

DETEKTOR



International

Publisher's comment

**Cybersecurity – a new buzzword
for video surveillance providers**

Keen Yao, Hikvision to Genetec

"Vague accusations and outrageous claims"

Security technology market

**Security Solutions market predicted
to hit 370 billion dollars by 2022**

Security technology trends

Internet of Things – heaven or hell?

Business news

Alarm.com acquires Objectvideo

The interview

- **Martin Gren, co-founder, Axis**
- **Mario Kahlert, Head of Fire, Siemens**
- **Marc Handels, co-founder of Salto**

Security events

ISC West Expo in Las Vegas

VIDEO ANALYTICS REVIEW:

WILL DEEP LEARNING BRING A REVOLUTION?

Everybody.



Everywhere.



Every day.



Ordinary days require extraordinary protection.

Find out more about the software behind the everyday at
IFSEC (London), stand #F500
or at [genetec.com/protectingeveryday](https://www.genetec.com/protectingeveryday)

[genetec.com](https://www.genetec.com)

Genetec™

© 2017 Genetec Inc. GENETEC and the GENETEC LOGO are trademarks of Genetec Inc., and may be registered or pending registration in several jurisdictions.



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

Head office:

AR Media International AB
Västberga Allé 32 • S-126 30 Hägersten
SWEDEN
Tel: +46 8 556 306 80 • Fax: +46 8 19 10 11
E-mail: info@armedia.se
www.detektor.com
www.armedia.se

Asia Office

Asia office
Asha Chang
AR Media International (Asian Branch)15F,
No 55, Binhai Rd. Sec. 1,
Danshui Dist., New Taipei City 251
Taiwan
Office phone: +(886-2) 2622 1365,
+(886-2) 2622 1385
Office fax: +(886-2) 2622 1305
Mobile: +(886) 922 116272
Email: asha@armediaint.com
ashachang@gmail.com

General Information

- Detektor International is published quarterly.
- 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@securityworldhotel.com

Subscriptions

Anette Friberg
Rate for four issues is Euro 50
+46 8 556 306 80

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

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

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Carlos Cisternas
carlos.cisternas@armediaint.com

Printing

Sörmlands Printing Solutions AB, Sweden, 2017



Lennart Alexandrie, Publisher

Cybersecurity –a new buzzword for video surveillance providers

As technology development moves on at an increasing pace the security industry is constantly taking advantage of the progress. The migration from an analogue to a digital technology was a real game changer. Suddenly technology integration has become much easier and cost effective. User friendliness and flexibility seem to no longer have any limits.

The development towards integration between different technology systems will of course continue. Security technology is of course attractive, and increasingly in higher demand in building automation projects as we enter the new world of smart buildings and smart cities. Internet of Things is not just a buzzword, it is a real revolution in the history of mankind.

The opportunities to successfully create customer designed solutions have become better than ever before – through technology based services targeted towards companies, public organisations and private homes. We live in an era where the Internet of Things is becoming the key to the modern efficient and environmentally durable society. Or at least it looks that way.

But IoT is also an opener for serious threats to the privacy and security of individuals. It is for sure also a threat for corporate and government organisations as well as to entire nations. Our connected devices are potential distributors of both value added services and vicious network attacks. Do we have a track of all the purposes our online devices serve? The question is rhetoric. There are jobs that have to be done in order to make IoT safer. Connected devices can be and are hacked and used for initiating and conducting intrusions and attacks on servers. There are several examples where security technology devices have been hijacked and then used to become the distributor of harmful malware. Mostly this has involved IP cameras or DVRs.

A general view in the western world is that we should watch out for Chinese security products for this reason, but it's not that simple. Big Japanese, US and European manufacturers' brands

are also listed among the products that have been hacked and used to infect networks to cause a costly mess. All online products represent risks. The risks could easily be considerably reduced if the users of the IoT devices were to avoid using manufacturer's preset user names and passwords. It is through continuous scanning of the manufacturers data that hackers often succeed in hijacking devices and then using them to distribute malicious code, such as Mirai, and subsequently force down the servers or deliberately cause other damage.

The security industry has to take more responsibility, not only the manufacturers, but also distributors, integrators and installers. Make demands on suppliers, inform/educate the customers and do not always let price be the guide to finding the product of choice. Learn about cyber security and demand that your suppliers also are aware and educated. Increasing the security within the products will create costs for the manufacturers. I believe the market is willing to pay for it. Choosing the cheapest alternatives may be a very expensive and unpleasant experience.

In the previous issue of Detektor (1/2017), we published a special editorial about video surveillance and cyber security. In this issue, we follow it up by publishing what was said about IoT and cyber security at the recent Sectech exhibition in Norway. It is a wider perspective of the subject which is very much about the threats and the challenges we have to meet.

At the recent ISC West Expo there were several exhibitors, not least among the video surveillance product providers, that highly profiled their approach to cyber security during the show. Cyber security has become a new strong buzzword and there are no doubts that the whole professional security technology industry is taking the cyber security threat seriously – not only western companies. This is a necessary first step before running too deep into IoT projects. There are several challenges to solve and the security technology industry has to take its share of responsibility. I believe it's about to happen.

- 3 Publisher's Comment.** Cybersecurity – a new buzzword for video surveillance providers.
- 8 Voice of the Security Industry.** Hikvision to Genetec – Vague accusations and outrageous claims
- 10 Security Technology Market.** The video surveillance market to double in revenue by 2022.
- 14 Technology Trends.** Internet of Things – Heaven or hell?
- 18 Business News.** Alarm.com acquires Objectvideo.
- 25 The Interview 1.** Martin Gren, co-founder of Axis.
- 26 The Interview 2.** Marc Handels, co-founder of Salto.
- 27 The Interview 3.** Mario Kahlert, Siemens Head of Fire.
- 28 Security Technology Inside.** Video analytics review.
- 30 Security Events.** Report from ISC West.
- 31 Security Events.** ISC West product overview.
- 36 Security Events.** Ifsec International – Europe's largest security event in 2017.
- 38 Security Events Calendar.** The international overview of scheduled security shows.
- 28 Security Buyers Guide.** The directory of important suppliers of security products & services.



Electronic perimeter security highly focused in Las Vegas

ISC West was held from the 5th to the 7th of April. It was a great manifestation of how technology can make a difference to help companies and other organisations to fight crimes and other unwanted events through technology that either prevents those crimes or alerts operators before the crime or the fire even starts.

Page 30



Martin Gren believes in IP audio and IP intercoms.

Page 25



Marc Handels about main trends in the access control market.

Page 26



Mario Kahlert: "IP cameras will not replace fire detectors"

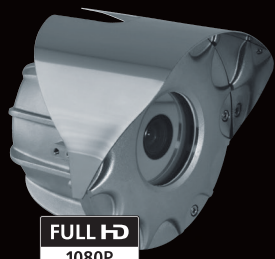
Page 27



ISC West product overview.

Page 31

BE READY FOR AN **EXTRA**-ORDINARY NEW WORLD



FULL HD
1080P

- **Extra**-competitive
- **Extra**-light
- **Extra**-compact
- **Extra**-flexible

With the MAXIMUS MMX cameras, a new world of cost effective solutions is available for monitoring tasks in the most challenging conditions in onshore, offshore, marine and heavy industrial environments.

MAXIMUS **MMX** CAMERA



VIDEO SECURITY
PRODUCTS

www.videotec.com

Made in Italy



Dahua Video Intercom SIP Solution Give You Peace of Mind

With the rapid development of the social economy and the steady improvement of people's living standard, speed and safety is becoming increasingly important in people's personal and professional life. Now almost everything is expected to be done in a fast, real-time and safe way. Residential compounds and office buildings had difficulties managing visitors and in-house communication, causing efficiency decrease. Traditional way of visitor-managing requires security workers to call the relative person/people with visitors painfully waiting at the gate of the building or compound, which is very time and labor consuming.

Dahua Video Intercom SIP Solution

Dahua has created this new comprehensive and intelligent Video Intercom SIP Solution. Dahua Video Intercom SIP Solution enables residential compounds, office buildings and other fields requiring audio and video intercom to manage visitors and in-house communication using less manual labor while delivering better safety and higher efficiency. SIP is an international standard video phone protocol, featuring open and easy access. The end-to-end Dahua video intercom systems support

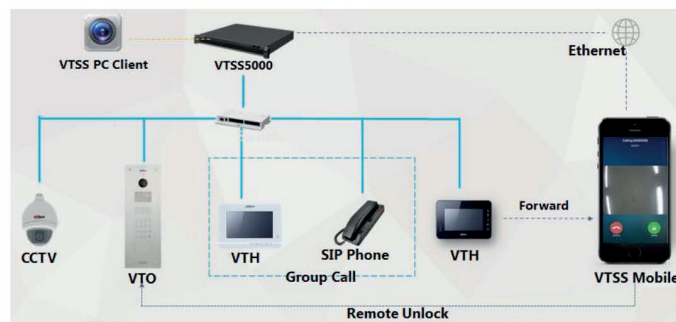
standard SIP protocols, providing reliable cameras, mobile phone App, integrated platform and intelligent technologies to ensure residential compounds, office buildings and other fields requiring audio and video intercom are well guarded and efficiently run.

Intercom

Intercom units can be installed indoors or you can choose a SIP phone. Units installed next to doors and indoor areas can be equipped with audio and video intercom, and SIP phones with voice intercom. SIP phones can create group calls between indoor units so people are able to listen in from anywhere. Calls can be made within the house or to other houses with indoor units and SIP phones. Two-way calls can be made between all devices and management centers, enabling calls to be made for emergency assistance to property management centers.

Mobile Phone APP Function

Finding out how to receive information from external visitors is a commonly faced problem. To specifically deal with this situation, the SIP solution is designed with a mobile phone APP function, so when visitors drop by and press the intercom, it will be forwarded through the indoor unit to your phone. When you go out, you can set calls to be forwarded directly to your mobile phone; by using the settings, the indoor unit can be programmed to forward to your mobile phone when no one answers the intercom or the intercom is busy, ensuring that



responding to visitors is quick and easy.

