ability to learn license plate information and recognise a broader range of vehicle plates than conventional LPR systems.

eras are also configured in a vandal-proof IK10 housing with NEMA 4x anti-corrosion coating to protect the units in harsh environments. The series includes three lens options with a total recognition range of 2m (7 ft.) to 60 m (197 ft.) 

Axis launches three ways to accelerate forensic search

Lund, Sweden



The Onvif Profile M offering is available as a native integration within Centralized Search for Milestone and Siemens Siveillance.

Axis Communications has announced the global availability of three integrations that use metadata from Axis devices to enable forensic search investigations in partner video management systems Milestone Xprotect and Siemens Siveillance.

Each of the integrations streamlines the search for objects or events in a scene using metadata sent from Axis devices. Investigators can pinpoint a single incident from archives of video footage, reducing analysis time from hours to minutes or seconds.

The three forensic search integrations include Axis Optimizer forensic search based on metadata about motion of objects in a scene; Axis Optimizer forensic search using object classification metadata from Axis Object Analytics; and, Onvif Profile M open object classification using metadata from Axis Object Analytics. The first two

offerings being globally available via Axis Optimizer.

The motion-based integration enables searches of video recordings based on moving objects, people and events in a scene. It is ideally suited for investigations that begin with only a minimal number of known details, for example where the only known detail is the location of an incident.

The object classification-based Axis Optimizer forensic search integration suits searches involving a broader range of known details about objects or people in a scene. Based on metadata generated inside Axis cameras with deep learning

processing units, a group of pixels can further classify objects by more refined description types or attributes. For example: a specific type of vehicle (car, truck, bike, etc.).

The Onvif Profile M offering is available as a native integration within Centralized Search for Milestone and Siemens Siveillance. Released in June 2021, it is based on Axis OS 10.6 and thus supported by a broad and growing range of Axis products. It enables standardised streaming of metadata and event sending from edge-based analytics applications in a best-of-breed multi-vendor surveillance system. 

Eagle Eye gains SOC 2 Type 2 and ISO 27001 certification

Austin, Tx (USA) and Amsterdam, The Netherlands

Eagle Eye Networks has completed the SOC 2 (System and Organization Controls) Type 2 examination, a rigorous security standard, which certifies that Eagle Eye Networks policies and procedures securely protect and manage customer data. The company also announced it has completed conformance with ISO 27001 security standards.

The SOC 2 Type 2 audit evaluated internal controls over six months to ensure that Eagle Eye Networks satisfies the Trust Services Criteria defined by the American Institute of Certified Public Accountants (AICPA). The criteria include security, availability, processing integrity, confidentiality and privacy.

"Our customers value the priority Eagle Eye Networks places on data security and cyber security; it is a foundation on which our company was built and a responsibility we take very seriously," states Dean Drako, Eagle Eye Networks CEO. "This important audit reinforces our commitment to our customers and provides independent valida-



Dean Drako, CEO, Eagle Eye Networks.

tion of our ongoing efforts to meet and exceed industry standards."

Eagle Eye Networks originally successfully completed the SOC 2 Type 1, in December 2020. 

Launch of industry's first cloud-native multi-sensor camera

London, UK

Ava Security is planning to release Ava Quad in the 2nd quarter of 2022. According to the company this will be the first cloud-native multi-sensor security camera on the market and will further expand the suite of cloud-connected video monitoring tools available on the Ava Aware platform.

Multi-sensor security cameras are designed to provide 360° visibility through multiple sensors, which is advantageous for customers looking for multi-angle coverage over wide outdoor or indoor areas, such as large crossroads, parking lots, campuses, and stadiums. With more area covered by a single device, multi-sensor cameras are also more cost and time effective

when it comes to installation and maintenance. However, until now, multi-sensor cameras have only been available for on-premise instalments, which has meant a lack of flexibility and remote access and left cameras vulnerable to out-of-date software.

Pioneering multi-sensor camera

The launch of Ava Quad, expected in Q2 of this year, will bring the first multi-sensor security camera in the cloud to market. Customers will benefit from easier access to security data and in-built video and audio analytics, which further reduces costs for organisations by cutting the time and staff needed

to analyse the footage. It also improves response to incidents with machine learning algorithms that can identify critical events before they escalate. Additionally, it brings the ability to store forensic details that customers might need to detect threats without the additional burden of storing large volumes of footage.

Ava Quad is the latest in the suite of intelligent cloud security cameras added to the Ava Aware video security data platform.

