

DETEKTOR



International

Publisher's comment

**This is what we can
expect from 2023**

The Security Technology Market

**Incident and emergency management
market to hit \$163 billion by 2027**

**Shift to interactive systems drives
the market for home security systems**

**Racz, Gren and Drako discuss
future video surveillance trends**

Business news

**Bosch wins contract for innovative
building project in Poland**

SPECIAL EDITORIAL FEATURE 1:

PERIMETER SURVEILLANCE
Technology-driven sub-sector with challenges

SPECIAL EDITORIAL FEATURE 2:

ACCESS CONTROL
Cyber security – an important factor for growth

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
Elektravägen 14 • 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 €26
 +46 8 556 306 80

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

Rachel Ward Owens, Markus Lahtinen,
 Jonny Sjöberg, Lennart Alexandrie
info@armedia.se

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Deniz Baykal
deniz.baykal@armedia.se

Printing

Stibo, 2023



Lennart Alexandrie, Publisher

This is what we can expect from 2023

There is no doubt that 2023 is a year that breathes a lot of uncertainty. 2022 did not just become a year of post-pandemic recovery. Russia's brutal attack on Ukraine left its mark on the year and is also a strong inhibiting factor for global economic growth in 2023.

At the start of 2023, we see increasingly clearly how rising interest rates and inflation, largely driven by continued high energy prices, are slowing down the economy. Add to that a global geopolitical concern that China's threat to the island nation of Taiwan will develop into an armed conflict.

At the same time as all this, we are grappling with a growth in serious crime, where not least cyber attacks are a major problem for both authorities and companies. Add to that gang crime that has become increasingly brutal and established in many countries, not least Sweden, my home country, which has become Europe's top tier when it comes to fatal shootings in just a few years.

So how will all of this be reflected in the security market in Europe and the rest of the world in 2023? It is not an easy question to answer.

Since the pandemic, the ongoing component shortage is already a hindrance to technology deliveries in the security market. How long that situation lasts remains to be seen. Downsizing and bankruptcies as well as reduced construction are also negative factors and will obviously have an impact on demand generally. At the same time, protection against crime has been given increased priority, not least when it comes to critical infrastructure.

So what can be predicted with reasonable precision regarding the physical security market in 2023? It is safest to stick to the two megatrends that stand out most and can be expected to characterise the development of the market for electronic systems for physical security.

The development of AI is perhaps the main megatrend. The reason for that is simple – AI streamlines and revolutionises companies, cities and countries by enabling the automation of processes and services. AI will in all probab-

ity contribute to the fact that many security services that are currently based on manual surveillance will be replaced by technology-based solutions. The AI trend in the security market is most clearly reflected in the video surveillance sector, but the ID and access control sector is also driving the AI implementation in security systems.

Cyber security is – along with the technology trend AI – the biggest megatrend in terms of its importance and impact on the physical security market. It is driven by end customers' constant concern about cyber attacks. A nightmare scenario is that financially driven criminals hack a security system and demand a ransom. Another is if a nation-state wants to create instability and cause damage in a country by hacking authorities or breaching security systems for critical infrastructure. Even in the field of cyber security, the video surveillance manufacturers have been driving and working hard to strengthen the cyber security of their products. However, there is much more to be done here, not least to increase the cyber security knowledge of both the system suppliers and their customers. Therefore, cyber security will continue to be a significant megatrend not only in 2023 but also in the years to come.

Another trend that will characterise 2023 is the development towards open platforms, driven by the market's need for integration and interoperability. Service-based business models are also an obvious trend, not least as consequence of the growing adoption of cloud solutions. Increasing usage of the industry's technology for more than security purposes comes also as sub-trend due to the acceptance of cloud solutions and development of service-based services. With data collecting, security technology vendors will be able to add values that support customers' ambitions to streamline operations, work sustainably, save energy costs and contribute to increase profitability.

Finally, it will be interesting to see how the M&A market will be in 2023, but also to follow the first year with Securitas Technology – namely the merger of Securitas and Stanley Security – arguably, one of the biggest global acquisition events in many years.



3 Publisher's Comment. This is what we can expect from 2023.

6 Security Technology Market.

Security market remains resilient in spite of unprecedented challenges.

7 Shift to interactive systems drives the market for home security systems

8 Incident and emergency management market to hit \$163 billion by 2027.

10 Special Feature: Perimeter Surveillance

The global perimeter security market is projected to grow from \$70.8 billion in 2022 to \$100.2 billion in 2027.

15 Business News. Bosch wins contract for innovative building project in Poland.

18 Security Technology Insights. Super-entrepreneurs on future trends in video surveillance.

22 Special Feature: Access Control

Cyber security has become increasingly important for the access control industry.

31 Security Events. Calendar for physical events.



Security Technology Market

Security market remains resilient in spite of unprecedented challenges, according to James McHale, managing director of Memoori.

Page 6



Security Technology Market

An increase in global natural disasters are expected to boost the incident and emergency management market.

Page 8



Special Feature: Perimeter Surveillance

The global perimeter security market is projected to grow from \$70.8 billion in 2022 to \$100.2 billion in 2027.

Page 10



Super-entrepreneurs

Martin Gren, Pierre Racz and Dean Drako in discussion

Page 18



Special Feature: Access control

Cyber security has become increasingly important for the access control industry.

Page 22

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.

Security market remains resilient in spite of unprecedented challenges

A new research report from Memoori, “The Physical Security Business 2022 to 2027”, shows that the global market for physical security products (access control, video surveillance, intruder alarm & perimeter protection) has demonstrated both resilience and adaptability in the face of growing geopolitical tensions and looming economic recession.

Stockholm, Sweden

Trade tensions between China and the US have seen a series of legislative moves that have disrupted the flow of both physical security products and key product components. These tensions are also spilling over into Europe, states Memoori.

“If further trade barriers are erected, we will see a polarisation of the physical security global market,” states James McHale, managing director of Memoori.

9% growth in 2022

Memoori estimates that annual revenues from the physical security product market increased over 9% in 2022, rising to \$42.3 billion. Going forward growth will be tempered somewhat, aver-

aging 6.5% per annum to 2027.

Video surveillance dominate

Video surveillance makes up nearly 58% of the market in 2022, with China continuing to dominate sales in this sector, accounting for just under one-third of the total global market. Whilst China’s Sharp Eyes projects are winding down, Memoori analysts suggest that continued state investment into smart cities as well as programmes such as the Safe China initiative should continue to drive sales of security products in China.

Video analytics trend becomes stronger

The development and commer-



James McHale, managing director and founder of Memoori.

cialisation of new technologies continue to drive growth in the physical security market. Memoori’s recent analysis of Artificial Intelligence (AI) in Smart Buildings found that the security

market, and particularly video analytics generated the largest share of overall AI revenues in smart buildings, representing just under 50% of total sales in 2020 at \$558 million.

Little appetite for 5G

However, the research explains that clearly not all new technology has the same impact. For example, despite various projections, Memoori finds little current momentum or market appetite for the deployment of 5G wireless video surveillance at scale. The research company estimates that the introduction of 5G for video surveillance data transmission will take at least another 5 years to achieve the levels of coverage, reliability and falls in cost to have any kind of real impact.

Footnote: To order “The Physical Security Business 2022 to 2027” or just to get more info about the report: Log into www.armedia.se/en/products_other_physicalSecurity.asp

Gunshot detection systems market projected for \$7.8 billion by 2027

According to Marketsandmarkets the gunshot detection systems market is projected to grow from \$4.9 Billion in 2022 to \$7.8 Billion by 2027, at a CAGR of 9.7% from 2022 to 2027.

Northbrook, IL (USA)

To efficiently detect and track threats, according to the analysts, advanced technologies like artificial intelligence will merge optical and acoustic data, and in the upcoming years, these innovations are anticipated to accelerate market expansion.

North America takes the largest market share

The gunshot detection systems market industry has been studied by the Marketsandmarkets

researchers in North America, Europe, Asia Pacific, Middle East & Africa and Latin America. And, perhaps unsurprisingly, it is the North American market that accounted for the largest market share in 2022. Law enforcement agencies are also increasingly using the technology, particularly in this region. And the analysts suggest that market growth in the upcoming years is probably going to be driven by increased spending in border security. These tools can aid

border patrol agents in detecting and stopping smuggling, infiltration, and illegal immigration.

Applications, solutions and players

Fixed Installations are proving to be the most popular, and account for the largest share of the market in 2022. The advanced fixed Gunshot Detection Systems are being installed around the city to enhance the civilian security and also to safeguard the country border.

In terms of solutions the system market is most dominant. For example, a system would include the sensors and hardware required to detect gunshots. Numerous sensors, including display systems

and acoustic sensors, are used in gunshot detection systems.

The outdoor segment is projected to dominate market share in the system segment during the forecast period. The need for gunshot detection systems is rising due to an increase in firearm events throughout the world.

Major players

Some of the major players operating in the gunshot detection systems market include Shot spotter, Shooter Detection Systems, Raytheon Technologies Corporation, and Qinetiq Group, all based in the United States, and then ACOEM Group and Thales both from France, and Elta Systems from Israel.

Shift to interactive systems drives the market for home security systems

In a new report on home security systems and small businesses, Berg Insight predicts that the number of professionally monitored alarm systems in Europe will grow at a compound annual growth rate (CAGR) of 4.5 percent, from 17.6 million in 2021 to 21.9 million installations in 2026.

In North America, the number of monitored alarm systems is forecasted to grow at a CAGR of 3.0 percent, from 33.6 million in 2021 to 39.0 million in 2026.

The report states that mobile connection is rapidly becoming a standard function in security alarm systems for the consumer and small business markets.

Berg Insights estimate the numbers of cellular IoT connections for home and small business security systems in Europe and North America is growing at a CAGR rate of 6.7 percent from 39.9 million in 2021 to 55.2 million in 2026.

Three categories

Security systems for small businesses and private homes can be divided into three main categories:

• Local security systems.

It emits an alarm sound to alert the surroundings and scare off intruders. Such systems are not monitored and cannot be accessed remotely.

• Self-monitored security system.

The system is connected and when an alarm goes off it informs the owner of the premises by sending a text message, email or push notification through a smartphone app.

• Professionally monitored security systems.

The system is connected to an Alarm Receiving Centre (ARC). When an alarm is triggered, the ARC can dispatch a security patrol and contact emergency services.

The market vendors

The traditional home and small business security systems market in Europe and North America is fragmented. It is served by specialist home security companies such as ADT, Verisure, Brinks Home (Monitronics) and Sector Alarm, but also by security service companies such as Prosegur, Securitas and G4S; telecommunications and cable television companies such as Comcast, Telus, Cox Communications and Bell Canada. Furthermore it is also served by utilities, banks and insurance companies such as EPS (Crédit Mutuel), Crédit Agricole and Groupama.



Martin Bäckman, Senior Analyst at Berg Insight.

DIY market vendors

Traditional home security systems include professional alarm monitoring. Providers of DIY home security systems include Simplisafe, Frontpoint, Ring (Amazon), Yale (Assa Abloy), Arlo, Somfy, Scout Security, Canary, Minut and Wyze Labs. DIY security systems typically include self-monitoring as a standard feature and professional alarm monitoring services are offered as an option.

ADT and Verisure the market leaders

ADT and Verisure are the two largest providers of professionally monitored alarm systems for homes and small businesses, with 6.3 million and 4.3 million customers respectively at the end of 2021.

ADT is only active in the US while Verisure is active in 13 European countries and four countries in South America.



Martin Bäckman also emphasises that security cameras are now also commonly part of new home security system installations.

Shift to interactive systems

Martin Bäckman, Senior Analyst at Berg Insight, comments on the report.

“The market for security systems for homes and small businesses in Europe and North America continues to grow steadily, driven by a shift to interactive systems that provide increased safety and convenience for users”, he says.