Security Upgrade

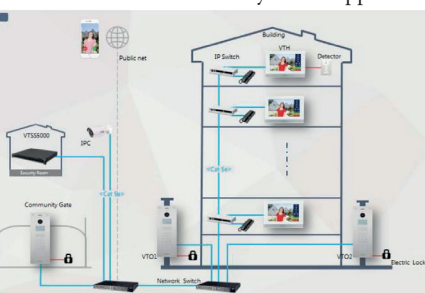
House doors can be installed with a single-button device to serve as a secondary confirmation by guests. Indoor devices provide real-time IPC monitoring and can switch between multiple channels. In addition, the indoor units can also be connected to multiple alarm sensors, providing all-round security. So when you go out or stay at home you can enjoy unparalleled peace of mind and comfort.

Platform Management – SIP Server VTSS5000

SIP Server VTSS5000 is an integrated system for video intercom and video management offering storage services, an operating system and hardware in one box, enabling true plug-and-play and easy deployment. It is light and small. The VTSS5000 optimized software services can manage 5000 video intercom IDs and 200 IP devices and is a professional management platform that can be utilized in fields requiring video intercoms. The embedded Linux system is safe and reliable, with support available 7/24 ensuring

stable operation. C/S architecture separates the client and the management terminals, so that the administrator's authority to allocate and configure the management and use by the operator are separate and easy to use. The administrator supports the management of the tenants in the residential area, including the creation and maintenance of personnel information, the issuance of card information, the issuance of fingerprint information and management of access rights. Everything is devoted to increasing security.

Using advanced technologies (Mobile Phone App, SIP Server VTSS5000 and etc.), Dahua Video Intercom SIP Solution provides comprehensive security services whenever and wherever you are. After being widely applied in many cities, Dahua Video Intercom SIP Solution has been proven efficiently and effectively in managing visitors more safely and efficiently, as well as in-house communication. In addition, because of its innovative system architecture, this solution is flexible to upgrade with technology change and expand with compound and building infrastructure growth.



About Dahua Technology

Zhejiang Dahua Technology is a leading product and solution provider in the global video surveillance industry. We had the 2nd highest market share of global video surveillance equipment market in 2015 according to IHS 2016 report. We were ranked 4th in 2016 by a&s Security 50, which ranks global security industry players according to total security equipment sales.

We commit to provide the highest quality product with the latest technology to enable our customers to perform their business successfully. Our company invests about

10% of annual sales revenue in R&D since 2010. We have more than 5,000 R&D engineers today. Our engineers work on cutting edge technologies in camera lens, image sensor, video encoding & transmission, embedded processor, graphic processing, video analytics, software reliability and network security technology. We partner with leaders in respective areas to make sure our customers enjoy the latest and the best technologies. Numerous Dahua products have been acknowledged and awarded by professional associations and organizations in the security industry.

Visit: <http://www.dahuasecurity.com>

Visualize every detail in its original and natural form

180° panoramic camera without image distortion



Features

- 3 sensors in 1 camera and 1 IP address
- Seamless splicing technology for perfect image presentation
- 180° viewing angle without image distortion
- Easy installation to save cost both in cabling and labor cost
- All models come with IP67 & IK 10, designed for outdoor application



CE FC CCC UL RoHS ISO 9001:2000



DAHUA TECHNOLOGY CO., LTD.

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

Keen Yao, Hikvision, responds to statements about cyber security by the CEO of Genetec, Pierre Racz

"Racz provides vague accusations and

Pierre Racz, CEO of Genetec was interviewed by Detektor International 1/2017. His claims in that interview (also published on Securityworldhotel.com) are the target for the heavy criticism in the open letter, written by Keen Yao, the VP of Hikvision International Business Center.

In the Detektor-interview Pierre Racz talks about why Genetec has imposed special restrictions on the use of Hikvision products, connected to the Genetec VMS platform.

Keen Yao responds with this open letter:

"Genetec's CEO Pierre Racz's recent comments in an interview with Detektor Magazine, mimic an American blogger site (John Honovich, IPVM.com, publisher's note), whose sole business goal appears to be instilling fear, uncertainty and doubt about Hikvision because it is a Chinese company.

The Genetec leader's rants about war, espionage and treachery are certainly worthy of a Hollywood tabloid, but security professionals and integrators can see through Pierre Racz's fear-mongering. They notice that Racz provides vague accusations and outrageous claims.

In the interview with Detektor Magazine, Pierre Racz proclaims that "governments have told us they are extremely concerned with the origin of these [Hikvision] products." Racz does not specify which

governments are concerned, but those governments must have their proverbial heads in the proverbial sand, because there are no secrets about the origins of Hikvision products. All Hikvision products are proudly "Made in China."

Hikvision products are manufactured, inspected and tested in world-class factories in Hangzhou, China, a city that Westerners often refer to as the "Silicon Valley of China." Hikvision regularly hosts security integrators and security professionals from the West and all over the globe for tours of our factories. Our visitors are interested to see our industry-leading cybersecurity best practices at work, and how we continually increase efficiency by using robots and other sophisticated processes, and they're also interested in witnessing the sheer scale of our operation.

The Genetec leader's rants about war, espionage and treachery are certainly worthy of a Hollywood tabloid.

Genetec's leader regurgitates insinuations about Hikvision products providing access to the Chinese government. This claim is absurd. There is no motive for a commercial company to provide access to a government, whether it's an American, Swedish or Chinese company. Hikvision has sold tens of millions of network-connected devices—IP cameras and NVRs—that sit on the Internet. There is no report anywhere that such access has taken place. Any claim otherwise is just hogwash.

Exhibit at Denmark's biggest security exhibition in 2017

**SecurityUser
EXPO!**

27–28 September 2017



Security User Expo will take place at the Bella Center in Copenhagen from 27th to 28th of September 2017. It is the fourth time that this biennial exhibition and conference is being organised by AR Media International in collaboration with Sikkerhedsbranchen, the Danish Security Industry association.

For stand reservations and more info: www.securityuserexpo.com



Deniz Baykal,
Event Manager
Tel. +46 8 556 306 80
Mob. +46 73 987 53 33

Organiser:

In cooperation with:

ar media
Connecting Security Buyers and Suppliers

Sikkerhedsbranchen
Den Danske Brancheforening for Sikkerhed og Sikring

Media partners:

DETEKTOR

**SECURITY
WORLDHOTEL.COM**

SecurityUser.com

A new concept this year is that the event will be held over two days instead of three. This means that not only will the event be more concentrated in terms of time but also at a lower cost for exhibitors.

The event is aimed at security managers and coordinators in private companies or public institutions but also at the supplier chain – from distributors to system integrators, installers, consultants and guarding companies.

The mini conferences include topics such as counter terrorism, IoT and Smart Cities, and also include the yearly Safety Camera Day, that deals with the crime fighting benefits and integrity aspects that come with the increasing use of video surveillance systems.

The Security Industry Award dinner will be held on the 27th of September, after the first exhibition day, and includes entertainment and award presentations.

Don't miss out on the one and only security exhibition in Denmark, 2017. Book your stand now!



outrageous claims"

Furthermore, anyone who knows anything about technology and engineering understands that these arguments are laughable. Interestingly, the Genetec leader appears to lack both understanding of how the systems work, and he appears to have very little respect for the infosec professionals who protect their companies.

A video surveillance system is comprised of front-end devices, back-end devices, network devices and a system platform. This is where the CISOs and other infosec professionals come in. If any change is made to an edge device – like a camera – it would immediately be detected by the network devices and security platforms.

Pierre Racz is fabricating disinformation about Hikvision's ownership and financing. He says that Hikvision is "owned by the government and has been given a \$6 billion subsidy."

Pierre Racz is fabricating disinformation about Hikvision's ownership and financing.

These claims are false, misleading, and irresponsible. Hikvision is a publicly traded company, listed on the Shenzhen Stock Exchange. As of 30 September 2016, our shareholders include government entities (42 percent of our stock is held by two state-owned enterprises). Major stockholders include a Hong Kong businessman, and common-shares investors, including international institutional investors. UBS AG and JP Morgan are among Hikvision's top 10 shareholders.

Also, the subsidy myth has been debunked repeatedly. Like other major corporations, Hikvision uses different types of financing channels

Pierre Racz, CEO of Genetec, about Hikvision:

"Governments are extremely concerned"

Genetec will continue to support devices from Huawei and Hikvision, but new customers using these devices will need to sign the waiver and pay a special 250 USD connection license in addition to standard license fees.

end-user", stated Pierre Racz. "Such risk assessments are made by the end-user based on the end-users' circumstances."

He also adds that Genetec sheds light on obfuscated origins of equipment – so customers can

organisation, the answer is yes. If you are an American governmental organisation, the answer is definitely no. If the risk factor is between 0 and 1, I can guarantee it is not 0. It is somewhere in between 0 and 1. A simple, hypothetical

"Dahua is a private company and you can sue them and they are motivated by the risk of losing the trust of their customer base. The risk is not zero, but less than with a company that is owned by the government and has been given a

such as an IPO, bank credit facilities and bond issuances.

Hikvision in August 2016 closed a credit facility of more than \$3 billion, with the Export-Import Bank of China. In November 2015, Hikvision secured approximately \$3 billion line of credit with the China Development Bank.

These are lines of credit. If and when Hikvision takes a loan on a credit line, the entire amount must be repaid with interest. It is not a subsidy or free gift. It works the same way as the other lines of credit that Hikvision has with other international financial institutions including Citibank, HSBC and Deutsche Bank, among others.