"Ava Quad marks another market-first for Ava Security, as we continue to add to our world-class portfolio of cloud-native cameras. This cloud multi-sensor camera will round out our line-up

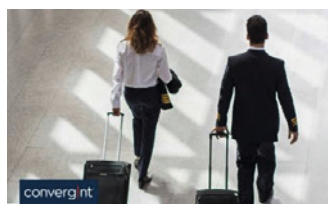


Ava Security is planning to release Ava Quad in the 2nd quarter of 2022

of video monitoring tools, as we continue to lead the industry in the transition from on-premise to the cloud—delivering storage, cost, AI, and analytics benefits. The continued growth of our product portfolio bolsters our position as the most open security platform in the market," comments Tormod Ree, CEO and Co-Founder of Ava Security. 

Convergint and Genetec team up to streamline airport badging system

Chicago, IL (USA) and Montreal, Canada



Streamlining the airport badging process allows organisations to operate more efficiently.

Convergint recently deployed a turnkey, streamlined badging solution at a large airport in Southwest United States. Together, Convergint worked with Genetec to ensure the safety and security of the airport's staff, passengers, and facilities, while improving operational efficiencies and compliance.

To keep airport employees

and passengers safe, airports must comply with strict regulations regarding the credentialing of staff through complex and time-consuming badging processes. All individuals needing access to secure areas of commercial airports must undergo background checks before being granted badges that allow them unescorted access to secure areas. This application process can be inefficient, paper-driven, prone to error, and overly complex, so it is beneficial to automate and simplify it.

Minimizing human errors

Some examples of the main benefits derived from the system include minimizing the potential for human error that comes with

disparate systems and manual processing; the ability to meet audit and compliance requirements set by authorities, such as the TSA and FAA; eliminating system upgrade issues that come with integrating multiple systems; and, the benefit of customised dashboards to showcase insights, such as real-time applicant status, to improve awareness of airport badging operations and make more informed decisions.

Managing badging lifecycles

With sophisticated software and a truly unified platform that provides complete means of managing badging lifecycles from start to finish on a single pane of glass, streamlining the airport badging

process allows organisations to operate more efficiently. All this can result in lower overhead costs, reduced system and server maintenance, improved operational efficiencies and effective regulatory compliance.

A complete package of services

With this system Convergint provides customisable, scalable security solutions for aviation infrastructure to enhance operational awareness and optimise the passenger experience. Paired with end-to-end security services, Convergint offers comprehensive support, including asset management, monitoring, cyber security, and preventative maintenance. 

RTI and Ksenia partner on technical integration

Ripatransone, Italy

RTI and **Ksenia** have partnered to create a new driver to manage home automation applications, by developing an integration between the *Ksenia Lares 4.0* control unit and the RTI controller.

RTI allows total control of any intelligent home automation environment, from residential to commercial, focusing on customised automation. The goal

is to create solutions that can automate, and therefore simplify, the control of audio, video and other aspects that are part of Home Entertainment.

The driver was developed to integrate the Lares 4.0 system into the RTI platform, interfacing thanks to the supervisor plugin. The integration currently provides for the activation / deactivation of

the security system and the execution of the various scenarios such as inclusion / exclusion of zones; arming / disarming of the single partition; on / off and switching of outputs, manageable from the keyboard after entering the user PIN; status management with relative run-time update of the icons on the graphic map.



The driver was developed to integrate the Lares 4.0 system into the RTI platform, interfacing thanks to the supervisor plugin.

Security Events



Crowded event. Sectech Norway was successfully organised on the 9th and 10th of March 2022.

April

 **25-27 April**
Securex Poland - Poznan Poland
Venue: MTP Poznań EXPO
Organiser: MTP Group
Tel: +48 (0)61 8692000
Email: securex@grupamtp.pl
Website: www.securex.pl/en

 **27-29 April**
Secutech - Taipei, Taiwan
Venue: Venue: Taipei Nangang Exhibition Center
Organiser: Messe Frankfurt
Tel: +886 2 8729 1099
Email: services@secutech.com
Website: secutech.tw.messefrankfurt.com/taipei/en.html

May

 **10-12 May**
Securex West Africa 2021 - Lagos, Nigeria
Venue: Landmark Centre
Organiser: Montgomery Group
Tel: +44 (0) 20 7886 3048
Email: ben.dale@montex.co.uk
Website: www.securexwestafrica.com/

 **17-19 May**
IFSEC 2022 - London, United Kingdom
Venue: ExCeL London
Organiser: Informa PLC
Tel: +44 (0)20 7921 8166
Email: ifsecustomerservice@informa.com
Website: <https://www.ifsecglobal.com/event/en/home.html>