Cameras add value

Martin Bäckman also emphasises that security cameras are now also commonly part of new home security system installations, as the price for such devices has dropped in recent years and developments of video software has enabled a greater value for home and small business owners.

“Modern security camera solutions can distinguish between humans, pets, vehicles and other objects and notify the user only if there is an actual threat to the premises” continues Martin Bäckman.

The cameras provide an extra layer of security as the security system extends to the perimeter of the property.

“Security and safety are basic human needs and therefore the home and small business security system market is anticipated to stay strong in the coming years despite high inflation and rising costs of living and doing business”, concludes Martin Bäckman.



Photo: SpaceX-imagery / Pixabay

Incident and emergency management market to hit \$163 billion by 2027

According to a research report on the incident and emergency management market with a global forecast to 2027 from Marketsandmarkets, this sector is predicted to grow from an estimated \$121.4 billion in 2022 to \$163.6 billion by 2027, at a compound annual growth rate of 6.2%.

Northbrook, IL (USA)

An increase in global natural disasters is expected to boost the market. However, according to the findings, disparities in costs of incident and emergency management systems may hinder the market growth.

Emergency/mass notification solutions enable organisations to quickly inform the masses in a particular area, building, or commercial installation about the occurrence of an emergency and the most likely action that should be taken. The mass notification system usually sends alerts through cell phone notifications, apps, emails, and texts to notify the masses individually and reduce the panic and chaos among them. The system can further help propagate messages, advising rescue and relief agencies and law enforcement agencies about the due course of engagement during an emergency.

There has been a heightened demand for MNS to protect, alert, and inform people in an emergency. Mass notification systems are designed to protect, alert, and inform resources and people with critical alerts (natural disasters, HAZMAT) when it matters most.

Utilities vertical is at most risk

A natural disaster is a global phenomenon that severely impacts people and resources. Such adverse events have a major impact on energy and utilities companies and cause disruptions in their services, creating significant ripple effects. The energy and utilities vertical comprises thermal, nuclear, solar, wind, and hydropower plant infrastructure, which are of acute importance to the country. Hence, this vertical plays a major role in the growth of various developing

and developed countries.

Business alerts and notifications related to power outages, work shifts, and workflow management are also provided by incident and emergency management solutions, specifically in the energy and utilities sector, for streamlining business operations and enabling robust business continuity. These solutions further help emergency and security teams to execute evacuation or emergency management activities more efficiently.

Geographical outlook

The global incident and emergency management market is dominated by North America, which is considered the most advanced region in terms of the adoption of advanced incident and emergency management technologies. In recent years, this region has been increasingly exposed to man-made disasters, such as terrorist attacks, strikes and protests, and chemical attacks. These issues have pushed the region to adopt incident and emergency management solutions and services. Post the terrorist attacks, the DoD issued stringent norms related to the installation and management of mass notification systems in industrial

enterprises, public installations, and defence installations.

Most of the US law enforcement agencies, such as federal agencies, the Marine Corps, the US army, and defense, have deployed mass notification systems for instant intelligent alerts and quick response management.

Governments are focusing on incidents and emergency management in their countries. For example, the Government of Canada is extending the use of its incident management system Long-Term Care Table mandate, which is also expected to drive the growth of the incident and emergency management market.

Key players

The major vendors in the incident and emergency management market, named by the Marketsandmarkets include Honeywell, Lockheed Martin, Motorola Solutions, Siemens, NEC, IBM, Hexagon, Collins Aerospace, Esri, LTI Mindtree, Johnson Controls, Alert Technologies, Everbridge, The Response Group, Haystack Technology, Metricstream, BlackBerry, Eaton, Veoci, Noggins, 4C Strategies, Resolver, Arcos, Juvare, Logicgate and Onsolve.



FlipX Series

NOW THERE ARE TWO WAYS TO DETECT IN JUST ONE SENSOR



The **OPTEX FlipX** is a new series of Grade 2 and Grade 3 detection sensors suitable for any indoor installation site, from residential, right the way through to logistics and high security locations. Boasting a switchable lens that flips between wide to narrow detection, the sensors feature an innovative pyroelectric sensor that uniquely adapts to the human size and shape, dramatically cutting false alarms. Meanwhile, its flexible mounting height up to 3m and viewable LED indicator ensures easy set up. And thanks to the compact, sleek design, **FlipX** always blends neatly into any space.

For more information visit www.optex-europe.com



Intelligent video surveillance is considered to provide robust security against both conventional criminal attacks and terrorist attacks, which explains why video surveillance systems are predicted to continue having the largest share of the perimeter security market.



Perimeter security

– technology-driven sub-sector with challenges

Perimeter security is increasingly about proactivity. Fences and guards take all the glory, but it is with the rapid development of technology that 24/7 monitoring can become a reality. So how big is the market for perimeter security technology and how fast is it growing?

Detektor has looked at how Marketsandmarkets and Grand View Research respectively assesses the perimeter security market from a global perspective.

By Lennart Alexandrie

It can be assumed that the technology's improved capacity in combination with a favourable cost development on the products are strong contributory reasons why the perimeter security sub-sector has had a steady and high growth rate in recent years. But how is it then with the size of the market and the rate of growth?

Total turnover: \$65–70 billion

According to a new report by Marketsandmarkets, the global perimeter security market is projected to grow from \$70.8 billion in 2022 to \$100.2 billion in 2027 at a CAGR of 7.2 percent during the forecast period.

Grand View Research has the year 2021 as its starting point, when it is estimated that the perimeter security market had a turnover of \$59.21 billion. The average annual growth is estimated at 9.4 percent during the period 2022

to 2030. With that growth rate in 2021, Grandview Research's estimate of the market's total turnover landed at around \$65 billion.

It can be said that the two market research companies are quite close in their assessment of the market, despite that the parameters they use to define the market – in some cases – differ.

Critical infrastructure

Grandview Research claims that the increasing threat of terrorism and governments' need for effective security around their national borders are growth driving factors. Government investments in security also include government support for implementing various security systems in critical locations. As growth factors, Grandview Research also cites technological advances in the field of automation and the receptivity to new technologies, such as video analytics and drones

to give better results.

Marketsandmarkets believes that a global increase in crime is a significant factor, not least for the retail sector. Shopping centres and larger stores (especially in home electronics and car retail) see a need for enhanced perimeter security. But above all, it is airports, border controls and facilities for energy and water supply as well as other important infrastructure that account for the large investments in perimeter security.

AI drives growth

Another growth factor is the increasing demand for video surveillance, access control systems and other technology solutions that can streamline perimeter surveillance. Not least the increasing use of intelligent technology linked to artificial intelligence, such as Machine Learning (ML) and Deep Learning (DL), are strongly influencing growth factors.

Intelligent video surveillance is considered to provide robust security against both conventional criminal attacks and terrorist attacks, which explains why video surveillance systems are predicted to continue having the largest share of the perimeter security market.

Video surveillance systems dominate

Grand View Research highlights that the growing security con-

cerns have led to new multi-layer solutions for perimeter protection. Some of the technologies gaining popularity are electronic fences with sensors and integrated fiber optic intrusion detection systems.

The fact that digital technology has had a major impact on the market for perimeter security is confirmed by the fact that software-based video surveillance systems dominated the industry, accounting for the highest market share – more than 45.5 percent of global revenue in 2021.

Grand View Research believes – as does Marketsandmarkets – that video surveillance systems are the fastest growing segment on the market. Easy installation and countless application possibilities are factors that have resulted in the increased use of video surveillance systems.

Highest growth in APAC

According to Marketsandmarkets, Asia and the Pacific (APAC) has the highest growth as a result of escalating criminality and growing public anxiety, but also major investments in smart cities and infrastructure in the region are growth driving factors for perimeter security solutions in the APAC.

The APAC-countries with the fastest economic growth include China, Japan, India, Singapore, Australia and New Zealand.

Industry people in a panel discussion about perimeter security technology

In a recent video panel discussion, organised by Securityworldmarket.com, a highly experienced panel of participants shared their insights regarding the current state and the future of perimeter surveillance.

By Lennart Alexandrie

The participants in the panel discussion were all representing companies with a strong connection to perimeter surveillance.

- **Mark Cosgrave**, Divisional Director of Optex Security EMEA.
- **Sonny Hardarsson**, Sales Engineer at Axis Communications.
- **Robert Jansson**, Director of Sales for Nordics, Eastern Europe and South Africa at Stid Security.
- **Erik Nord**, Business Development Manager at Genetec.
- **Kenneth Nyström**, CEO of the system distributor Securify, specialised in perimeter surveillance.

Here follows a short summary of the panel discussion, that was moderated by Detektor's Editor-in-chief Lennart Alexandrie.

Commercial applications

Historically, this field of security is most associated with critical infrastructure, but demand the demand is also rising in commercial areas, which was the main focus of discussion.

"Retail is maybe not the first vertical you come to think of when discussing perimeter solutions, but the increase in online shopping has rapidly put more pressure on the logistical hubs, and the security for those," stated Kenneth Nyström, CEO of Securify, a system distributor, specialised in perimeter surveillance.

An important remark was also made on the changing modus operandi of the criminals, warranting the need for more advanced perimeter solutions.

"Every now and then, there are smash and grab incidents involving large vehicles enforcing the walls and barriers. It's over in a couple of minutes, driving the need for new approaches to mitigate this", stated

Kenneth Nyström and pointing to the need for very early detection.

"I call it beyond the defence line" he said.

Nuisance Alarms

The problem of nuisance alarms in security systems for high-security industrial applications is a critical issue that was also discussed. This can lead to unnecessary disruptions, wasted resources, and even compromise of the security system itself. Nuisance alarms seem to be more related to how installations are conducted than a technology problem. But how should an end-user know which supplier to choose when looking for an advanced perimeter surveillance solution that detects intrusions and ignores natural changes in the perimeter?

"There is nothing wrong with asking questions! Be a bit of a sleuth, be like Sherlock Holmes" was the recommendation to end-users, put forward by Mark Cosgrave from Optex.

The industry panelists were also agreeing that all players in the delivery chain probably could step up their efforts; end-users included.

Erik Nord from Genetec was further stressing the importance of consultants, but also the role of certifications and the partner-network managed by the leading security brands. Among the panelists there was also a consensus concerning the importance of continuous training among installers.

Different technologies

Perimeter surveillance has always been a tough task for the security industry, but the panelists pointed to numerous technological developments that have served to develop perimeter protection in past years. An example is Lidar technology, which uses laser light to measure



The online panel: Lennart Alexandrie (moderator), Kenneth Nyström, Securify, Mark Cosgrave, Optex, Sonny Hardarsson, Axis, Erik Nord, Genetec and Robert Jansson, Stid.

distances.

"By installing Lidar sensors along a perimeter, the technology can detect any objects or people that cross it and create a detailed 3D map of the surroundings", said Mark Cosgrave.

Additionally, radar technology – also used for object detection – can operate in adverse weather conditions and can detect threats at a longer range compared to other technologies.

"The combination of object detection technologies, for example radar, cameras and analytics, offer value in a broad range of use cases and applications," said Sonny Hardarsson from Axis Communications.

It also became clear that improvements in user experience and usability is findings its way into the perimeter surveillance mix.

"It has become a lot easier to set up analytics for the basic demands, fence-line detection for example. It is virtually effortless to set up today", said Erik Nord from Genetec.

Access control perspective

Robert Jansson, representing the access control dimension of perimeter protection, was asked to point out the advancements being made in his area of expertise.

"Two-factor authentication is coming to vehicles now. License-plate recognition is a cost-efficient and convenient method, that could be combined – depending on the hour – with optical authentication

as well as with encrypted UHF tokens, said Robert Jansson who also lifted the need to secure the identity of the driver.

"Who is driving the car? Two-factor authentication is coming to the driver-side of the vehicle now. And it is coming in a convenient way, meaning that the driver doesn't have to leave the seat. This has exploded over the past two years.

Cloud-Based perimeter security systems

It is often reported that moving perimeter security systems to the cloud can offer numerous benefits, including increased scalability, flexibility, and cost-effectiveness.