Genetec also makes assertions that Hikvision is not a commercial entity or is somehow not interested in commercial success. We are the world's leading video surveillance provider with extremely strong growth. Our preliminary 2016 financial results, released last week show year-over-year overall revenues increased 26 percent and overall profits increased 24 per cent".



Keen Yao, the VP for Hikvision International Business Center.

Keen Yao, VP of Hikvision International Business Center

PANOMERA® Multifocal sensor system

Stop looking in the wrong direction

There are thousands of PTZ cameras in use today, however when video recorded evidence is required they are often found to be looking in the wrong direction. Similarly there are hundreds of thousands of static cameras that might be looking in the right direction, however when reviewed and a digital zoom function is used, the images are too pixelated to get any relevant evidence.

With the multifocal sensor technology from Dallmeier these issues have been eradicated. With Panomera®, a huge area can be displayed with a completely new resolution quality, in real time and at high frame rates of up to 30 fps. Live or playback, Panomera® is never "looking in the wrong direction"!



www.panomera.com



Dallmeier

Video surveillance market to double in revenue by 2022

Hadapsar, India

New information from researchers Marketsandmarkets estimates that the video surveillance market was worth 30.37 billion dollars in 2016 and is projected to reach 75.64 billion dollars by 2022.

Implementation of video analytics, increased installation of video surveillance systems, usage of cloud-based services for centralised data, use of high-definition cameras, and the need for physical security are the major factors cited in the report as being the driving factors for the growth of the video surveillance market.

Growing security concerns

Based on hardware, software, and service, the hardware segment is expected to lead the video surveillance market between 2017 and 2022. Hardware comprises the major part of video surveillance systems and includes cameras, monitors, and storage solutions, among others. Hardware products for video surveillance have become technologically advanced

and affordable. Growing safety and security concerns, rising crime rates, and increasing terror attacks are some of the factors driving the growth of the camera sub segment of the hardware arena. Continuously decreasing prices of cameras have resulted in an increase in the adoption of surveillance cameras across the globe. With the increasing use of cameras, the servers, storage devices, and monitors sub segments of the hardware area are also growing at a significant rate.

High growth in commercial segments

Based on vertical, the commercial segment is expected to grow at a high CAGR between 2017 and 2022. The high demand for security systems from large and

small retail businesses is increasing to reduce robbery and inventory loss. In the commercial sector, financial institutions and banks prefer video surveillance systems to provide security to buildings, maintaining cash management, and monitoring customer and staff activities. This enhances security parameters and is driving the commercial segment of the video surveillance market.

APAC leads the market

According to the researchers, the APAC region is expected to lead the video surveillance market during the forecast period. The growth can be attributed to the adoption of new technologies (cloud services and other analytics technologies) and security systems to protect economy and infrastructure from criminal activities and terror attacks.



The detailed images are helping the cameras' inbuilt analytics to detect and analyse incidents more accurately.

Thus, a decline in the prices of IP cameras and the presence of big players are the factors that are expected to drive the video surveillance market in the region. Currently, China is undertaking several projects, especially in the infrastructure sector such as rail, airport, stadia, and highway systems, which are expected to require high definition surveillance systems that can capture clear images even in the dark.

Strong growth ahead for two factor authentication market

Ontario, Canada

As users become more concerned about the safety of their data, two factor authentication, or, TFA is gaining momentum. According to research analysts at Technavio, the global market was valued at 4.73 billion dollars in 2016, and is expected to reach 13.63 billion by 2021 at a CAGR of 23.57%.

Currently North America has the largest share of the market at 36.79 percent, but Europe will likely make the highest contribution to the market's growth with a CAGR of 24.19 percent.

"Strong customer authentication"

One indication of this is a move by the European Banking Authority (EBA) to require "strong customer authentication" for all electronic payments over 10 euros (or about 10.60 dollars). With the average online retail purchase in Europe being over 85 dollars, this proposed standard would create substantial demand for services such as TFA,

requiring many retailers to adapt their checkout processes.

Internet giants supports TFA

Internet giants such as Facebook and Google are also implementing TFA, though this is currently optional rather than a requirement. Facebook recently announced that it will support USB keys for TFA, as an alternative to sending a code to the user's mobile device. The social media company has already offered TFA for several years, but the option to use a USB key makes the service more flexible.

Google's alternative

Google has also recently added

to its security options, making it possible for IT administrators to require a company's employees and other users to authenticate with a security key. This provides the protection of TFA without the need for mobile apps or text messages, and is the highest level of security available under this system.

Consumers resistance

Google's newest move addresses one of the challenges associated with TFA: it's inconvenient. Many people object to having to go through an additional step whenever they need to log in, even if that step is relatively quick and simple. By allowing security keys,

Google alleviates this somewhat. Consumer resistance to TFA is one of the factors making retailers apprehensive about the EBA's proposal to increase security. The concern is that consumers will be more likely to abandon their shopping carts and not go through with online purchases because of the added step.

Technavio researchers believe that this challenge can actually be an opportunity for TFA, however. It means there is space in the market for more tools to streamline the process and make it faster and more user-friendly. If the EBA introduces this new standard, there will be significant new demand for secure, customer-friendly TFA solutions. Organisations outside of Europe will also likely adopt these solutions for their own purposes.

TFA is not loved but many market opportunities still exist.



IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK

THE ONLY LARGE SCALE SECURITY EVENT IN EUROPE THIS YEAR



Over 10,000 security products to test & trial

- Find your perfect solution from over 600 leading security suppliers
- Pre-book 1-2-1 meetings with the suppliers you want to work with
- Discover future trends with free education seminars & discussion panels
- Grow your network with over 27,000 other security professionals
- Get discounted air travel & accommodation exclusively for IFSEC visitors

REGISTER TO GET YOUR **FREE** BADGE TODAY AT IFSEC.EVENTS

Supported by:



Your badge also gives you entry to:



Commercial drones pose security threat to the West

London, UK

Commercial unmanned aerial vehicles (UAVs) are a growing security threat in the West, according to jihadist media monitoring conducted by Jane's by IHS Markit, a world leader in critical information, analytics and solutions.

"The Islamic State's use of weaponised UAVs represents a growing security threat to the region and in the West more generally," says Otso Iho, senior analyst, Jane's Terrorism and Insurgency Centre (JTIC).

The JTIC team monitored and analysed the growing use of UAVs for operational purposes by militant Islamist groups over the past 12 months, covering a broad range of propaganda channels and formats.

Is already in use by Islamists

The Islamic State has been the most notable and predominant militant group making use of UAVs in both propaganda and tactical military contexts. However, other militant groups in Iraq and Syria have used UAVs for reconnaissance and propaganda, and also to conduct attacks on their adversaries.

Harakat Ahrar al-Sham al-Islamiyya illustrated its use of reconnaissance UAVs in its video "Winds of Rage" in 2016, while groups such as Hizbullah and Hamas have made use of UAVs against Israel. More recently, Islamist militant group Jund

al-Aqsa released a video on 2 September 2016 purportedly showing a UAV dropping small, unguided explosive devices on military positions in Syria's Hama governorate. The Islamic State has subsequently built on this, conducting multiple such attacks on security forces during ongoing fighting in the Iraqi city of Mosul, which it highlighted in its "Knights of the Departments" video released on 24 January.

Propaganda may inspire

Otso Iho emphasizes that the Islamic State is very particular with its propaganda.

"The group uses it as a weapon to inspire at home and abroad, When it calls on its followers to conduct attacks with knives, vehicles, and IEDs, the calls are answered. As such, the more frequent use of weaponised UAVs in videos – and the wider commercial availability of UAVs – is

likely to be of inspiration for both supporters of the group and other militant groups beyond Iraq and Syria, and indeed beyond militant Islamist actors.

Groups with lower profiles – such as right-wing extremists across Europe or dissident republicans in the United Kingdom – will appreciate the significant attention brought by attacks involving UAVs. It is possible that their

use may have entered these actors' tactical thinking as a viable weapon, given their widely publicised use and availability, states Iho, Otso Iho claims further that the force multiplier and value-add from a militant group's perspective is enhanced by the propaganda value afforded by a UAV-facilitated attack, as well as the footage that can be recorded of such attacks and exploited for propaganda and recruitment purposes.

Symbolic attacks

Chris Hawkins, JTIC analyst, also comments on the UAV threat.

"Although the use of UAVs in an attack context – both in dropping munitions and in booby-traps – has garnered significant media attention through the



Commercial unmanned aerial vehicles (UAVs) are a growing security threat in the West, according to jihadist media monitoring conducted by Jane's by IHS Markit.

novelty attached to it, its use as an effective military weapon in a battlefield context is limited more to symbolic and propaganda use."

The commercially-available UAVs used by the Islamic State – including fixed-wing Skywalker X7s or similar, and quadcopter-type UAVs – offer relatively small payloads, typically approximately 1-2kg. Although 1-2kg of explosives could cause significant damage, this payload also has to include cameras and other navigational systems, meaning at least half of the payload could be used for explosives. This, coupled with a short operation time of between 23 minutes and two and a half hours, means the efficacy of using UAVs in such contexts is largely limited to symbolic attacks, the JTIC report said.

Security Solutions market predicted to hit 370 billions dollar by 2022

Hadapsar, India

The security solutions market is expected to grow from USD 206.69 Billion in 2016 to reach USD 372.90 Billion by 2022, at a CAGR of 10.16% – this is according to the latest research analysis from Marketsandmarkets.

The growth of the security solutions market is expected to be driven by the necessity to protect individuals as well as property from rapidly evolving threats, increasing consumer awareness and security concerns, willingness to pay for security systems, growing demand

for the use of wireless technology in security systems, and adoption of IoT-based security systems.

Property protection

The commercial end-use industry in the security solutions market held the largest share in 2016. The increasing incidences of crimes such as theft of physical as well as data/information have led to a need for security systems to protect not only the property owners but the property as well. With this intention, corporate organisations are

investing substantial amounts to protect sensitive data and their employees. For instance, access control systems or biometric security systems are used in server rooms of organisations that deal with sensitive data. Such security solutions prevent unauthorised access and thus safeguard property and people from untoward incidences.