 **25-26 May**
EXPOKOS - Pristina, Kosovo
Venue: Emerald Convention Center
Organiser: CEO shpk Congress & Event Organization
Tel: +383 (0) 38 516 013
Email: info@ceokos.com
Website: www.ceokos.com/expokos/en/

 **31 May - 2 June**
Securex South Africa - Johannesburg, South Africa
Venue: Gallagher Convention Centre
Organiser: Montgomery Group
Tel: +27 10 003 3082
Email: zeldaj@specialised.com
Website: www.securex.co.za/

 **31 May - 2 June**
Eliaden - Lillestrøm, Norway
Venue: Norges Varemesse
Organiser: Eliaden
Tel: +47 23087700
Email: post@eliaden.no
Website: www.eliaden.no/

June

 **20-25 June**
INTERSCHUTZ - Hannover, Germany
Venue: Hannover Exhibition Grounds
Organiser: Deutsche Messe
Tel: +49 5118931404
Email: info@tradefairagency.se
Website: www.interschutz.de/en/

July

 **6-7 July**
Homeland Security Expo - New Delhi, India
Venue: Pragati Maidan
Organiser: NEXGEN EXHIBITIONS
Tel: +91-11-41536990
Email: mukesh@nexgenexhibitions.com
Website: <http://homelandsecurityexpo.in>

 **6-7 July**
Police Expo - New Delhi, India
Venue: Pragati Maidan
Organiser: NEXGEN EXHIBITIONS
Tel: +91-11-41536990
Email: ashish@nexgenexhibitions.com
Website: <https://internationalpoliceexpo.com/>

August

 **24-26 August**
Intersec Buenos Aires - Buenos Aires, Argentina
Venue: La Rural Trade Center
Organiser: Messe Frankfurt Argentina
Tel: +54 11 4514 1400
Email: intersec@argentina.messefrankfurt.com
Website: www.intersec-buenos-aires.ar.messefrankfurt.com/buenos-aires/en.html

 **29 August - 1 September**
Defense & Security 2021 - Bangkok, Thailand
Venue: IMPACT Exhibition and Convention Center
Organiser: GML Exhibition (Thailand) Co., Ltd.
Tel: +66 (0) 2036 0500
Website: www.asiandefense.com

September

 **13-15 September**
Intersec Saudi Arabia - Riyadh, Saudi Arabia
Venue: Riyadh International Convention & Exhibition Center (RICEC)
Organiser: Al-Harthy Company for Exhibitions (ACE)
Tel: +971 4 389 4500
Email: intersec-KSA@uae.messefrankfurt.com
Website: www.intersec-ksa.com

 **20-23 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: https://www.security-essen.de/impetus_provider/

October

 **25-27 October**
Skydd - Stockholm, Sweden
Venue: Stockholmsmässan
Organiser: Stockholmsmässan
Tel: +46 8 749 4100
Email: info@stockholmsmassan.se
Website: www.skydd.net
Visit AR Media at Skydd

November

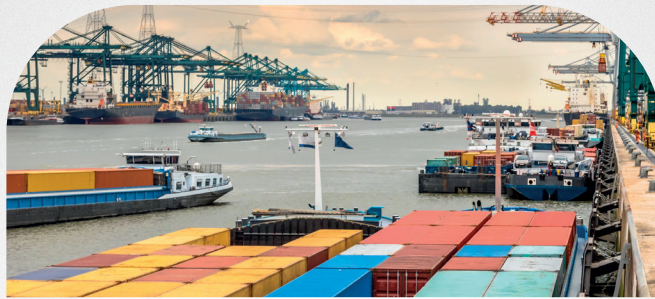
 **30 November - 2 December**
Secutech Thailand - Bangkok, Thailand
Venue: Bangkok International Trade & Exhibition Center (BITEC), Bangkok
Organiser: Messe Frankfurt New Era Business Media (MFNE)
Tel: +886 2 8729 1099 ext 531
Email: Israel.gogol@newera.messefrankfurt.com
Website: www.secutechthailand.com

2023

 **17-19 January**
Perimeter Protection - Nurnberg, Germany
Venue: Exhibition Centre Nuremberg
Organiser: Nurnberg Messe GmbH
Tel: +49 911 8606 8499
Email: perimeter-protection@nuernbergmesse.de
Website: www.perimeter-protection.de/en

HIKVISION®

Big picture and details
in one view.



TandemVu
P T Z C A M E R A S



SF8C

SE7C



Headquarters
No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
Business: overseasbusiness@hikvision.com
Technical Support: support@hikvision.com



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



hikvisionhq



Hikvision Corporate Channel