However, there are also risks associated with moving physical security systems to the cloud. One such significant risk is the potential for service outages or disruptions, which can leave organisations vulnerable to security breaches during periods when the cloud-based system is unavailable. Additionally, there is a regulatory risk – especially with the updated and various data protection acts coming into force in recent years.

Given the tailored solutions often required for perimeter surveillance, it is difficult to work with a standard solution, according to Kenneth Nyström.

"There are no silver bullets" he stated clearly and stated that "not every end-user is prepared to send data to the cloud".



Integrated security solution helps global logistics firm work safer and smarter

At one of the UK's larger distribution centres, security used to equate to a number of guards, backed up by a network of analogue CCTV cameras.

Today, a cutting-edge security technology solution is protecting the site against both internal and external threats, whilst also improving the safety of the work environment.

As rapid business growth saw an increase in the number of high-value items passing through the site, the global logistics and distribution specialist chose Acctive Systems to replace the system and secure this large and most important distribution centre.

Acctive Systems is one of the leading privately-owned integrators of electronic security systems in the UK, with an extensive experience within the logistics sector. With support from their trusted technology partner Axis, they started developing what would become a high security solution which would also deliver health and safety improvements and substantial cost savings.

Advanced levels of protection

The solution included installation of 180 Axis network cameras across a large 300 x 200 metre site, with onboard analytics used to differentiate between people and vehicles.

At the perimeter, automatic number plate recognition (ANPR) cameras serve to further enhance vehicle identification, helping to initiate smoother passage for authorised delivery trucks. IP audio speakers, triggered by cameras at the site perimeter, are primed to issue alarms or pre-determined and real-time alerts to deter criminal activity or trespassing.

"The system is very sophisticated with cameras, analytics, IP audio and access control all interconnected to guard against any

unexpected visitor. Our customer runs an incredibly slick operation, and this now extends to the security provision employed inside and out," states Andy Moseley, technical sales and technical designer at Acctive Systems.

Guarding against loss and insider threat

Inside the warehouse, cameras are positioned above giant roller-shutters for an ideal perspective of the main floor while also monitoring passage through the main access points. Axis' open-platform approach facilitates third-party access-control mechanisms and intruder alarms that seamlessly link to Axis' network cameras, IP audio solutions and centralised video management system (VMS).

With internal theft being of great concern, mini-dome cameras, positioned to cover the many packing benches, serve as a tool for profit protection that also doubles as quality control. High-definition video of the packing of all goods can be retrieved as required to solve any query or dispute.

"Imagine a situation where a truck goes to leave the premises but is short of an order. Distribution managers can now check an Axis recorder for video evidence from the packing area relating to that specific order, compare this with footage from the loading area, and quickly establish what has happened. This serves to help differentiate between a security-related situation or a genuine



Inside the warehouse, cameras are positioned above giant roller-shutters for an ideal perspective of the main floor while also monitoring passage through the main access points.

mistake, ultimately saving the business time and money," comments Andy Moseley.

Monitoring for health and safety

With trucks arriving and departing in quick succession, it is imperative that the fast-paced environment of the delivery and collection area is made as safe as possible. Staff need to always remain alert, which is where technology can help. The combination of cameras and IP audio technology helps to drastically reduce the likelihood of incidents occurring, and in the unfortunate event that one does occur, can provide vital evidence.

"On-camera analytics can be configured to detect anomalies in a scene and promptly address them, with IP audio speakers configured to warn of approaching vehicles or any situation that might prove hazardous," states Sean McNaboe, Key Account Manager at Axis.

"This serves to remind operatives of correct protocols and further improves health and safety standards across the site."

For health and safety, as well as security purposes, audio can be targeted towards relevant zones to ensure that the right person receives the message. When a fire drill is conducted, for example,

an alarm sounds which can be accompanied by an audio announcement, reminding the workforce in a certain area of the number and location of their muster point. Pre-determined doors can then be selected to open through the VMS software.

At the designated assembly area, operatives swipe their ID cards against a third-party proximity reader to engage the automated roll-call system which logs their attendance. In this way, the entire workforce can be accounted for swiftly and accurately in an automated way.

The power of Axis Site Designer

Acctive Systems has also utilised the capabilities of Axis Site Designer. This innovative web-based tool can simplify and streamline the design of security and surveillance systems, assist quotation workflows and make projects easier to specify, revise and implement. The application removes any guesswork and allows cameras to be virtually positioned and their coverage visually demonstrated. It helps to identify potential issues such as blind spots affecting the field of view and is also essential to ensure that onboard analytics function correctly.

Callum Ryder, Raytec on:

Comparing light types for perimeter surveillance systems

Raytec is a world leader in LED lighting for security and safety applications. In this article, Callum Ryder, Raytec marketing manager, offers his views on lighting requirements for perimeter surveillance systems.

Quality images are a necessity for any security system or transport monitoring application, including perimeter surveillance applications. Not only does the performance of the system rely on the camera and lens, but also on the quantity, quality, and distribution of available light.

“Light determines whether a subject can be viewed at all, and at what distance. The quality and direction of the light also controls the appearance of the subject. However, there are lots of different types and wavelengths of light available and to consider”, states Callum Ryder.

White-light

White-light is one of the most widely used wavelengths of light and is something we're all used to seeing and using in day-to-day life. A main advantage of using white-light as part of a security system is its ability to provide colour images, if being used with a colour camera. Identifying the colour of someone's clothes, hair, or other features, could provide crucial evidence for prosecution.

The defining characteristic of white-light illumination is that it is highly visible to the human eye, hence its use for general area illumination. For perimeter surveillance applications, this is also useful when using white-light as a deterrent to ward off potential intruders. On the contrary, if covert surveillance is the aim, white-light illumination is unlikely to be the answer.

Using constant white-light at night may not be suitable for all applications, due to the fact that the target area is lit up, and therefore, potentially assisting an intruder in undertaking a crime. When using white-light, consideration also needs to be given

towards light pollution.

“While the use of LED technology means the light can be targeted accurately, some applications may be restricted in their ability to use white-light for environmental reasons such as protecting the night sky or wildlife,” comments Callum Ryder.

Infra-red (850nm)

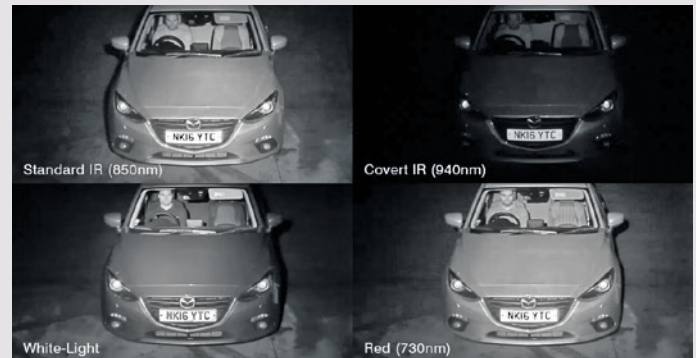
850nm is a semi-covert light and the preferred choice for most CCTV systems. Security cameras are most receptive to this wavelength of IR and, therefore, it gives the best night-time images. Being semi-covert, the illuminator does give off a slight red glow, visible up close or when looking directly into the light.

“However, for most applications this is not an issue and we would always recommend the use of 850nm over other wavelengths of IR. 850nm will provide the best night-time images and allow the camera to perform at its optimum,” says Callum Ryder.

Infra-red (940nm)

940nm is a fully covert wavelength of IR light. A 940nm illuminator does not emit any red glow, making it an option for applications where the red glow from an 850nm light is deemed unacceptable. However, the use of 940nm will mean a significant drop in image quality and achievable distances when compared to an equivalent level of 850nm light. The performance sensitivity of the camera will drop by as much as 50% compared to 850nm.

“If possible, we would always recommend the use of 850nm over 940nm. And when using 940nm, always ensure a suitable camera setup is being used,” comments Callum Ryder.



In tests conducted by Raytec for the purpose of seeing through windscreens, it is clear that 730nm light provides the clearest images to identify the individual within the vehicle, compared to the other tested wavelengths.

Hybrid

Another option which specifiers should consider is the use of hybrid illuminators. Hybrid illuminators provide an all-in-one solution, combining both IR (850nm) and white-light into a single unit.

“This means one illuminator can be used for both covert surveillance, and as a white-light deterrent. This is commonly used for perimeter surveillance systems where the end user would like to ward off an intruder before they commit the crime”, explains Callum Ryder.

FAR-RED (730NM)

While unlikely to be relevant for perimeter applications, a wavelength of 730nm (known as ‘Far-Red’), is becoming an increasingly popular choice for transport applications where driver or passenger identification inside the vehicle is required. Modern windscreens are designed to block out certain wavelengths of light. This is mainly to protect the occupants of the vehicle from ultraviolet (UV) rays but is also an attempt to keep the cabin cool by blocking a proportion of infrared (IR) light. 730nm is commonly used as less light is blocked by the windscreen.

Seeing through windscreen-test

In tests conducted by Raytec for the purpose of seeing through



Perimeter surveillance installation with Vario2 white-light illuminators from Raytec.

windscreens, it is clear that 730nm light provides the clearest images to identify the individual within the vehicle, compared to the other wavelengths discussed above. However, a 730nm illuminator does give off an obvious red glow, which could become distracting for drivers in certain cases.

“In an ideal world, the quality of images produced using 730nm could be achieved using an illuminator which gives off no visible light and, therefore, offers no distraction to the driver. However, in reality, the further down the spectrum one moves, the more light becomes visible to the driver,” concludes Callum Ryder.



Mark Cosgrave, Optex:

“Sensing technologies for detection can bring intelligence to the security system”

Perimeter protection is the first line of defence and is a key element of any security system. As with any intrusion, early detection is critical as it gives security teams the opportunity to anticipate any potential threats.

Mark Cosgrave, Divisional Director Optex Security EMEA, gives his views on the importance of using sensing technologies for effective perimeter protection.

Effectively monitoring perimeters requires security technologies to locate intrusions quickly and accurately. This can be particularly challenging for certain technologies as perimeters are exposed to external changing conditions.

“One of the main issues faced by security systems relying on AI and cameras with analytics is the number of nuisance alarms. Sensing technologies can efficiently solve this problem and are successfully deployed in many sites to improve the efficiency of surveillance and security system”, states Mark Cosgrave.

Challenging environment

Environmental factors such as rain, snow or extreme temperatures can indeed have a significant impact on the performance and reliability of some security technologies.

“Cameras can be affected by light conditions and can struggle to classify objects in spaces where the field of view is narrow – for instance outdoor corridors and areas with occlusions. Foliage and wildlife can also be triggers of false alerts.”

Nuisance alarms

As a solution to minimise nuisance alarms in certain areas of the perimeter, security teams may consider excluding entire zones, which then leads to the problem of keeping wide areas unsecured and vulnerable to intrusion, which troubles Mark Cosgrave.

“Excessive false alarms become costly as it requires more

resources to verify activations, but also requires installers to keep coming back for tweaking the system, which is unfortunately inefficient and frustrating. Systems with excessive false alarms become unreliable which means surveillance personnel are not confident on the solution, and this can lead to an even worst outcome: failing to react to real intrusions,” he says.

A reliable system

Mark Cosgrave claims that the performance of the security system should not be compromised by lighting, weather or other outdoor conditions. He emphasises that sensing technologies have been specifically designed to ‘detect’ and are not affected by light, variable temperature or external factors such as wind, rain or snow.”

In addition, sensors can learn and adapt to the environment, enabling them to filter out common causes of nuisance alarms.

“For instance, continuously adjusting the detection area to take into consideration changes happening on ground such as accumulation of snow or leaves. Some of the most advanced sensors can also be equipped with environmental resistance functions to reduce false alarms due to harsh environments like fog or snow,” states Mark Cosgrave.