Wireless systems market at the highest growth

The wireless systems segment is projected to grow at the highest

rate in the security solutions market between 2017 and 2022. Wireless systems are not only easy to install but can also improve the interactive monitoring services of a system. They can be remotely operated, which makes them easy to use. Considering these benefits that wireless systems offer, the segment is expected to grow at the highest rate during the forecast period. Big players such as Frontpoint Security Solutions (U.S.) and ADT Corporation (U.S.) provide wireless security systems.

Massive growth predicted for passenger screening market

London, UK

In a highly dynamic security threat landscape, the key to capturing market share is not advanced equipment, but its associated support system. The \$1.74 billion passenger screening market will hit the \$11-billion mark over the next five years on the strength of futuristic products, as well as system maintenance and upgrades - according to analysts from research company, Frost & Sullivan.

Screening systems used at checkpoints require service at specific intervals, which can be a challenge due to high passenger rates during seasonal travel. Therefore, there is a large market for service providers that can ensure quick parts replacement during maintenance checks.

“The passenger screening market will get a boost from the

airport construction and modernisation boom in Asia-Pacific and Middle East,” said Frost & Sullivan Aerospace & Defence Research Analyst John Hernandez. “Additionally, countries competing to host world events will have to build infrastructure to handle the surge in tourists, which translates to massive revenue opportunities for the passenger screening market.”

Global Passenger Screening Market, Forecast to 2021 is part of Frost & Sullivan’s Security Growth Partnership Subscription. It finds that while passenger screening is necessary, the failure of US Transportation Security Administration (TSA) screeners to detect fake explosives has made the government take a closer look at checkpoint proce-

dures and training.

Biometric technologies are being implemented in a variety of commercial markets for use at checkpoints and border control stations. Cell phone applications that make use of biometrics have significant potential as screening devices. Passenger screening will eventually evolve into a subtle process, wherein travellers will be screened discretely, without causing any inconvenience. This is key since the public has voiced its concerns about invasion of privacy and identity theft when using biometric technologies.

“Meanwhile, retailers could promote the use of biometrics at the time of sales in order to



The passenger screening market will get a boost from the airport construction and modernisation boom in Asia-Pacific and Middle East

obtain market intelligence and the ability to personalise offerings,” noted Hernandez. “In due course, the consolidation of identification documents such as passport, driver’s license, credit cards and access cards may well transform the security industry.”



VARIO2 Next Generation LED Illuminators

Up to Double the Power Output - Greater Illumination Distances - Outstanding Surveillance Images at night
Standardised Specification Data - Advanced Security Settings

rayTEC
www.rayteccctv.com

Internet of Things – heaven or hell?

There is talk that the Internet of Things is a saviour that will solve everything from welfare problems to environmental degradation and revolutionise people's everyday life. Even in the security industry, IoT is seen as the path to value-added services that will open up for a new growing

market. However, during the last year, the vision of salvation has become clouded due to frequent and serious cyber attacks. At the Sectech security show in Oslo, security professionals gathered to hear three speakers discuss IoT and security. Detektor has summarised the main points.

The number of connected devices is booming, but at the same time, the last year has shown that IoT is vulnerable to hacker attacks. James McHale, Senior Analyst at the market analysis company Memoori, believes that education and faster standardisation are the solution to cyber security problems. "There is technology in order to make the devices safer, we just need to do it more efficiently", he says.

By Henrik Söderlund



James McHale, Senior Analyst at the market analysis company Memoori.

James McHale, Memoori:

"We can reach a new level"

There is a great variation in predictions about how many units will be connected in the future. Some market research companies claim that there will be 20 billion connected devices by 2020, others believe there will be 50 billion. This means the CAGR will be more than 30 per cent and regardless of who is right, James McHale claims it is extremely important that IoT should not only be about collecting data, but converting it into information that adds value to the end customers.

"We believe that smarter devices at the edge and platforms, in order to be able to present this collected data to people, will allow us to ultimately move to a situation where we can provide valuable insights to clients and that is really important", he says.

Problems with cyber attacks

Over the past year it has become clear that many IoT devices are poorly protected and easy to hack. James McHale says: "There is a big problem with IoT and that is cyber security. We have seen several cases where both security cameras and other products have been used in DDoS attacks on major websites like Twitter and Spotify. This was done with a malware called Mirai, which basically scanned the internet looking for devices that were poorly protected

and used default settings".

He also stresses that the physical security industry must focus on solving security problems and provide safer and more robust solutions. The technical solutions are already available.

Back doors

Another problem that has attracted a lot of attention lately is the so-called back doors in security cameras. This was highlighted in the last issue of the Detektor magazine. The Chinese camera manufacturer Hikvision has been accused of having back doors in their cameras, which would make it possible for the Chinese government to take part of video footage from cameras (but no evidence has been presented and Hikvision has called the allegations baseless). James McHale believes this may have negative consequences for Hikvision and it will make it more difficult for the company to sell surveillance cameras to government projects around the world. However, he also believes that Hikvision is aware of the situation and is good at producing cheap cameras with high quality, and this will continue to make them attractive on the market.

A new way to look at buildings

James McHale has scrutinised

IoT in smart buildings and the percentage of products in those buildings that are connected to the internet. Video surveillance products are most common: 54 per cent of them are online, followed by 33 per cent of the access control systems, 30 per cent of the building automation systems and 29 per cent of the lighting systems. The market for IoT in buildings is expected to almost double from 2017 to 2021.

"I believe that the Internet of Things fundamentally will change the way we design and manage buildings. I also believe that the buildings will shape our behaviour. We will no longer say that a building will be great if only occupants know how to use it, but that a building will be great if it understands its occupants", says James McHale.

He argues that those who use a building want working environments that embrace technology and they want it to operate smoothly.

"It may not be reasonable to believe that every smart building should be designed purely for its occupants, but that does not mean we should not strive towards that goal and if it is done, then the return on investment will increase", says James McHale.

Focus on value-adding

Big data and cloud-based software

services will occupy an important part of the future of smart buildings.

According to James McHale, the value will be about 32 billion dollars in 2021. It equals an annual growth rate of more than 25 per cent. At the same time, the global data volume will grow nearly 40 per cent annually from 16.2 zettabytes in 2017 to 60 zettabytes in 2021.

It is important to point out that despite increasing urbanisation, and thus a great demand for construction, 8 per cent of today's buildings are estimated to still look the same by 2050.

"It means that we must not only build better and smarter buildings, but also that we need to think smarter in terms of buildings that already exist", says James McHale.

He believes that it is important to focus on outcomes rather than outputs. Outcomes refers to the value or contribution that the products or services will bring to customers and users, while output refers to the actual products or services themselves.

"It is IoT that will give us the platform to collect and analyse data so we can measure and validate the outcomes. I think that is really important in order to move smart buildings forward", James McHale concludes.

Bjørn Søland, Nexus:

"IoT reminds me of the land rush"

The development of IoT is reminiscent of the land rush in Oklahoma in 1889, when an area of unassigned land was opened to settlement – it is all about market share and positioning, not security, according to Bjørn Søland, Head of IoT Business Development, Nexus Group. He warns that IoT can become the Internet of Listeners and the Army of Things if security is not taken more seriously.

By Henrik Söderlund

When Bjørn Søland visited the Mobile World Congress in late February and beginning of March, he did a search on how many of the companies present were working with IoT. The result showed a total of 1021; then he made a second search on "IoT security" which resulted in only four hits. Bjørn Søland believes this is a clear indication of what is happening right now.

"IoT reminds me of the land rush that took place in Oklahoma, USA, in the late 19th century. Everyone wanted to go out and acquire their own piece of land. There are many people who talk a lot about

IoT today, saying it is safe, but the focus is on market share and positioning", he says.

Important to make updates

Bjørn Søland emphasises that connected devices must be secured. Some of them may be used for as long as 20 years and it is important that software is updated, and encryption keys and algorithms are renewed. Strong authentication and digital signing is important in order to secure access to data and to verify who owns it and how access to data should be managed.

"Today data is leaking, and if

you do not update the encryption keys or the software for 20 years, I can guarantee that there is a whole lot of data leaking. If you do not update, the client will not have a secure system", says Bjørn Søland.

Secure identity

It is not only security products that suffer from an insufficient level of security – the same goes for many different types of connected devices. Bjørn Søland gives an example from the US in 2015, when a blood infusion pump was hacked. It did not require any authentication and the hacker could get access rights and basically control it anyway he wanted. Bjørn Søland believes that the identity of things is crucial if you want to ensure security.

"We have to have that and we need to improve security. The identity concept is extremely important", he says.

Individuals will suffer

Businesses and organisations



Bjørn Søland, Head of IoT Business Development, Nexus Group.

that are taking the step into the world of IoT, tend to focus more on interoperability and connectivity rather than security. One way to improve security is to establish clear policies on digital and physical access rights. At the same time, two out of three connected devices are estimated to be private, so the problem of cyber security very much concerns individuals, not just companies.

"It is clear that this will affect us", Bjørn Søland concludes.

Per-Christian Foss, Addsecure:

"Security has lagged behind the pace of innovation"

How can communication be secured in a connected world? Per-Christian Foss, Head of Sales for IoT at Addsecure, stresses that security must be emphasised from the beginning.

"Always start with conducting a risk assessment", he says

By Henrik Söderlund

Per-Christian Foss identifies five security challenges with the Internet of Things: an insufficient focus on safety, poor default passwords which makes the devices easy to hack, lack of updating routines, the communication not being secure and finally the large amount of IoT devices increase the risk.

A lot of incidents

"IoT brings great opportunities and will provide great benefits, both for businesses and individuals, as well as for society as a

whole. But there are clearly things that can go wrong. The problem is that IoT security has lagged behind the pace of innovation", Per-Christian Foss says.

In addition IoT devices can be used, and have been used in DDoS attacks against websites, there are also risks of attacks on critical infrastructure and theft of sensitive data.

"Before 2020, I believe that at least 25 per cent of all registered security incidents will involve IoT solutions. In order for IoT to reach its full potential, we need

to bring order to the security", Per-Christian Foss says.

Risk assessment and automatic updates

According to Per-Christian Foss, a cornerstone for improving security is to look at the whole solution, not just individual devices and to remember to think about security from the start.

"It is difficult to add security afterwards. Conduct a risk assessment and consider which devices could be hacked and what the consequences would be if that were to happen and how big the risk is", he says.

Other basic measures are to change passwords and use anti-virus software and the best possible operating system. The latter is often neglected because manufacturers want to keep the costs down. Software should pref-



Per-Christian Foss, Head of Sales for IoT at Addsecure.

erably be automatically updated, according to Per-Christian Foss.

He says: "When it comes to communication, one should question whether you need to be constantly connected to the internet. If we are talking about solutions for a fire alarm, we believe that communication should be carried out via a VPN channel in a private network."

H.265+ Takes Video Surveillance to the 4K Era



H.265+ Introduction and Background

Recently, ultra-high-definition surveillance cameras introduced 4K resolution to the security industry. However, 4K resolution has yet to achieve wide application, mainly because of the tremendous bandwidth and data storage requirements. Limiting the bitrate of an ultra-HD video feed while retaining a high-quality, 4K-image remains the biggest problem—a problem whose solution will decide the fate of ultra-HD surveillance video. Video transmission balances image quality, transmission capabilities, and data requirements – i.e., how much information and how it's handled. Therefore, image transmission optimization lies in advancements in video compression technology.

Until now, H.264 compression has been the industry-standard codec. When the H.264 codec found wide use, Hikvision developed its own compatible algorithm to go the next step, calling it “H.264+”. The next iteration in this codec lineage – H.265 – presently stands at the cusp of widespread adoption. And once again, Hikvision has already pushed this compression

technology to a new level. H.265+ employs an intelligent algorithm whose encoding technology stems from the H.265/High Efficiency Video Coding (HEVC) standard.

H.265+ optimizes the existing codec most strikingly where specific criteria are met in a surveillance video feed. This criteria consists of: 1.) a stable background where information rarely changes; 2.) a primary focus on the objects moving across that stagnant scene; 3.) a substantial period of time where a scene's moving objects appear only occasionally; and 4.) 24-hour non-stop surveillance where visual noise has a relatively large impact on image quality. In this type of environment, field-tests show H.265+ radically decreases the required bitrate of the ultra-high-definition surveillance video by up to 67% over H.265, thereby reducing required

bandwidth and storage. Bitrate reduction means cost reduction for consumers, as well as increased efficiency, stability, and reliability of all the hardware in a given surveillance system. Here's how it works.

Three Keys: Encoding, Noise, and Bitrates

With ultra-HD resolutions and higher efficiency transmission as the two primary objectives, H.265+ improves the compression ratio based on three key technologies: 1.) predictive encoding technology based on a background or reference frame, 2.) digital noise suppression technology, and 3.) long-term bitrate control technology.

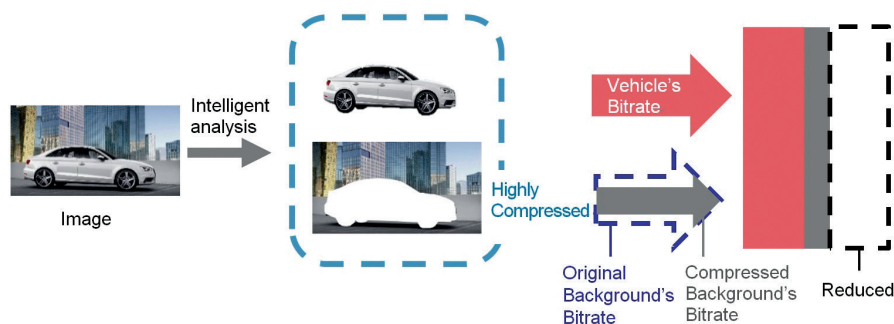
Predictive Encoding

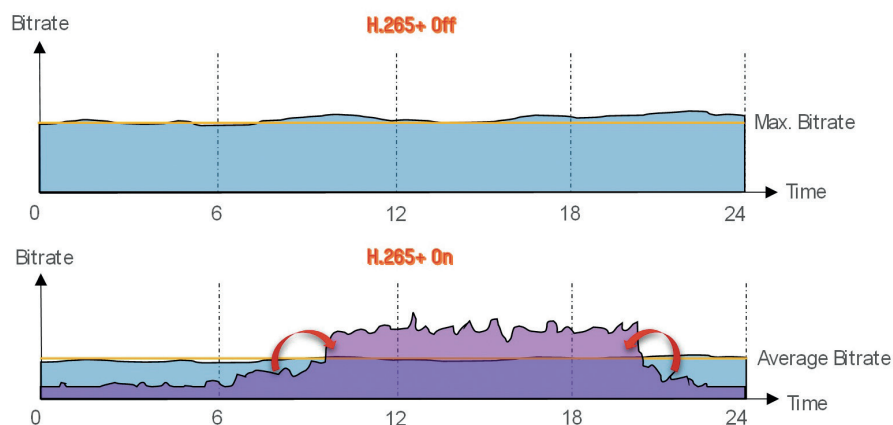
Predictive encoding can be divided into “Inter-frame prediction,”

creating a prediction model from one or more previously encoded video frames, and “Intra-frame prediction,” where the samples of a macroblock (processing unit) are predicted by using only information of previously transmitted macroblocks of the same frame. With inter-frame prediction, bitrate can be reduced by compressing only the difference in rates between a reference frame and any other frame. This reference frame – usually the background of a scene – will contain few if any moving objects. Fortunately, in most security surveillance, the background remains stagnant.

Noise Suppression

In order to guarantee a high image quality of moving objects, the encoding module also encodes the visual noise in the scene. However, using the predictive





encoding methods mentioned above, the H.265+ intelligent analysis algorithm distinguishes between the background image and moving objects so that each can be encoded with different encoding strategies.

A background image is encoded with high compression in order to suppress noise and applies data to new or moving objects. Since data transmission is limited, the overall bitrate dips substantially when compared against conventional video compression.

Long-Term Bitrate Control

Hikvision has introduced a concept it calls “Long-Term Average Bitrate” to make full use of a data from a video feed. Long-Term Average Bitrate calculates the rates over a specified time period (usually 24 hours). With the average bitrate control, the camera can assign higher bitrates to busier hours while reducing it during idle hours—e.g., midnight to 6 AM outdoors, or 8 PM to 7 AM in an office. In the case of a constant bitrate mode for H.265 encoding, the bitrate varies slightly but stays near the predefined maximum bitrate value. Using H.265+, average bitrate can be as low as half of the maximum bitrate. Image quality can still be optimized since the H.265+ technology makes full use of every bit.

Real-World 24-Hour Testing

A bitrate-reduction test was conducted, based on cameras featuring 1080p resolution at 25 fps. The scene was a small café under video surveillance feed for a 24-hour period.

Instant Bitrate Comparison between Two Scenes

Testing the same scene—a busy café—at different times of day, showed that the rate difference between codecs appears less significant as the number of moving objects in the scene increases. Nevertheless, the numbers are still remarkable. The average bitrate between H.264 and Hikvision’s H.265+ decreased by a substantial 83%. The rate between the standard H.265 and Hikvision’s H.265+ codec decreased by 67%—a smaller difference, but nonetheless significant when applied to real-world surveillance systems.

In discreet, 24-hour file size comparison of two different scenes, drastic reductions were plain to see. Scene one was a café, where the H.264 codec yielded an average of 22.7 GB, and H.265 yielded 11.8 GB, on average. Remarkably, Hikvision’s H.265+ averaged only 3.9 GB. Scene two was a traffic Intersection. Here, the 24-hour file size comparison yielded similar results. H.264 averaged 36.4 GB, H.265 averaged 21.1 GB, and H.265+ averaged the lowest bitrate again at only 7.5 GB.

Here are in those numbers in percentages. In the café monitoring scenario, the rate of the 24-hour file size between H.265 and Hikvision H.265+ decreased by 66.4%, while the rate between H.264 and Hikvision H.265+ decreased by a substantial 82.5%. For the traffic intersection monitoring, the rate of the 24-hour file size between H.265 and Hikvision H.265+ decreased by 64.5%, while the rate between H.264 and Hikvision H.265+ decreased by 79.4%.

Benefits: Improved Bandwidth, Storage, Imaging, & VCAs

First, H.265+ makes the best use of every bit, so HD and ultra-HD resolutions looks as clear, sharp, and focused as possible. Also, as H.265+ improves image transmission, target objects will have more pixels so the use of VCAs will arguably become more precise, more accurate. Next, a network utilizing H.265+ has more bandwidth available at any given time. More bandwidth means better system functioning all around. In real terms, on a 20 Mb broadband network, the H.264 codec can accommodate five cameras. H.265 doubles that, carrying the load of 10 cameras. But H.265+ doubles even that, accommodating 20 or more cameras on the single network. Therefore, H.265+ will be the best choice for users expanding an installation and moving to 4K at the same time.

What’s more, users reduce costs and other resources involved in storing video-feed data. Here’s another scenario: when eight 2-Megapixel cameras are connected to a network, and a storage device holds five 5-Terrabyte hard drives, recording capacities vary significantly. A system running on H.264 will hit its storage ceiling in about two weeks. H.265 will do a bit better, filling up after about one month. Hikvision’s H.265+, however, will continue recording—up to about two full months. When considering these results on a monthly or annual basis for budgeting expenses and hardware allocations, H.265+ reduces expenditures all around. While the jump to H.265+ might be slow initially, the benefits will

prove advantageous far into the future.