Brings intelligence

Sensing technologies can make a big difference to quickly and



Camera view of area where Lidar detector Optex Redscan Pro monitors long and narrow corridor in perimeter protection. The picture below on the right shows an installation of the same detector, which is able to adapt to the environment and location where it is installed.

accurately detect an intrusion and pinpoint its location, according to Mark Cosgrave.

“With a wide array of active and passive sensing technologies available in the market, customers have a choice of solutions to adapt to their security needs and help them achieve an intelligent security system. Alerts can be set to be triggered based on certain events happening, certain areas been accessed or based on a specified target size or height,” he says and adds:

“With sensors, the detection performance is not to be affected by the distance and sensors should be able to reliably detect at any point within their field of detection and without losing perspective. Lastly sensing technologies will be able to adapt to the required detection area, whether this is a very narrow corridor or an open area.”

Advantages of sensors

One of the goals of perimeter security is to enable a system that can anticipate potential threats and take actions appropriately. An advantage of sensing technologies is they are actively looking out for any suspicious activity and have the intelligence to identify situations that require immediate attention.

“More importantly, sensors will rapidly initiate a pre-determined security response, whether it is



triggering lights, activating audio alerts, guiding security cameras or alerting security guards, contributing to an automated system,” comments Mark Cosgrave.

Efficient security

When designing a perimeter security system the first step should be identifying what are the goals, which are the key areas in the perimeter and establish what is the level of security required.

“Different security technologies serve different purposes and relying on sensing technologies for detection can bring intelligence to the security system, minimize nuisance alarms and contribute to more efficient and powerful security, he says in conclusion.

HID ranks top in biometric ID solutions

Austin, Tx (USA)

HID has ranked highest among 19 solution providers on the growth index of the Frost Radar benchmarking system for analysing biometric authentication solution suppliers.

Frost & Sullivan said **HID** and the other 18 other companies in the report, titled **Frost Radar: Biometric Authentication Solutions, 2022**, should be considered first for investment, partnerships,

or benchmarking in this market segment.

“Earning the highest score on the Frost Radar growth index is a testament to the hard work and investment that HID has

put into its biometric authentication portfolio,” comments *Steve Currie*, Senior Vice President and Managing Director of Extended Access Technologies at HID.

HID’s overall Growth Leadership ranking was based on how it builds upon its end-to-end identity portfolio and how HID offers a wealth of biometric reader hardware and software platforms using a wide range of biometric

modalities and furthers its customers’ digital identity ecosystem.

On the innovation index, HID was recognised for successfully pivoting to more digital identity solutions over the last decade, ongoing solution development for biometric credentials, and ensuring its solutions work with its legacy hardware as new capability upgrades.

Hanwha Techwin changes name to Hanwha Vision

Chertsey, Surrey (UK)

Hanwha Techwin is changing its name to **Hanwha Vision**, as the company expands its offering as a global vision solution provider.

Through this expansion, Hanwha Vision will go beyond its video surveillance products to provide next-generation vision solutions that integrate artificial intelligence (AI) and cloud

technologies to deliver insights into customers’ business operations, while driving global market innovation.

“By building on our core competitiveness through innovation, we will continue to alleviate our customers’ pain points while adding new value with advanced vision solutions,” states *Soon-*

hong Ahn, President and CEO of Hanwha Vision.

“As we expand our business from surveillance monitoring and post-event analysis, we will provide customised information through big data analytics and actionable solutions that not only prevent incidents but also respond to them in real time.

Our new vision solutions will be instrumental in advancing customers operational strategies,” CEO Ahn added.

In line with this business development, Hanwha Vision will gradually roll out the rebranding of its overseas subsidiaries, products and solutions, based on market conditions.

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.raytecled.com

Bosch wins contract for innovative building project in Poland

Warsaw, Poland

Bosch has been selected as the provider for an integrated safety and security solution in the new flagship Central Point skyscraper in downtown Warsaw, Poland – an ambitious new project built atop a metro station.

A key benefit is that the solution can easily be adapted to the different ways tenants would like to use their office space and can easily adapt to any future changes.

Central Point is a 21-storey skyscraper with 19,100 square metres of space. Because occupants come and go, the building owners wanted a solution that was scalable and flexible. Also, they wished for a solution which would adapt

interfaces, as well as other safety components in the system. Meanwhile, the fire alarm and the voice alarm system Paviro is interfaced via Smart Safety Link. Besides its use in emergencies, Paviro enables the management of all announce-

” The Bosch BIS Building Integration System software pulls all the solutions and technologies together, allowing for the building’s complete safety and security system to be centrally monitored.”

easily to the needs of individual occupants new or existing, requiring minimal changes to the safety and security infrastructure if new tenants want to change the floor layout, making sure, for example, that the announcements and voice alarms can be heard by everyone no matter how the office space is divided.

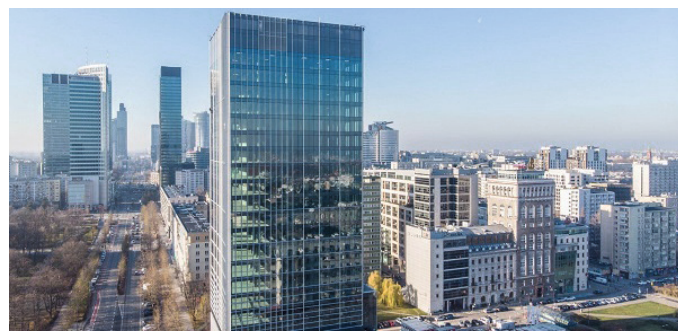
Total integration

Bosch integrated every single component of the custom safety solution. Avenar panel 8000 manage all of the building’s detectors and

ments in the building, or to play music, for example in the lobby of the building. And the Access Management System provides flexible access control for the building and elevator entrance. Video security cameras are installed around the building’s perimeter, as well as in each storey of the skyscraper and its central lobby.

Fire detection in tandem with video security

The Bosch BIS Building Integration System software pulls all the solutions and technologies



Bosch has been selected to supply a complete integrated safety and security solution at Central Point in Warsaw.

together, allowing for the building’s complete safety and security system to be centrally monitored. Thanks to the full integration of all solutions the building management is, for example, automatically notified when fire detectors need cleaning. Also, the fire detectors act in tandem with the video security cameras – with the BIS enabling to display a floor map showing precisely where the alarm was triggered and by which detector, enabling staff to switch to the video camera closest to where the event happened to manually verify the incident.

Software update over-the-air

The cost-effective set of solutions was simple to install and is easy for building management and security personnel to use. Software can be updated remotely over-the-air. This is how the completely integrated Bosch solution sets up Central Point with the flexibility and scalability to meet the needs of all existing and future occupants.

BUSINESS PEOPLE



Christian Cabirol becomes the new CTO of Mobotix.

Cabirol new CTO of Mobotix

Langmeil, Germany

Chief Technology Officer (CTO) Hartmut Sprave will leave Mobotix AG at his request after five years of service, with his contract expiring on May 31, 2023, to take on new professional challenges.

He will be succeeded by Christian Cabirol, who will be responsible for all R&D focus areas and technology partnerships as key elements of a solution-oriented strategy based on “Made in Germany” quality and the highest cyber security.

Christian Cabirol has been working for Mobotix since 2016. He currently leads the development of camera software as a fundamental part of the R&D strategy. Cabirol will take over the Executive Board position from Hartmut Sprave by June 1, 2023, at the latest.

Toshiya Eguchi, chairman of the supervisory board, welcomes Christian Cabirol as the new CTO at Mobotix.

“He has an excellent understanding of the strengths that Mobotix possesses in both hardware and software development and how he can further expand them. Christian Cabirol’s strategic vision for developing value-added solutions will help expand sales worldwide,” he comments.

Allegion completes acquisition of Plano

Dublin, Ireland

Allegion plc, a leading global security products and solutions provider, has, through one of its subsidiaries, completed its previously announced acquisition of Plano group assets, a software-as-a-service (SaaS) workforce manage-

ment solution provider.

Based in Germany, Plano has been a long-time service provider and development partner for Allegion’s leading European workforce management brand, Interflex, and its SP-Expert software platform.

Now a part of Interflex’s portfolio, Plano will continue to serve advanced workforce management customers.

Allegion originally announced its intent to purchase Plano in November 2022.

Teledyne Flir wins \$13 million contract

Elkridge, Md (USA)

Teledyne Flir Defense has been awarded a \$13.3 million contract by the U.S. Department of Defense to further expand the capabilities of its R80D Skyraider unmanned aerial system to autonomously perform chemical, biological, radiological and nuclear (CBRN) reconnaissance missions.

Teledyne Flir Defense will integrate flight control software that enables the Skyraider Unmanned Aerial System (UAS) to autonomously fly CBRN missions currently performed by soldiers hand-carrying detection sensors into hazardous areas. Blending the new technology with Skyraider's existing capabilities will allow soldiers to complete these missions without directly controlling the drone – and without exposing themselves to toxic substances.

Unmanned platforms

Teledyne Flir also will design and build prototype chemical and radiological sensor payloads for the R80D Skyraider, as well as integrate existing detectors in the U.S. Army's inventory. This effort builds on three years of investment by several joint programme offices to develop new and improved UAS capabilities for CBRN missions.

"For many good reasons, militaries are shifting their CBRN defence strategy from manned to unmanned platforms," said Dr. *David Cullin*, vice president of technology and product management at Teledyne Flir Defense.

"Employing unmanned air and ground assets to assess risks from weapons of mass destruction is an increasingly sought-after capability. We'll continue our customers' important work to enhance situational awareness for mounted and dismounted operations, enabling greater maneuverability on future CBRN-contested battlefields.



Teledyne Flir Defense Skyraider Image courtesy of Teledyne Flir.

"This project also complements our existing portfolio of CBRN sensing drone payloads – the MUVE C360, MUVE B330, and MUVE R430 – all of which allow users to remotely detect and identify a broad spectrum of potentially lethal threats," Cullin added.

The prime integrator

Both the autonomous Skyraider and the new sensor payloads will be designed to operate with the command and control user interface for the U.S. Army's Nuclear, Biological and Chemical Reconnaissance Vehicle (NBCRV) Stryker platform, for which Teledyne Flir Defense is the prime systems integrator.

Initial deliveries in the autumn

For the base contract, Teledyne Flir will deliver four Skyraidors and six of each sensor payload, with options to support training, documentation, plus the delivery of additional UAS and payloads. The award was made through the Joint Program Executive Office for Chemical, Biological, Radiological, and Nuclear Defense; Joint Product Manager for Reconnaissance and Platform Integration (JPdM RPI); and the Chemical, Biological, Radiological, and Nuclear Sensor Integration on Robotics Platforms Program Office (CSIRP).

Initial deliveries are scheduled for the autumn of 2023.



ASSA ABLOY
Opening Solutions

Unlock savings
of up to 80%
with Aperio®
wireless access
control*



Cut your costs – and do your
bit without doing a lot.

*See the full calculation and
Download our free Solution Guide:



Experience a safer
and more open world

Acre completes acquisition of Premisys

Las Vegas, Nv (USA)

Acre has completed its acquisition of the Premisys software and hardware portfolio and assets from Identicard. The company continues its strategy to drive consolidation and acquire technologies that broaden its portfolio and serve the expanding needs of its customer base.

Premisys' technologies enable organisations to self-manage door access, view integrated video and lockdown facilities. The acquisition

also extends opportunities for Acre in health-care, education, data centres, and senior living facilities.

"Since its inception, Acre's overarching goal has been to consolidate access control and customers under one umbrella," said *Darren Learmonth*, CTO, Acre

The financial details of the transaction were not disclosed.

Martin Gren, Pierre Racz and Dean Drako in discussion:

Super-entrepreneurs on future

Martin Gren, Pierre Racz and Dean Drako – the founders of Axis, Genetec and Eagle Eye Networks respectively – were all invited to Stockholm International Fairs, to speak on the opening day of the security trade show Skydd about the future trends in video surveillance. Obviously, a short summary of this opening talk is a necessity when addressing video surveillance as a theme.

By Markus Lahtinen

At the security trade show Skydd in Stockholm in late October 2022, it was a highly sought-after moment when some of the real super-entrepreneurs of the security industry shared their views on the trends that shape the industry and the future market.

It came across as being almost too good to be true with such a line-up, and to some extent that became true as well. Dean Drako, the founder of Eagle Eye Networks and the cyber security firm Barracuda Networks, couldn't join the panel last minute. Instead, Dean participated via video where he pointed out AI the most important video surveillance mega-trend.

Drako praised AI

According to Dean Drako the most important technology trend in the industry is the opportunities associated with the increased use of Artificial Intelligence (AI). While AI may offer value in several sectors, Dean made it clear that security applications lie at the heart of the development of AI.

– There will be opportunities using AI in assisting camera operators, where AI currently can detect a person attempting to climb a fence, detect a person running. Furthermore, Dean Drako also mentioned the possibility of using AI to assist in classifying and identifying objects using AI-powered video surveillance.

– This will play an important role in supporting the camera operators, not having the time or attention to monitor all events happening in real-time.

Dean Drako's conclusion was crystal clear.

– AI will have a big impact on our industry, he stated clearly.

AI should be renamed IA

Pierre Racz commented on Dean's view on AI and brought to mind some important limitations to the often-endless possibilities attributed to AI. Instead, he believes there is an over-reliance on the possibilities of AI. A bit jokingly he sometimes refers to AI as Absolute Ignorance instead. On stage he explained that we should rather focus our attention to Intelligent Automation rather than AI.

– Humans will continue to be key in the future. The benefit of AI primarily lies in its ability to capture routines and reoccurring patterns, but a criminal will unlikely follow a routine pattern, he said and suggested that AI can be a vulnerability in itself, since it will not detect this type of deviant behaviour.

– IA stands for Intelligent Automation, and it is a more promising and human-centred direction for the future, according to Pierre Racz.

Make room for increased technology use

Martin Gren was also skeptical to Dean's view on AI, but not as categorical as Pierre Racz. He acknowledges AI as a trend, but believes it won't have such a revolutionary effect as put forward by Dean Drako. Instead, he pointed to another trend, more related to the general direction of where

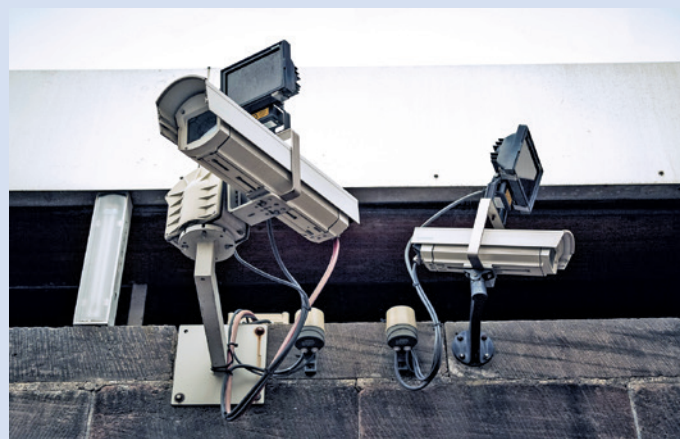


Photo: Pixabay

One trend is the development towards technology that aims to protect people's personal privacy while video surveillance can be conducted effectively.

society is going. A trend that will impact the security industry in general and video surveillance in particular.

– Demand for security and safety is rising – much driven by the debate on public safety in Sweden – in particular the rise of organised crime and gang-related crimes in recent years.

– It's important not to limit the response to the number of police officers and security guards. The key is to empower guards and police with technology.

Martin Gren also highlighted that 80% of the security costs in the private sector is spent on manned guarding.

– They should use cameras instead. Cameras that direct security staff to a location where something is happening, said Martin Gren

Privacy protection

An additional trend raised by Pierre Racz is the development of technologies that combine the need for privacy while at the same operating an effective use of video surveillance. He mentioned that at Genetec they are looking into a solution where the video management system (VMS) takes two video streams as input – one programmed to be somewhat blurred and another encrypted hires stream that may be unlocked upon decision from law-enforce-

ment agencies.

– The privacy aspect is important – and I embrace privacy laws that protect citizen's right to privacy, and as a force for designing privacy-centred technologies, he stated.

Cyber security – the big trend

With regards to mega-trends Martin Gren and Pierre Racz agreed on much of what was being mentioned. But most of all they were in full agreement on the importance of cyber security for the future. This development is not unique to the video surveillance market but also society more broadly. Pierre Racz stated that this is a severe challenge at many levels.

– Business leaders have no knowledge on how to deal with cyber threats. In case a business is attacked it is not unusual to hear business leaders blaming the IT department for the intrusion. This needs to be dealt with forcefully.

– I would go as far as to propose that these cyber incompetent leaders should go to jail. They need to be held accountable.

Suing the manufacturer

Pierre Racz also commented on what is the responsibility of the customer with regards to security sourcing. He pointed to the

trends in video surveillance



Pierre Racz and Martin Gren on stage together with moderator Lennart Alexandrie at the opening day of the security fair Skydd.



Dean Drake sent a video greeting (from which the image is taken) where he pointed out AI as the most important video surveillance mega-trend.

importance of considering the geopolitical dimension, and avoid sourcing from countries with autocratic rule, for example relying on manufactures with strong ties to the government.

– When choosing security equipment – that will be put on the internet – it is important to ask yourself: can I as a customer sue a manufacturer of cameras for faulty engineering or for not disclosing secret backdoors to access the equipment? Pierre mentioned that we've seen examples of hidden backdoors, clearly implying Chinese manufactures.

Martin Gren, on the other hand, reiterated the wide scope and constant challenge of cyber-threats.

– Cyber security needs to be treated as a constant ongoing process and not as a checklist, he stated.

On-prem still in demand – despite the rise of the cloud

Cloud services were also addressed during the panel session. The rise of cloud services was clearly acknowledged as a significant development in past years.

– Much is about timing. Martin mentioned that Axis pioneered some of the earliest cloud offerings, but on-prem solutions still has a future.

– It all depends on the needs of the customers. A national

retail chain has similar requirements at each store, then the obvious choice is a cloud solution. But for other types of customers, enterprise-type, there is still a need to control both hardware and software, Martin argued.

Martin Gren also mentioned the European Union-wide Data Privacy Act that requires awareness as to where the data is physically stored.

– This is made easier with on-prem solutions and is made more difficult when it is put in an unknown location in the cloud.

The needs of the customers as guiding principle

Pierre Racz pointed to the cloud as being merely a distribution format. And just like Martin, Pierre stressed the importance of understanding the needs of the customers.

– For some customers the most important thing might be being able to watch video in real-time, while for other customers video recordings must never be lost under any circumstance. This provides room for various solutions and distribution formats depending on the type of customers, Pierre stated.

Volume and niche as business strategies

The video surveillance market is

getting increasingly consolidated; consequently volume, capital and skills are increasingly important for manufacturers. Martin Gren put it in more blunt terms.

– If you wish to be in this industry you need to be number one or number two, or be a niche player.

Martin Gren further elaborated on this point.

– At Axis we are now at the 8th generation of camera chips. We spend \$50 million dollars to develop the next generation of chips. Few companies possess the skills and have sufficient capital to make such investments.

Martin Gren also sees growth potential for “beyond security” applications for Axis as well as for the security industry.

– Our cameras can be used for a range of other things than security only. There are future business opportunities to develop smaller as well as broader software applications for use cases beyond security, Martin argued.

The role of the distributor

For many years the pure-play security distributor has lost sales volumes. Martin Gren and Pierre Racz were asked the question if they are about to go out of business.

– They will continue to exist argued Martin. You can't simply

say that they will go away due to technology developments. They are still a part of it; they keep an inventory of cameras, cabling, other hardware, and software. There is also a role to be played by the installer in the future, of course someone needs to make the installation – but also offer a point of contact to the customer, Martin stated.

Pierre Racz agreed.

– The distributor is not going away. Twenty years ago, it was suggested that the brick-and-mortar stores would go away. They still haven't. The same applies to distributors – I am thinking about the management of logistics, payments but also dealing with taxation. In the US each state sets their individual sales tax which is hard for a big manufacturer to manage. And it is even worse for smaller companies. Here the distributor has a role to play.

Component shortages – the light in the tunnel

The final topic of the panel concerned the shortage of components and supply-chain issues.

– It's been a challenge, but we are starting to see the light in the tunnel. But – I do think we will continue to experience supply-chain disruptions in the future as well, Martin concluded.

HID acquires Guard RFID acquisition

Austin, Tx (USA) and Vancouver, Canada

HID has acquired Guard RFID, a leading provider of real-time location services (RTLS) hardware and software solutions in the healthcare space.

The addition of Guard RFID expands HID's offering and relevance in the active RFID and RTLS space, including the support for new use cases catered to the needs of healthcare facilities.

"Bringing Guard RFID and its innovative RTLS technology into the HID family allows us to enhance our healthcare presence to better protect patients and staff," said *Björn Lidefelt*, EVP and Head of HID. "As incidents

in healthcare facilities continue to rise, these solutions will help providers do what they do best – making their patients feel better, faster."

"Incorporating Guard RFID into HID's Identification Technologies grows and reasserts our expansion as a major player in the healthcare industry," states *Marc Biemann*, SVP and Head of Identification Technologies, HID. "This acquisition, along with our

growing portfolio of RTLS and active RFID solutions, provides new and existing healthcare clients with even more options to protect their patients and staff."

Founded in 2007 and headquartered in Vancouver, Canada, Guard RFID is now part of HID's Identification Technologies Business Area led by Marc Biemann. The Guard RFID offering will merge into HID's Internet of Things (IoT) Business Unit and benefit from HID's sales and other global functions to support its offering.



"Bringing Guard RFID and its innovative RTLS technology into the HID family allows us to enhance our healthcare presence to better protect patients and staff," says Björn Lidefelt, EVP and Head of HID.

Battery Ventures sells Qognify to Hexagon

Pearl River, NY (USA) and Stockholm, Sweden

Qognify, a leading provider of Physical Security and Enterprise Incident Management software solutions, is being acquired by Hexagon AB.

With its headquarters in Stockholm, Sweden, **Hexagon** is a global leader in digital reality solutions combining sensor, software, and autonomous technologies. Hexagon acquires Qognify from Battery Ventures, a global, technology-focused investment firm.

Qognify was formed in 2015 when Battery Ventures acquired the physical security division of Nice Systems, thus creating a new brand in the market. In 2018, Qognify acquired On-Net Surveillance Systems Inc. with its brands ONSSI and Seetec, forming a leading global player in the physical security market. Qognify's

video management (VMS) and incident management (EIM) solutions are used by companies and organisations around the world to mitigate risk and reduce the impact of incidents related to security, safety and operations.

Steve Shine, President and CEO at Qognify, highlights the opportunity the acquisition creates for Qognify: "Joining Hexagon gives Qognify the ability to expand its footprint in the area of true enterprise-class physical security solutions – especially in key verticals such as public safety, infrastructure and transportation. Qognify will be able to leverage Hexagon's geo-

graphic reach to address additional markets. The acquisition creates a solid basis for continuous growth and development, from which also existing customers and partners will benefit."

"Hexagon has long been a leader in public safety solutions that deliver situational awareness and insights to emergency services and others – improving operations, minimising risk and saving lives," says Hexagon President and CEO *Ola Rollén*. "Qognify's solutions are a natural expansion of our public safety portfolio, adding comprehensive and tightly integrated video capabilities that can provide dispatchers, responders and investigators with new levels of intelligence to serve and protect their communities."