Applications are Everywhere

The applications here extend at least as wide as those of any previous codec. However, under conditions like an unstable network or limited bandwidth, or where customers are required to store data for extended periods of time, H.265+ will be most profoundly effective. Furthermore, this codec can be integrated into comprehensive security solutions for specific functions—4K, Panoramic, and explosion-proof cameras, ultra-low light products, and anti-corrosion products are a few examples.

As with any new technological improvement, industry-wide upgrading from current or legacy standards requires investing time and resources. For H.265, migration is accelerating, primarily in newly designed systems since upgrading existing H.264 systems only increases expenditure. H.265 will become more desirable to system integrators and end-users since its decreased bitrates yield high-definition resolutions and images come through more clearly. Added to that, target objects can be isolated and enlarged with more clarity, and more accurate VCAs can be employed.

Summary

Hikvision’s H.265+ codec optimizes the H.265/HEVC encoding technology, meeting its compression standards and operating with the vast majority of hardware and software designed to employ H.265. With H.265+, video quality remains virtually the same as that of H.265/HEVC while radically reducing transmission bandwidth and data storage capacity requirements. The H.265+ codec will serve to widen the application of ultra-HD resolutions in video surveillance, such as 8 MP and 12 MP devices. Wherever applied, this new codec will cut storage costs, make the fullest use of surveillance video investments, and broaden the use of 4K and ultra-HD security video.

Source: Hikvision Digital Technology Co., Ltd.

EU directive for radio equipment results in loss of revenue for alarm manufacturers

Zug, Switzerland

On 16 April 2014, the European Union adopted a new set of rules for placing radio equipment on the European market, and putting them into service: the Radio Equipment Directive (RED). Anything which uses radio for communications will need to meet these new requirements to be placed on the market in the EU. This includes radio-transmitting electronic fire safety and security devices.

EU Member States have had to apply its provisions from 13

June 2016. Manufacturers who were compliant with the existing legislation (R&TTE, LV or EMC Directives) will have until 13 June 2017, to comply with the new requirements. Euralarm has indicated early on that it considers the one-year transition period to be far too short.

Now, the advancement of the standardisation initiated by ETSI, the European Telecommunications Standards Institute, seems to prove Euralarm right. Public enquiries

have been delayed and the publication of the new standards in the EU's Official Journal, signalling their effective entry into force, will most likely take place earliest in April 2017, in certain cases even after June 2017. Alarm manufacturers will not be able to place compliant products on the market for an undetermined period of time until compliance is achieved. Loss of revenue could potentially be up to 50% for some companies resulting in significant losses. Figures

could be in excess of €0.6 billion across the European supply chain.

Market Surveillance authorities shall be made aware of the situation to reassure manufacturers that they will not face legal uncertainty or risk being challenged in the next two years. Euralarm works hand in hand with the European Commission, ETSI and national regulators to minimise negative impact on the industry and monitors the advancement of the standardisation work.

H&M renews global loss prevention contract with Nedap

Groenlo, The Netherlands

Nedap has renewed the global agreement with Hennes & Mauritz (H&M), one of the world's largest fashion retailers, for the supply of intelligent article surveillance systems.

The multi-year contract encompasses the supply and installation of Nedap's !Sense hardware and tags for new stores and refurbishments.

The !Sense solution offers an effective detection performance, enables easy IP-integrations with other devices and direct insights via on board dashboards. The hardware is also fully RFID-ready, which means that a future RFID upgrade is possible with the least complexity and with minimal additional investments.

Rob Schuurman, Managing

Director at Nedap Retail, commented: "We are extremely proud that H&M has renewed the partnership with us. In fact, we have designed !Sense with global retailers like H&M in mind, who need an effective and future-proof loss prevention solution that reinforces their global expansion and future business plans."



Hennes & Mauritz (H&M), one of the world's largest fashion retailers.

Cisco completes acquisition of Appdynamics

San Jose, Ca (USA)

Cisco has completed the acquisition of Appdynamics, a leader in application and business monitoring. Together, Cisco and Appdynamics aim to deliver visibility across the network, data centre, security and applications and drive digital transformation that improves customer experiences.

Together with Appdynamics, Cisco will now be able to offer intelligence, correlation and insights at every level of the infrastructure, security and application. This will enable customers to make more informed IT decisions and improve business results.

"In a digital world, the user ex-

perience, application, and business are converged and inseparable. Appdynamics sits at this intersection monitoring the impact of every line of code on business outcomes," said *David Wadhvani*, current chief executive officer, Appdynamics. "By joining forces with Cisco, we're able to double down on our vision of helping companies overcome the complexity of modern software so they can deliver exceptional customer experiences and drive better business performance."

"We acquired Appdynamics because they are a market leader in a category that will be a cornerstone for how enterprises drive their busi-

ness forward," said *Rowan Trollope*, senior vice president and general manager, Internet of Things (IoT) and Applications, Cisco. "Together, Appdynamics and Cisco will be the only company that can deliver complete visibility spanning from the infrastructure to application to end user."

In its last fiscal period as an independent company, Appdynamics saw year over year revenue growth of over 50%, with approximately 75% of last year's product revenue purely subscription-based*. The company has enjoyed significant success and customer traction, including continued

growth with customer wins with the European Organization for Nuclear Research (CERN), Vodafone, and Wells Fargo.

Appdynamics will continue to be led by David Wadhvani as a new software business unit in Cisco's IoT and Applications business, reporting to senior vice president Rowan Trollope. As part of Cisco, Appdynamics will serve a critical role in helping drive Cisco's continued transformation into a software company. Under the terms of the agreement, Cisco paid approximately \$3.7 billion in cash and assumed equity awards.

JFK upgrades terminal 1 to IP VMS

New York, NY (USA) and Copenhagen, Denmark

Milestone Systems open platform IP video management software (VMS) has been installed at JFK International Airport's Terminal 1 to help manage the safety of more than 27 million passengers a year.

Previously, T1 at JFK relied on a limited analogue surveillance system and an older IP system that were independent of each other. Both were inadequate and lacked some necessary functionality. Operators could only view video from specific workstations, it was difficult to replace or add cameras, and the system did not integrate easily with other systems.

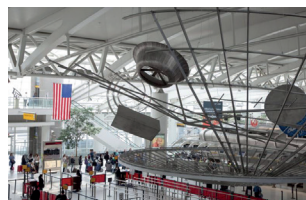
No small feat

Migrating the terminal's old analogue system to an advanced IP video management software platform was no small feat. Due to the airport's high-security environment, the system and all of its cameras had to remain operational

around the clock throughout the migration.

To design and implement the new solution, the airport worked with security integrator Media Wire, LLC, who designed and implemented a Milestone Xprotect Corporate VMS solution to manage its 500 to 600 cameras, including the installation of 160 new network cameras from Axis Communications. Providing greater access to video, the Milestone Mobile client is used by air terminal managers to view video on their smartphones.

"We installed an extensive 10 gig fibre network to support the bandwidth needed for current and future cameras. All cameras provide



The new system is easily scalable and can accommodate additional cameras at any time.

video at the maximum resolutions and frame rates, no corners are cut," said Laszlo Tordai, Owner, Engineer and Technician at Media Wire. "It is simply unacceptable to minimize the system's capabilities and performance because a component is not up to par with the rest of the system. We are keeping this a top-notch installation."

Migrating Terminal 1's system required upgrades to ensure a solid solution from the ground up. New high-speed fibre optics, switches, PoE injectors, software, worksta-

tions and operating systems were installed. Tordai estimates the terminal has close to one Petabyte of storage due to both security requirements, and powerful analytics from Agent Vi that are used on recorded video and to search across camera views.

Combined with Axis cameras

The new system is easily scalable and can accommodate additional cameras at any time. Terminal 1's new Axis cameras easily integrated with the Milestone system and require less bandwidth that better allow the security team to meet the airport's lengthy storage requirements.

"When you look at a whole system and deploy the right parts, you actually save the customer a lot of money," Tordai said. "It's a win-win across the board."

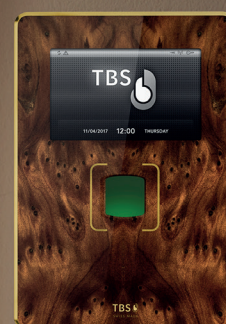


CUSTOMIZED BIOMETRIC SOLUTIONS

Not yet familiar with biometrics or not sure if your team will like it?

We will provide you with a fully operational test device to try out for two months – for free.

Request your free trial now!



tbs-biometrics.com

Antitrust authority sanctions Bosch Sony partnership

Grasbrunn, Germany

After the official approval of the antitrust authorities, the business partnership between **Bosch Security Systems** and **Sony Corporation** in the field of video security solutions became effective from February 1, 2017 – except for in China where the partnership started on April 1, 2017. Both companies will now focus on strengthening the collaboration that was first announced in November 2016.

The partnership entails both a sales and marketing cooperation as well as a technical collaboration. As part of the sales and marketing

partnership, Sony's video security sales and marketing associates has joined a newly formed dedicated team within the Bosch Security System organisation.

Sony's video security customers, in all markets except Japan, will be served and supported by this sales and marketing team.

"We are happy to welcome these experienced colleagues into our organisation and we are convinced we will further grow the business with Sony's products by providing excellent support and service to our customers", says Michael Hirsch, Vice President for

Sales and Marketing of the Sony Security Business within Bosch.

"We are delighted that Sony's video security customers are now being supported by Bosch Security Systems. We are moving forward with this partnership which will feature jointly developed products that fully leverage our industry-leading expertise in video image quality and performance", adds Toru Katsumoto, Deputy President of Imaging Products and Solutions Sector, President of Professional Products Group, Sony Corporation.

Regarding the technical

cooperation, both companies are aiming to set new standards with regard to high resolution video imaging, combined with excellent light sensitivity, complemented by Bosch's expertise in built-in video analytics and latest bitrate management techniques.

The first jointly developed products are expected to be launched in 2018. "We are looking forward to delivering best-in-class video security solutions to our customers for both existing and new market segments", says Gert van Iperen, President of Bosch Security Systems.

Dahua partners to create IoT intelligence team

Hangzhou, China

Dahua has signed a strategic agreement with Dbapp Security Ltd to establish a "Safety Eco-system" in the field of IoT security. Dbapp Security, a leading company, focusing on data security and web application security in China, is a known brand in the information security fields for government and military application plus public security, telecommunications, finance, energy and IoT.

Dbapp Security are specialists in offering network information security services to major events, such as three consecutive sessions of the World Internet Conference, as well

as the G20 Summit in Hangzhou.

Dahua prioritises R&D investment to focus on the development of safer products, especially in the territory of information security. Dahua initiated this in depth cooperation with Dbapp Security regarding security situation awareness, cyber safety assessment and IoT security personnel training, so that Dahua could deliver products, solutions and services with a high standard in cyber security.

In this era of IoT, where new IoT business and technologies quickly develop, the need for information security is escalating.

Dahua and Dbapp Security

will put together an IoT Network Security Threat Intelligence Team, to look into the collection, analysis, utilisation and research of IoT data. A virtual IoT security lab will be jointly established to research and discuss the technical development, threat development and system architecture of IoT security. The lab will also be utilised to share the updates and research results on IoT security, build IoT information security related products,



Fu Liqian (center right), Chairman and CEO of Zhejiang Dahua Technology Co., Ltd., and Fan Yuan (center left), Chairman and CEO of DBAPP Security Ltd. participated at the contract-signing ceremony

and jointly promote broader and deeper applications of IoT security products and solutions.

Flir wins 54 million dollar order for US Defense

Wilsonville, Or (USA)

Flir Systems, Inc. has received a delivery order for 50 U.S. Army Chemical, Biological, Radiological, and Nuclear Dismounted Reconnaissance Sets, Kits, and Outfits (CBRN DR-SKO) systems.

The delivery order is under a five-year indefinite delivery, indefinite quantity (IDIQ) contract from the U.S. Department of Defense, in support of the Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD)

DR-SKO Program of Record. The order is valued at \$54.2 million, with deliveries extending through the second quarter of 2018.

The CBRN DR-SKO system is a set of mission specific kits that characterise and provide full spectrum CBRN dismantled reconnaissance capability utilised by the U.S. Military Joint Services, including units within the Army, Navy, Air Force, Marines, and National Guard Weapons of

Mass Destruction-Civil Support Teams. The programme has been in development since 2008 with Flir Systems, Inc. as the prime contractor.

"We are honoured to continue providing our turnkey DR-SKO solution that addresses the current and emerging threats by equipping U.S. soldiers with the best-in-class technology for their mission," said Andy Teich, President and CEO of Flir. "This

delivery solidifies our continued support to provide innovative, mission-critical solutions to keep our country safe and maintain our stance as a leader in the CBRN market."

Since the CBRN DR-SKO IDIQ was awarded in December 2014, over 100 systems have been delivered to the U.S. Department of Defense, with production being performed out of Flir's facility in Elkridge, Md.(USA).

Alarm.com acquires Objectvideo

Tysons, Va (USA)

Alarm.com an USA-based leading platform for the connected home and business, is acquiring substantially all of Objectvideo, Inc.'s business, including the company's products, technology portfolio and personnel.

Objectvideo is a pioneer in the fields of video analytics and computer vision, with technology that extracts meaning and intelligence from video streams in real-time to enable object tracking, pattern recognition and activity identification. The business, now called Objectvideo Labs, will accelerate Alarm.com's research and development of video services and video analytics applications, and will continue

to provide advanced research and engineering services for federal government customers.

Founded in 1998 by scientists and programme managers from the Defense Advanced Research Projects Agency (DARPA), Objectvideo was a privately held, venture-backed leader in the rapidly growing field of computer vision. With a history of supporting the complex mission requirements of the U.S. Defense and Intelligence communities, the team averages more than 15 years of experience and includes a mix of computer vision scientists and video software engineers that have expertise in machine learning, 3D modelling, and complex activ-

ity recognition.

"Objectvideo Labs brings deep expertise in the field of video analytics, and we're excited to welcome them to the Alarm.com team," said Jeff Bedell, Alarm.com's Chief Strategy and Innovation Officer. "As video applications grow rapidly in both the residential and commercial spaces, this acquisition will reinforce our ability to continue to lead in the development of proactive, next generation connected home and business solutions. Unlike standalone devices and point products, the Alarm.com platform can extract meaning from a broad ecosystem of connected devices to deliver enhanced security and a

highly-valued user experience."

"I am excited for the opportunities ahead for the Objectvideo Labs research and engineering team," said Raul Fernandez, President of Objectvideo Inc. "Incorporating their pioneering work into the sophistication and scale of the Alarm.com platform will yield exciting opportunities for innovative new features and applications, and can drive Alarm.com into a leadership position in the emerging fields of video analytics and computer vision."



Raul Fernandez,
President of
Objectvideo Inc.



Business & Product News – Every Day!

www.securityworldhotel.com



FORTEZA JSC - manufacturer and developer of the modern and high-performance outdoor perimeter security systems

MICROWAVE BISTATIC SENSORS FORTEZA FMC

-  Operating Frequency 10.525 GHz or 24.15GHz
-  Set up using PC or Android device
-  High resistance to interference
-  Independent 4 channels
-  Warranty 2 years



FENCE PROTECTION SYSTEM FORTEZA TRIBO-M

-  Set up using PC
-  High resistance to interference
-  Four wings - 300 meters each
-  Network addresses
-  Warranty 2 years

Easy to install
Comfortable to use

www.forteza.com
www.forteza.eu






The entire system can be centrally managed, monitored and maintained, as well as ensuring maximum security for all bank branches.

Vanderbilt secures Italian bank

Parsippany, NJ (USA) and Cesena, Italy

Vanderbilt technology is currently being installed across Italy's Credito Cooperativo (BCC) consortium of banks. Work has already started on Banca di Cesena e Banca di Gatteo di Credito Cooperativo S.Coop, which is benefitting from the specification of Vanderbilt's SPC5000 and SPC6000 control panels, which provide integration of intrusion and access functionality.

BCCs are found throughout the length and breadth of Italy and have served local communities for the past 134 years. There are 317 mutual not-for-profit organisations comprising over 4,300 branches, all of which work together to guarantee a range of products in keeping with the values and identity of a cooperative. BCCs offer all of the banking services normally offered by other financial institutions and look to improve moral, cultural and economic conditions, promote collaboration and teach the benefits of saving and forward planning.

Headquartered in Cesena, Banca di Cesena e Banca di Gatteo Credito Cooperativo S.Coop is the first member of the BCC to initiate a new security infrastructure, which is being implemented by Gatteo based Smart Security.

Hybrid intrusion system

Vanderbilt's SPC is a true hybrid intrusion detection system that meets EN 50131 standards and has unmatched flexibility and scalability. SPC5000 and SPC6000 control panels are being installed at each branch, with the former able to be expanded according to specific customers and project needs with up to 128 zones, 128 outputs, 16 system keypads, 16 doors and eight verification zones. SPC6000 expands upon this functionality

with up to 512 zones, 512 outputs, 32 system keypads, 64 doors and 16 verification zones.

Cloud-based solution

The control panels are being fully integrated with Vanderbilt's pioneering SPC Connect system – a cloud-based solution that allows Smart Security to monitor, manage and control the SPC control panels remotely from any location. By logging in installers can gain access through an internet connected laptop or desktop PC, as well as mobile devices. SPC Connect offers the ability to customise how data is viewed by setting up a feature that allows Smart Security to manage and control access rights to individual panels and groups of panels. This means that tasks such as configuration management, troubleshooting and regular maintenance can be carried out remotely, saving massive amounts of time and money, and also enabling a swift resolution to any issues.

"The high-end operability we provide means that the entire system can be centrally managed, monitored and maintained by Smart Security. As well as ensuring maximum security for all bank branches, this approach is incredibly cost effective", comments Valerio Vittone, Vanderbilt's Country Head for Italy.

Securing care homes in the 21st century

London, UK

Smartair battery-powered wireless locks offer modern, easy, cost-effective installation, alongside features designed to put care home managers in more control of their premises, and are already deployed in residential care settings across Europe.

To assist in the care of over 500 residents, Pamplona's Casa de la Misericordia demanded a new access system that offered real-time control over the premises. The choice was Smartair Wireless Online.

Care homes present many unique security challenges. Above all, a residence needs to feel like an open, welcoming space. It must work for the resident, and provide a pleasant environment to greet family and other visitors. It should be a home, in every sense.

At the same time, managers must ensure security of the site, including its staff, sensitive data, and areas where medicines are kept. If there has been an unauthorised access attempt, staff need to know as soon as possible. When residents have dementia or other complex conditions, it is crucial that care workers can find out where they are at any time.

Easy to operate

Advanced access control – that is easy for everyone to operate – can have major benefits in a care home. A system that can feed back to site managers in real time, for example, can directly impact quality of care, enabling staff to quickly locate residents, to respond to incidents or problems as soon as they arise, and to organise staff workflows more efficiently, resulting in less staff time wasted handling keys.



Advanced access control – that is easy for everyone to operate – can have major benefits in a care home.

"In a residence like ours it is critical to have real-time management that allows us to interact with a door at any time," explains Ernesto Serra, Facility Manager at Casa de la Misericordia.

Wireless solution

The system had to be expandable, so it could be installed in two phases, starting with a new-build before moving on to a 1930s building. Advanced wireless technology suited to retrofitting an old building was a must-have: the older building has walls up to one meter thick.

"A wireless solution that allows us to install access control without wiring up the buildings is a big advantage," adds Ernesto Serra.