"The acquisition also opens up new opportunities for us in real-time monitoring and security – extending our reach into new markets and enabling the cross-sell of complementary Hexagon offerings to Qognify's customers, like our award-winning Leica BLK Series of reality capture sensors," continued Rollén. "Additionally, integrating video monitoring capabilities into our enterprise asset management solution will enable customers across diverse industries to further optimise the performance and reliability of their assets."

Qognify will operate as part of Hexagon's Safety, Infrastructure & Geospatial division. Completion of the transaction (closing) is subject to customary regulatory approvals.

Securitas strategy successfully gains new funding

Stockholm, Sweden

Securitas has this week concluded a successful *Schuldschein* loan transaction, raising MEUR 300 equivalent in the international *Schuldschein* market.

By entering into the *Schuld-*

schein market for the first time Securitas establishes a new source of long-term funding for the Group.

The issue was oversubscribed by more than triple the launch

amount. The majority of the funding is for five years and consists of Euro and US dollar tranches. The proceeds will be used to refinance part of the remaining MUSD 1,146 bridge

facility related to the acquisition of Stanley Security which was closed on July 22, 2022.

The joint arrangers were Commerzbank, ING, SEB and Unicredit.

Business & Product News – Every Day!

www.securityworldmarket.com

**ALLTID
SÄKER
ALDRIG
UTRÄKNAD**

ARCHITECT[®]



**Välj en läsare för ditt
passerkontrollsystem
som säkrar dig över tid.**

Architect[®] Vandalsäkra och handikappanpassade högsäkerhetsläsare för kort och mobil passar alla passersystem.

Architect[®] läsarna kan utökas med Biometri, QR kod och även modul för 125Khz prox så du kan leva med dem över lång tid och alla systemval idag och imorgon.

Alltid högsta säkerhet och högsta bekvämlighet, med öppen arkitektur och livstids garanti gör dom till världens mest dekorerade läsarfamilj.

SMARTER SECURITY ANSWERS



Founding member of



www.stid-security.com



Cyber security – a growth factor for the access control market

The global market for access control in 2021 had sales of about \$8.5 billion and is expected to grow by about 8 percent annually until 2027, according to a report by market research firm Imarc Group. A significant growth factor is the demands for increased security in general and cyber security in particular.

Imarc Group emphasises that more and more people are working remotely since Covid hit the world and that this has presented companies with new challenges at a time when cyber attacks are increasing sharply. Preventing data breaches and ensuring business continuity has become an increasingly high priority in organisations worldwide.

Video surveillance manufacturers were first

Of the electronic physical security sectors, video surveillance manufacturers were the first to push for increased cyber security. This after some large high-profile cyber attacks occurred in the 2010s, where the network intrusion began with the hacking of connected video surveillance equipment and came to cause serious damage. Attention to cyber attacks intensified when the US government, citing national security, banned a number of Chinese companies from government and infrastructure-sensitive installations, including well-known video surveillance equipment manufacturers Hikvision and Dahua, but also Huawei.

Focus on cyber threats after excommunication

The ban is filed under the John McCain National Defense Authorization Act (NDAA) and restricts the use, procurement or sale of certain brands of surveillance equipment to or for federal agencies. Government agencies are not only prohibited from purchasing equipment from these manufacturers, but also from doing business with contractors who use surveillance technology

from the blacklisted companies. The law also stipulates that all essential components of a video surveillance system manufactured by these manufacturers are also prohibited.

Cyber security – a means of competition

The blacklisting prompted many US and European video surveillance manufacturers to become NDAA compliant. In addition, the video surveillance companies have worked increasingly to increase security, not least via far-reaching collaborations with IT security companies that can contribute to product development that addresses the need for cyber security. Having certification according to existing cyber security standards has become customary. Cyber security has simply become a means of competition in the video surveillance market.

The industry has woken up

In the area of access control, the issue of cyber security has not been highlighted in the same way. This may have its explanation in the fact that the access control area was significantly later when it comes to connected systems. But now things are starting to happen, not least within the EU, where member states are required to implement measures to live up to the NIS2 directive's requirements for cyber security of communication in technical systems, for example for ID management or access control.

Suppliers drive development

The industry's suppliers are starting to drive cyber security issues



Of the electronic physical security sectors, video surveillance manufacturers were the first to push for increased cyber security.

more and more. The French manufacturer of readers, Stid Security, is one of the actors who, in debate articles and in panel discussions, is pushing for the industry to accelerate the development towards more secure technology solutions for access control and to live up to the NIS requirements. Genetec, the world's fastest growing provider of access control software, has also been a major driver for the access control industry to take the cyber threat seriously. Recently, the Canadian company went out and warned about cyber-attacks that can be initiated via, for example, old and poorly protected access control systems.

"Many organisations work with access systems that go back ten years or more. While these legacy systems still work to allow employees to log in and out, it is likely that these systems use technologies that are extremely vulnerable to modern cyber threats," said Christian Morin, Vice President of Product Engineering and Chief Security Officer at Genetec Inc.

"Older systems were not built to handle today's threats. When evaluating a new access system or upgrading an existing system, make sure that cyber security is a key component of the selection criteria for suppliers, he further suggests.

Multi-factor authentication

Another security trend, related

to the access control market, is that more and more small and medium-sized companies are starting to use multi-factor authentication, which for example is based on biometrics, key fob, password and personal identification number (PIN) to verify an individual's identity. With these combined solutions, access can limit access to buildings for staff on site and visitors, increasing physical security.

Other growth factors

Imarc Group also highlights some niche businesses that may have special access protection purposes, such as healthcare companies that use physical and electronic access control systems to prevent unauthorised disclosure of protected health information (PHI) and ensure the integrity of patient data.

The increasing threat of terrorism and geopolitical unrest are also growth driving factors for the market. In more and more countries, access protection is being strengthened at military locations and national borders. This in turn drives the demand for role-based access control to monitor applicant entry into restricted areas to maintain a secure location.

Finally, Imarc Group sees generally the increasing need for security and control for industry, schools, commercial buildings and even in private homes as major growth factors.



Unlock savings of up to 80% with Aperio[®] wireless access control*

ASSA ABLOY
Opening Solutions

Cut your costs – and do your bit without doing a lot.

*See the full calculation and
Download our free Solution Guide:



Experience a safer
and more open world

Genetec warns of rising cyber risks on legacy access control systems

With the ever-increasing rise in cyber crime, Genetec Inc. is cautioning organisations of all sizes to be vigilant about the cyber security risk posed by legacy access control systems. To improve the awareness of cyber security of access control systems, Genetec share their recommendations, divided into nine steps.

According to the latest report from research organisation Omdia, Genetec is recognised as the fastest-growing access control software provider in the world and ranked as number two among the world's biggest access control software providers.

Older systems – a risk factor

Christian Morin, Vice President of Product Engineering and Chief Security Officer at Genetec, is concerned about the fact that there are many organisations operating with access control systems that date back ten years or more.

“While these older systems still allow employees to badge in and out, there's a very high likelihood that these systems employ technologies that are extremely vulnerable to modern cyber threats,” he says.

Criminal's entry into the network

Vulnerabilities in legacy access control systems can introduce cyber security weaknesses that may put an entire organisation at risk. Cyber criminals can exploit weaknesses in access control system credentials, controllers, servers, readers, or workstations connected to the network. Once a cyber criminal has breached access control system credentials, they can then move on to an organisation's network and can gain control of other building systems, view or steal confidential information from internal records, or launch attacks designed to take key systems offline.

Average data breach cost – 4,3 million dollars

Companies that are affected pay a heavy price; the average cost of a data breach rose from 4.24 million dollars in 2021 to 4.35 million dollars in 2022. Hence, it's never been more important for organisations to be educated on the risks associated with legacy systems and the advantages that new cyber secure access solutions can offer.

Cyber security best practices for access control systems

To improve the cyber security of access control systems, Genetec recommends the following steps:

- **Upgrade the system.** Older systems were not built to address today's threats. When evaluating a new access control system or upgrading an existing system, make sure that cyber security is a key component of the vendor selection criteria.
- **Use advanced secure credentials** and the latest communications protocols to secure data transmission since older credentials are easy to clone using readily available tools.
- **Educate employees and partners** about cyber security best practices and ensure they are prompted to change passwords often.
- **Regularly check for firmware** and software updates and install once available.
- **Use a centralised identity access management system** to ensure virtual and physical au-



Photo: Pixabay

Customers are gradually freeing themselves from proprietary solutions and demanding more flexible, open solutions.

thentication and authorisation of employees for better control and more effective maintenance of your systems.

- **Create a dedicated network** for access control systems so that there is clear segregation of networks based on their purpose.

- **Choose a security provider** who can demonstrate compliance with established security certifications.

- **Ensure that the access control system** uses proven data encryption standards as well as multi-factor authentication.

- **Work with a partner** that has strong supply chain risk management, a dedicated team to monitor cyber threats, and ensures software is updated frequently and patched as needed.

A sector in transformation

Access control technology has undergone a huge transformation in recent years. Customers are gradually freeing themselves from proprietary solutions and demanding more flexible, open solutions. Forward-thinking technology manufacturers have now introduced a new breed of more cyber secure solutions that offer benefits beyond locking and



Christian Morin, Vice President of Product Engineering and Chief Security Officer at Genetec.

unlocking doors.

“A unified access control system that uses the latest cyber security standards to secure communication, servers, and data such as Genetec Security Center Synergis is able to not only protect an organisation's assets and people but help them improve their business operations and decision-making,” states Christian Morin.

“By choosing an open architecture IP-based access control system, organisations have the flexibility to upgrade to the latest supported technology at any time, move at their own pace, and work within their available budget,” he says in conclusion.

Further information on this subject is available for download online from Genetec.

Joachim Mahlstedt, Assa Abloy Opening Solutions

Cloud-based access control

– the key to effective facilities management from anywhere

Efficiency and convenience are important drivers across almost every area of economic activity. They certainly continue to drive global demand for cloud infrastructure — growing at an estimated 33% year-on-year, according to a report by IT analyst house Canals.

In this article Joachim Mahlstedt, at Assa Abloy Opening Solutions, gives his views on cloud-based access control and Incedo Cloud in particular.

“Access control is no different. Perhaps a third of security end-users have already adopted cloud-based software for access management,” states Joachim Mahlstedt, Product Marketing Director EMEA, referring to the “Wireless Access Control 2021” report by Ifsec Global.

“Managers want the power to manage from anywhere, at any time. This can be especially important in security, where unexpected issues are usually urgent — or time-sensitive, at the very least.”

No matter of the organisation's size, the manage-from-anywhere ethos powers an increasingly hybrid work landscape and is a major benefit of the cloud, according to Thomas Schulz.

“From wherever they are, a facilities manager remains in control of their premises,” he says.

Security, agility and efficiency

As well as complete control from the cloud, a modern access control solution should offer a wide range of digital locks and credentials, allowing a business to manage workspaces and workflows with maximum efficiency. Assa Abloy's Incedo access control platform was designed for this purpose, according to Joachim Mahlstedt.

“When Incedo is chosen, organisations secure almost any opening with autonomous electronic locks or in real time with online devices. They issue building users with credentials of their choice. And they manage everything from one place, via scalable, intuitive Incedo software,” he comments.

Easy to get started

As one major advantage Joachim Mahlstedt emphasises how easy it is to get started with Incedo.

“Businesses choose from a vast range of hardware. Doors, cabinets, gates, server racks and almost any other opening may be locked — with a wireless or wired device.”

User friendliness and convenience are further advantages, according to Joachim Mahlstedt.

“Building users gain access via smartcards, mobile keys stored on their smartphone, or battery-free smart keys. Incedo software manages doors and users securely — in the cloud, if required.”

Moreover, hardware and software installation are easy, with no complex integrations required.

“The entire ecosystem is modular, designed for simple adoption and easy expansion at any time and in any direction,” states Joachim Mahlstedt and concludes his view on Incedo.

“Incedo leaves business owners with more time to focus on their main task: the business”.

The easy way to take control

Different areas of a building often have different security requirements. Where entrance doors or critical areas need real-time monitoring including alerts, some other areas might have lower demands for physical security.

“Here, autonomous hardware can be installed faster and more cost-efficiently, with no need for network cables or wireless hubs,” comments Joachim Mahlstedt, and



Perhaps a third of security end-users have already adopted cloud-based software for access management,” states Joachim Mahlstedt.

explains further.

“Any Incedo system can include both wired and wireless locks, all natively integrated and covering almost any application. A vast choice of door and other hardware, to secure any type of opening, is available from a single manufacturer. Incedo controls everything.”

Whatever hardware is in place, building users can carry almost any credential. All common RFID technologies are supported, including Iclass and Mifare.

“Users can also unlock with an Incedo Mobile Key stored on a smartphone. A shared Seos backbone ensures all credential types may be deployed together in the same system, which makes gradual site upgrading easier,” says Joachim Mahlstedt.

All managed in the cloud

Incedo Cloud has the option to combine online and offline management. For example, controlling access to secure areas including entrances, labs, server rooms in real time, with online management.

“Adding autonomous offline devices alongside these enables the business to control access to areas that previously have been uneconomical to protect due to location, environment, or cost. It gives security managers even more choice and control,” adds Joachim Mahlstedt.

Because Incedo is built for flexibility, switching between online and offline management is always seamless, for both end-users and administrators. The only difference is how credentials are managed: online or via updaters.

Bike rental – an example

An example of the benefits of Incedo Cloud remote management is found at Kolovna Bike Rental in the Czech Republic.

Kolovna has placed secure bicycle containers at popular cycling locations all over the country. Access to each container is filtered by electronic locks, so customers can safely park their own bike or rent one from the container.

The containers combine security with easy customer access, including unlocking via mobile keys on a smartphone. Kolovna needed an access control platform which could multitask without additional technologies, software, or staff. Now, with readers, a controller, and a door module in every container, Incedo connects all Kolovna's security software and hardware within one seamless system.

“Cloud management keeps Kolovna staff in control of their premises from anywhere. They can work in an office — at home or on the road,” concludes Joachim Mahlstedt.

Robert Jansson, Stid Security:

“Secured access control of transport vehicles is not enough”

The word transport security leads the thought to how goods transport vehicles should be protected against theft. But how are “fake” carriers barred from entering an area to steal goods? And how is it done safely and smoothly?

Is an ID tag on the vehicle or number plate recognition the solution?

“It is not enough to check the vehicle, you also have to ensure that the driver is authorised,” says Robert Jansson, sales director at Stid Security.

In reality, a vehicle from a trusted transportation provider, whose ID tag verifies eligibility, is often enough to grant drivers access to a guarded area. In recent years, automatic number plate recognition (ANPR) has been increasingly used to check eligibility.

“Number plate registration is a smooth and fast way to handle access control on incoming vehicles, but it is not recommended as a security solution. License plates can easily be stolen or falsified,” says Robert Jansson, who is concerned about the often-insufficient control of people who come with vehicles.

“Unfortunately, control of both entry and exit of vehicles is often more characterised by the need for convenience than the demand for security. Convenient solutions are usually based on one-factor authentication, which is far from satisfactory,” he comments further.

Security comes second

Robert Jansson is sales director for the card technology manufacturer Stid Security in the Nordics, Eastern Europe and South Africa and has 35 years of industry experience. He is concerned that security often comes second, which opens the door for criminals. For example, at the gates of the perimeter protection for entry and exit, there are sometimes staff or there is a remote operator who checks the vehicle's authorisation and decides on access.

“Or there is only one card reader that checks the authorisation,” notes Robert Jansson.

“You want to get away from staffing. The question then is what is checked and how it is checked, that is crucial for the quality of the security you get. If you only check the vehicle's authorisation, it is more of a convenience solution than a security solution”, he says.

One-factor authentication

Robert Jansson is concerned about the naivety that prevails when it comes to, for example, checking transport vehicles, not least in Sweden, where Robert has his base. He claims that it is usually just an ID tag on the vehicle that is detected by a reader to determine whether access should be granted. The driver is often exempt from control or both the vehicle and the human behind the wheel have a UHF tag, meaning both use one-factor authentication.

“In the best case, the driver is forced to leave the vehicle to go to a reader, swipe his card and enter his PIN, which is then two-factor authentication. However, this means that the very purpose of long-distance reading has been abandoned, namely that transport should be smooth and with a lot of incoming and outgoing traffic, unwanted queues can be created,” states Robert Jansson.

“Since fast passage had a higher priority than security, the authorisation check was focused on the vehicle, which made theft possible.”

Two-factor authentication

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



Specter Nano checks the authorisation of both the vehicle and the driver simultaneously before access is granted.

Robert Jansson, Stid Security.

“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. In this way, the person's authorisation can be ensured before the gate is opened,” says Robert Jansson.

The two-factor authentication works so that the driver's mobile phone is detected, but only when the mobile phone is unlocked with a PIN code or a biometric template – with an addition of also having the particular credential card unlocked with a PIN code or biometric template – that becomes the virtual card's signature sent to the reader. Thus, no unauthorised person can use the ID carrier and gain passage into the area.

Simultaneous reading of vehicles and drivers

In 2021, Stid Security launched the multi-technology reader Specter Nano, which can remotely detect and read the authorisation of vehicles and people quickly, flexibly, safely and simultaneously. The reader can handle multiple vehicles and people at the same time and not only reads the mobile virtual card for two-factor authentication of people, but also all kinds of windshield tags, cards and key fobs.

“The reading distances can be adjusted both with Bluetooth and

UHF, and the fast reading means that the driver hardly needs to slow down, which contributes to ease of use without reducing security” explains Robert Jansson.

The working principle is simple. 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 risk of criminals entering an area via a stolen authorised vehicle is eliminated with this solution.”

“Two-factor rule”

The response to the launch of the Specter Nano has been very positive. However, being able to apply the “two-factor rule” via a single reader, where access is only granted if both the vehicle and the driver are authorised, is particularly appreciated in Norway, where there is a law on two-factor authentication if a transaction is to be logged in a pass system. If you bring one-factor authentication to a person, only the vehicle can be logged, not the person.

“Specter Nano is the first solution where, via a single reader, you can legally have a transaction of drivers and vehicles in a pass system. Interest in the solution is very high there,” he comments in conclusion.

Innovative technology combination brings “Axis powered by Genetec”

Montreal, Canada / Lund, Sweden

A new collaboration between Genetec and Axis Communications will see the introduction of Axis Powered by Genetec, the industry's first enterprise-level access control offering that combines Genetec access control software with Axis network door controllers in a single easy-to-deploy all-in-one offering.

Axis Powered by Genetec combines the Genetec Synergis access control software with the Axis A1210 and Axis A1610 network door controllers.

Long history of collaboration

Integrators are set to benefit from easy-to-deploy hardware pre-loaded with Genetec's innovative access control software, removing friction associated with traditional software/hardware integrations. Moreover, devices in the Axis Powered by Genetec programme benefit from continuous delivery of product and firmware improvements, new features, and important cyber security updates – all from two of the industry's leading innovators.

“Axis and Genetec share a trusted partnership based on a long history of collaboration and development ingenuity,” states Michel Chalouhi, Vice President of Global Sales at Genetec Inc.

“Our shared focus on delivering powerful and creative solutions to meet customer needs has underpinned the development of this sophisticated enterprise-level access control technology delivered in a streamlined, easy-to-acquire-and-deploy offering.”

” Harnessing the power of computing at the edge will become essential in modern system architecture.”

“Boosting cyber security”

Fredrik Nilsson, VP, Americas Axis Communications, “Axis and Genetec have a history of collaborative innovation. The new Axis Powered by Genetec solution exemplifies this relationship by truly integrating best-of-breed hardware and software thereby enhancing installation and maintenance while also boosting cyber security,” he says.

“Our longstanding and trusted partnership with Genetec means integrators and end users can rely on this solution to deliver continual innovation, quality, and value



New Genetec and Axis technology combination aims to transform physical access control.

for a wide range of physical access control needs.”

Hardware and software in one unit

Axis Powered by Genetec combines hardware and software in one unit which simplifies the installation process, reduces maintenance, and brings built-in cyber security features at both the hardware and software levels. The open platform solution expands the Genetec ecosystem of non-proprietary systems while providing customers with more flexibility to scale as their physical security needs evolve.

“Harnessing the power of computing at the edge will become essential in modern system architecture,” comments Christian Morin, Vice President of Research and Development at Genetec Inc. boosting cyber security

More edge initiative to come

Christian Morin stresses further that as “we reach the limits of Moore's Law, initiatives that distribute processing into containerised, hybrid edge/core structures will act to increase available computing power for complex applications.”

“Initiatives such as Axis Powered by Genetec are at the forefront of such innovation and mark the beginning of other edge initiatives at Genetec,” he says.

Genetec will be introducing select Powered by Genetec offerings across a range of edge devices in the coming quarters. According to the company, Genetec Certified channel partners will have access to part numbers and ready-to-ship inventory in April.



ASSA ABLOY
Opening Solutions

Unlock savings
of up to 80%
with Aperio®
wireless access
control*



Cut your costs – and do your
bit without doing a lot.

*See the full calculation and
Download our free Solution Guide:



Experience a safer
and more open world

Alcatraz AI

The Rock and facial authentication

– a game changer for intelligent access control

With the Rock, Alcatraz AI may well have introduced a game-changer to the access control market. This facial authentication solution is not just offering an intelligent tailgating detection, and a simplified enrollment process that works natively with existing access control systems – it is also designed to protect individual privacy.

Now Alcatraz AI invests in a global expansion, and as the Rock is designed in compliance with the GDPR and other privacy frameworks, the expectations are high.

The use of biometrics in access control systems is becoming increasingly common, especially fingerprint reading. Convenient facial recognition for access control is also in demand, but often difficult to adapt to meet different countries' privacy protection laws. However, Alcatraz AI has succeeded with their facial authentication solution. Their solution the Rock, is not just an unique approach to use the face as a credential, it is also designed in compliance with the latest privacy frameworks including General Data Protection Regulation (GDPR), the Illinois Biometric Information Protection Act (BIPA) and the California Consumer Privacy Act (CCPA).

A rainy day was a trigger

The company was founded in 2016 by Vince Gaydarzhiev, now the chief technology head of the company. He was part of the team that developed Apple FaceID.

The embryo to Alcatraz AI came as during a rainy and stormy day he and his fellow team members were getting drenched while slowly accessing the facility, according to Tad Druart, Vice President, Marketing at Alcatraz AI.

"They fumbled with badges and umbrellas, or misplaced their badge and were trying to talk to security at the entrance. He

thought, if I just put my phone on the door I could authenticate people more quickly and securely", states Tad Druart who also points out that Alcatraz AI is not using Apple technology, neither is Apple affiliated with Alcatraz AI.

So, then the ending of the short story about the birth of Alcatraz AI.

"Vince Gaydarzhiev started meeting with some of the world's largest corporations to ensure he understood their enterprise needs and the Rock was born," states Tad Druart.

Several awards

Quickly Alcatraz AI became a well-known name for its innovative approach to intelligent access control, based on face authentication. In 2019 the company received the awards "Startup of the Year" and the "Most Innovative Startup" by the Security Industry Association (SIA). The company was also named "Cool Vendor in IoT Security" in Gartner's 2019 report for its innovative approach to access control using facial recognition. In 2020 Alcatraz AI was also included in the "Top 50 Most Innovative Companies" by Built In San Francisco.

That the Security, Sales & Integration magazine named the Alcatraz Rock as one of the "30 Top Technology Innovations" of



Alcatraz AI uses AI and machine learning to deliver facial authentication solutions that work natively with existing access control systems eliminating the need to rip and replace infrastructure.

2020 and that Innovation & Tech Today in 2022 awarded the Rock a "Most Innovative Product" in 2022, speaks highly for the technology and problems it solves.

Facial authentication – a new approach

Alcatraz AI uses AI and machine learning to deliver facial authentication solutions that work natively with existing access control systems eliminating the need to rip and replace infrastructure.

But how does Alcatraz AI's facial authentication differ from the more common facial recognition systems on the market?

"Facial recognition software applies algorithmic pattern matching software to identify an individual's face in a digital image or video. Organisations can use it for a variety of purposes, such as verifying a person's identity for security purposes or tracking individuals as they move through a public space," states Tina D'Agostin, CEO of Alcatraz AI.

"By contrast, facial authentication uses the unique characteristics of an individual's face to verify their identity to authenticate the person at access points or for certain transactions. This gets done by using an algorithm to compare

a live image of the user's face to reference data to confirm that they are who they are supposed to be and that they are authorised to access a designated space, device or information, such as their iPhone."

The approach to privacy that facial authentication offers is something Tina D'Agostin likes to emphasise.

"Unlike facial recognition, which often takes place without either the knowledge or permission of an individual, facial authentication requires the user's consent," she says and adds.

"We take this a step further with our newest feature, Privacy Consent Management. Now, in addition to the technology being opt-in and private, customers can share their privacy processes, policies, and data retention practices with users ahead of enrollment and allow them to provide legal opt-in consent."

Cyber security and secured privacy

For Alcatraz AI privacy and cyber security are of high priority. The facial templates cannot be reconstituted to identify a person, yet they are still AES 256 encrypted at the Edge and are TLS 1.2 encrypted during transmission to the Cloud

or TLS 1.3 encrypted for on premise database. And as mentioned, the entire process includes voluntary opt-in, privacy protections and simplifies use for more rapid end user (consumer) adoption.

“We also have features such as the ability to delete data in compliance with regulations or more strict terms should the customer desire that. Eliminating privacy concerns and adopting a privacy first design and delivery posture has enabled more rapid growth,” states Tina D’Agostin, knowing that the Alcatraz AI’s vision of simplicity, security and privacy concerns have already had a powerful impact on the market, as the Rock, is deployed at some of the most successful enterprises in the world, including supporting access for more than one million employees at Fortune 500 companies

\$25 Million investment in global expansion

Since its founding in 2016, Alcatraz AI set out to transform the experience of entering spaces in the most highly secure manner, while enabling a completely passive and frictionless use case at doors for occupants and the security teams that manage them.

Since 2020, the company has seen rapid growth in the US and globally, with Alcatraz solutions being deployed in more than a dozen countries.

Now a new expansion phase will begin as Alcatraz AI has raised a \$25 million Series A round allowing the company to open operations in Europe (Nordics) and Middle East.

The round was led by Almaz Capital and included EBRD (The European Bank for Reconstruction and Development), Endeavor Catalyst, Silverline Capital, and Golden Seeds, along with participation from existing investors JCI Ventures (the corporate venture arm of Johnson Controls), Ray Stata and LDV Partners.

“At Alcatraz AI, we believe that safety and security is the first principle, and we are committed to leading a new era of frictionless access control by leveraging the

unique power of the human face to make accessing spaces as secure, quick and easy as unlocking your phone,” comments Tina D’Agostin.

“We are excited to enter the next phase of our company’s growth by partnering with our investors with a strong track record scaling companies globally that deliver next generation technology.”

The timing is right

Tina D’Agostin is convinced that the global physical access control market – valued to approximately \$70 billion – needs the next generation solutions that enable more modern and secure ways of unlocking where people work, live, study and play.

“Today, the most used credential to enter secured spaces is an access card that can be lost, replicated, or stolen. Alternative technologies, such as mobile and legacy biometric systems have not gained mainstream

momentum due to implementation and user challenges. The Rock solves the most difficult access control challenges to creating and maintaining safe spaces.

Differentiated customer base

Today Alcatraz AI’s customer base is found in many different verticals, such as:

- Corporate campuses/headquarters.
- Data centres.
- Financial institutions.
- Higher Education.
- Telecom.
- Critical infrastructure (Oil, gas, energy, chemical).
- Stadiums and arenas.
- Aviation facilities/airports (back-end infrastructure access).
- Healthcare.

“Our customers are looking for a solution that increases through-



Tina D’Agostin, CEO of Alcatraz AI.

put and increases security. In the past, facial recognition has been limited or perceived to be most useful in more secure, multi factor environments, but the Rock changes that making it frictionless and more secure,” comments Tina D’Agostin, and mentions the Rock’s strongest unique selling points.

“That reduced friction, along with our design which prioritises individual privacy and supports the major privacy frameworks such

as GDPR, make it popular with end users who quickly opt in to access points where the Rock is used.

“We’ve also had success as a better more efficient solution on turnstiles over access cards or other biometrics like iris, fingerprint or palm given the accuracy and speed of our device,” Tina D’Agostin claims.

Partner with Axis

The interest for the technology of Alcatraz AI is increasing fast. In early March it was confirmed once again as leader in autonomous access control solutions when it announced a partnership with Axis Communications. The Swedish company will provide Alcatraz AI’s flagship facial authentication product, the Rock as part of the Axis family of solutions that improve security and optimise business performance. Alcatraz AI is now a member of the Axis Tech-



Vince Gaydarzhiev, the founder of Alcatraz AI.

nology Integration Partner (TIP) programme.

“The way in which Alcatraz AI is transforming how people access buildings and secure areas aligns perfectly with the Axis vision of combining intelligent technology and human imagination to improve security and optimise business performance,” comments Tina D’Agostin, CEO.

Together Axis and Alcatraz deliver secure rapid authentication as a single-factor solution or access at the speed of single factor when used as part of a multi-factor system. The Rock’s intelligent tailgate detection can send alerts and actionable insights to Axis’ access control management software to reduce the threat of a breach due to tailgating and support compliance in zero trust environments.

The combination of Axis access control systems and the Rock’s simple and secure enrollment process improves efficiency and effectiveness for both administrators and users. Designed in compliance with the latest privacy frameworks, Axis channel partners and end customers now have an unmatched opportunity to manage and ensure privacy compliance.

“We are thrilled to have Alcatraz AI join our Axis Technology Integration Partner Program,” states Drew Pacino, Business Development Manager at Axis Communications.

“Their facial authentication product is truly unique, and by integrating this with Axis devices can offer even more value to our mutual Channel Partners and end customers. We look forward to a successful collaboration with Alcatraz AI.”



Alcatraz Rock was selected among the “30 Top Technology Innovations” of 2020 and awarded as a “Most Innovative Product” in 2022.

The Physical Security Business 2022–2027



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 2027?

The Physical Security Business 2022 to 2027 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, Elektravägen 14, 126 30 Hägersten, Sweden
Phone: +46 8 556 306 80, info@armedia.se, www.armediaint.com

Security Events

April



25-27 April
The Security Event -
Birmingham, United Kingdom
Venue: National Exhibition Centre (NEC)
Organiser: Nineteen Group
Tel: +44 (0)20 8947 9177
Email: info@thesecurityevent.co.uk
Website: www.thesecurityevent.co.uk/



26-28 April
Secutech Taiwan - Taipei, Taiwan
Venue: Taipei World Trade Center Nangang Exhibition Hall 2
Organiser: Messe Frankfurt (HK) Ltd
Tel: +886 2 8729 1099
Email: services@secutech.com
Website: secutech.tw.messefrankfurt.com

June



5-7 June
Algeria Fire, Safety & Security Expo
- Algiers, Algeria
Venue: Palais Expositions d'Algiers
Organiser: New-Fields Exhibitions, Inc.
Tel: +971-4-268-6870
Email: info@inf.ae
Website: inf.ae



6-8 June
Securex South Africa -
Johannesburg, South Africa
Venue: Gallagher Convention Centre
Organiser: Specialised Exhibitions
Tel: +27 (0)11 835 1565
Email: marketing@specialised.com
Website: securex.co.za

July



19-21 July
Secutech Vietnam -
Hanoi, Viet Nam
Venue: Friendship Cultural Palace
Organiser: Messe Frankfurt (HK) Ltd - Taiwan Branch
Tel: +886 2 8729 1068
Email: michelle.chu@taiwan.messefrankfurt.com
Website: www.secutechvietnam.com

September



19-21 September
SECURA - Algiers, Algeria
Venue: Venue: SAFEX (Union Hall)
Organiser: Easyfairs
Tel: +213 (0)550.853.033
Email: contact@securanorthafrica.com
Website: https://www.securanorthafrica.com/en/

October



9-10 October
OFSEC 2023 - Muscat, Oman
Venue: Oman Convention & Exhibition Centre
Organiser: Muscat Expo
Tel: +968 9123 7892
Email: nk@muscat-expo.com



11-12 October
FinnSec - Helsinki, Finland
Venue: Helsinki Expo and Convention Centre
Organiser: Messukeskus Helsinki
Tel: +358 40 450 3250
Email: customer.service@messukeskus.com
Website: finnsec.messukeskus.com



24-25 October
Sectech Sverige - Stockholm, Sweden
Venue: Stockholmsmässan
Organiser: AR Media International AB
Tel: +46 8 556 306 80
Email: deniz.baykal@armedia.se
Website: www.sectech.nu
Visit AR Media at Sectech

November



15-17 November
Sicurezza - Milano, Italy
Venue: Fiera Milano
Organiser: Fiera Milano S.p.A.
Tel: +39 02 4997.6224
Email: mara.borsani@fieramilano.it
Website: www.sicurezza.it

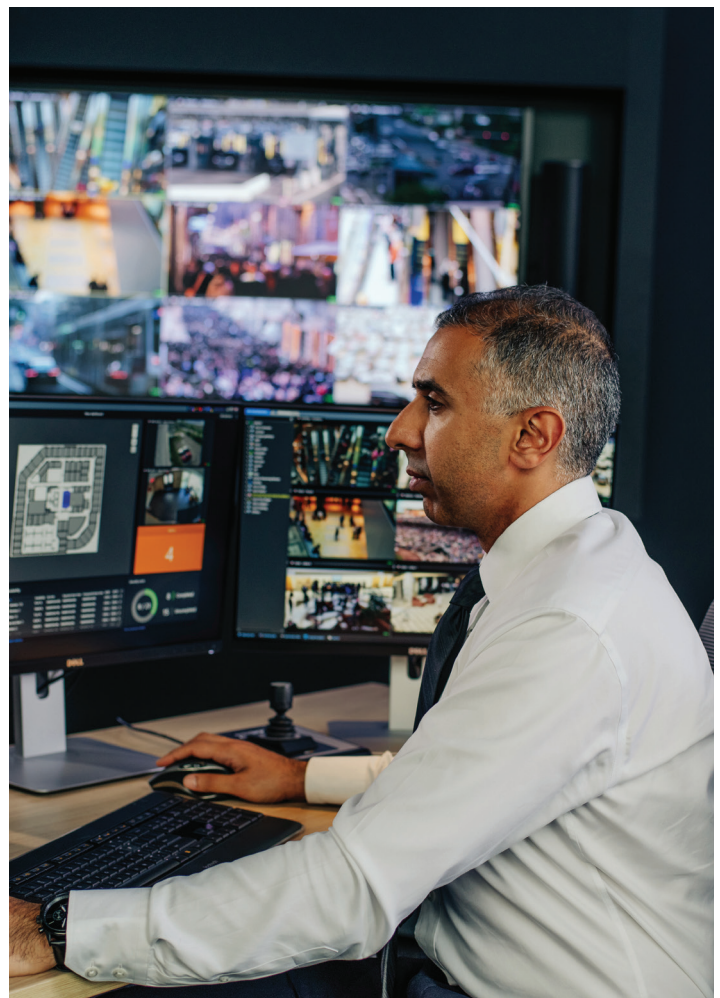
Changes may occur. Visit www.securityworldmarket.com for the latest updates.

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



Don't miss out!



24-25 October, 2023
Stockholmsmässan/Stockholm

SECTECH
EXPO & SEMINARS

www.sectech.se