Tailor made access privileges

The new system needed to be scalable, so staff could manage access to the two buildings from the same control point, amend access rights instantly, and tailor access privileges to the diverse profiles of staff, residents, volunteers, visitors and emergency workers. The two-stage project is now complete, and includes 650 additional Smartair-enabled doors in the old building.



Security News Every Day!

www.securityworldhotel.com

Less cameras are more in Cologne

Regensburg, Germany



The events of New Year's Eve 2015 in Cologne are seared into the memories of the entire population of the city.

The events of New Year's Eve 2015 in Cologne are seared into the memories of the entire population of the city. In the wake of countless incidents, including numerous cases of sexual harassment of women, police recognised the need to revise their existing security concept, particularly with regard to securing large public spaces.

A high number of criminal offences had been committed around Cologne Cathedral, and therefore this area in the inner city was selected as the basis for planning new security measures.

A logical way to successfully guarantee full coverage of large open spaces with visibility challenges is with as many cameras as possible. However it would still be very costly and it would still be hard to technically create satisfactory solutions.

"This was why in the past at least 30-40 percent of such projects were not even attempted", says Dieter Dallmeier, founder and CEO of Dallmeier, the manufacturer that has developed the multifocal sensor system Panomera.

Designed for large areas

Panomera is specially designed for the all-encompassing video surveillance of expansive areas. It manages huge widths, and areas with large distances can be displayed with a completely new resolution quality, in real time and at high frame rates of up to 30 fps. A huge area can be surveyed from a single location, and depending on the requirements of observation assignments, the resolution can be scaled nearly limitlessly. Hence, one Panomera, equipped with eight sensors, according to Dallmeier, is fully sufficient to replace 35 standard megapixel cameras.

8,800 square metres

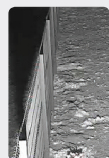
In spring 2016, the first concepts were presented to the city administration. Their main focus was on how the situational overview for police and therefore the delegation of police and other emergency personnel could be improved through

the use of video systems, especially in case of large gatherings. Even in those early stages of planning, the responsible officials encountered a massive problem: with the use of conventional video technology it would not have been possible to fully capture the required 8,800 square metres of monitoring area.

Cost effective

However, the project was awarded to the Regensburg-based manufacturer, and installation work for the Panomera system began in mid-December 2016. Instead of a system with numerous spread out cameras, Dallmeier deployed a system that discreetly covers the entire monitoring area. The Panomera solution required only two installation points. Hence, setting up the system was easy and the city will benefit significantly financially from much lower infrastructure and maintenance costs compared to the original planning.

Complete Clarity with **Clarius® PLUS** LED Illuminators



Next generation Dual Core LEDs for powerful illumination, long life and low running costs

Interchangeable lens diffusers deliver angles from 10° to 120°

Infra-Red and White-Light LED options

Enhanced optics provide ultra clear images

Lighting design service now available



AWARD WINNING
BRITISH MANUFACTURER

Unit 2, Birch Business Park, Whittle Lane, Heywood, Greater Manchester, OL10 2SX, UK
gjd.co.uk | info@gjd.co.uk | +44 (0) 1706 363 998

Pioneering UK police forces deploy body worn video

Whitley Bay, Tyne & Wear (UK)

Two police forces are pioneering the introduction of body-worn video (BWV) technology in the UK, following certification to the Surveillance Camera Code of Practice, completed by SSAIB auditors.

The Greater Manchester Police and Metropolitan Police Service are now using body worn camera devices for a variety of innovative and beneficial applications.

BWV technology is now being used in a variety of ways to capture police operational activity first hand, using helmet or vest-mounted cameras. These affordable cameras provide high-quality images and audio, which can be used for evidential purposes. Andy Marsh, who was the National Policing Lead for body-worn video (and is now Chief Constable of Avon and Somerset police), reported in 2014 that this technology's advantages include enhanced contemporaneous evidence capture and swifter justice through early guilty pleas and admissions.

"It can also inform more appropriate sentencing and help to reduce bureaucracy throughout the criminal justice processes by focusing on the needs of victims. Finally, it supports transparency, trust and confidence in the police," he added.

Greater Manchester Police

The Greater Manchester Police experience began with a trial of 80 BWV cameras among response teams in the north and south of Manchester between 2012-13. An initial 12-week pilot led to a roll-out of BWV cameras from March 2016 to all operational front-line police officers and specialist units.

Approximately 3200 units will eventually be deployed, with further plans for the scheme to additionally include police

community support officers in 2017. Operational use of the body-worn devices takes account of guidance published by Greater Manchester's Police & Crime Commissioner, following a report by the Independent Police Ethics Committee. It concluded that the technology could help improve the criminal justice process for victims of domestic abuse, by gathering crucial evidence to make it quicker and easier to obtain a conviction, and relieving the pressure on victims who don't feel able to attend court.

Metropolitan Police Service

Meanwhile, following an initial year-long pilot project involving the distribution of around 500 cameras among emergency response teams spread across 10 London Boroughs, the Metropolitan Police Service is now rolling out BWV technology across the capital. This three-phase programme entails the deployment of approximately 22,000 camera units, which is due for completion by mid-2017.

The force's initial pilot scheme was studied by the College of Policing and the Mayor's Office for Policing and Crime. Their reported findings included potential benefits from BWV including a reduced number of allegations against officers, particularly of oppressive behaviour. Complaints related to interactions with the public also reduced.



"It supports transparency, trust and confidence in the police," commented Andy Marsh, Chief Constable of Avon and Somerset Police.

Enjoyable experience

Commenting on the Metropolitan Police's accreditation to the Surveillance Camera Code of Practice, the force's Policy Lead, Digital Policing, Sam Harvey noted: "Achieving full certification has been a vital aspect of our assurance to the public that body-worn video is being used effectively in the Metropolitan Police Service (MPS). The Surveillance Camera Commissioner's comprehensive guiding principles have been invaluable for our BWV policy and rollout of the world's largest deployment of BWV. Independent accreditation for compliance has been a rewarding and enjoyable experience, both during document audits and on-site visits at key police stations in London. We anticipate that the MPS will continue to use the SCC framework in annual reviews and will work closely with the SCC in continuing to recognise the implications of BWV and maintaining this lead in best practice."

Significant assurance

Meantime, Mark Chaderton, Sys-

tem Support Manager at Greater Manchester Police declared: "Delivery of the certification process was easily understood and applied into all aspects of our BWV project across technical specifications, system administration and data sharing. Award of the Surveillance Camera Commissioner's certificate is a significant assurance to criminal justice partners, individuals and the wider community that our use of BWV is legitimate, effective and compliant. We are delighted to have achieved full certification and look forward to continuing to work within the Commissioner's 12 guiding principles as GMP's use of BWV develops."

"Good practice"

SSAIB provides a third party certification service to the Surveillance Camera Commissioner that enables local authorities and those operating public space camera surveillance systems to demonstrate their conformance with the Code of Practice, which the Commissioner calls a "universally accepted example of good practice".



**Business & Product News
– Every Day!**

www.securityworldhotel.com

Martin Gren believes in IP audio and IP intercoms

Axis co-founder Martin Gren is satisfied with the decision that Axis has taken over Canon's sales of IP cameras. Meanwhile, he continues to look towards new product areas.

"I believe that IP audio and IP intercoms are situated where IP cameras were 20 years ago", he says.

By Henrik Söderlund

In 2015, Martin Gren was one of the Axis' major shareholders who sold their shares to Canon. He has described the decision as very sad but rational. Canon promised that the brand, business model and development centre would remain and they have kept the promise.

In September last year, it was announced that Axis would take over marketing and sales of Canon's video surveillance products in EMEA and North America.

"It was quite confusing that both Canon and Axis were exhibiting at security shows and trying to sell products next to each other. So, I am very pleased that we have finally come to an agreement on how to deal with it", Martin Gren says.

You already have a full range of products; do you really need Canon's products?

"They have some products that we do not have, but there are also many products that are very similar."

How is your life today, do you work as much with Axis as before?

"Yes, I would say that there is very little change except that I travel and give speeches more often than before. But I continue to work with new products that are not IP cameras, for example both the intercom and the speakers that we have launched. I think IP audio and IP intercoms are in the same position as IP cameras were 20 years ago."

Talking about IP intercoms, why did you acquire the Czech IP intercom manufacturer 2N?

"2N was the first company

that released a video door phone that was based on IP and today they have a complete portfolio of IP-based intercoms. They are the world leader in this field. The company has more than 200 employees and worldwide sales presence, but of course, only a fraction of sales people compared to us. We hope to leverage our sales channel and learn from each other's technologies."

You have always emphasised the transition from analogue cameras to IP cameras. Today, the growth rate for HD analogue is higher than for IP cameras in some markets. What is your view on that?

"I think it applies primarily to small, very independent systems, which basically is not Axis' market. Analogue HD has clearly taken over much of the old analogue market. IP has always been relatively weak in the small independent stores segment."

Do you see any new trends in the market?

"I think the major trend is that integrated solutions are increasing. This has been the trend for quite a few years now, and it has become more and more obvious."

What about technology trends?

"Right now smart compression is the main trend. Then there are a few on-going trends: picture quality is becoming better and better, as well as light sensitivity. Also, the development of sensors is progressing really fast."

What will IP cameras look like in the future?

"If you believe in Moore's



Axis co-founder Martin Gren is satisfied with the decision that Axis has taken over Canon's sales of IP cameras.

law, it is possible to predict what will happen with resolution and image quality. Video analytics is a trend that has been around for a long time but has not yet become very big except for in some retail applications. For security applications, thermal cameras should still be used for high reliability. We have taken a partner approach there and have been very happy with it, but now we take one step further after acquiring the video analytics manufacturer Cognimatix. We still believe that you have to choose the right type of video analytics."

What is the right type?

"The trick is to start looking at the market need, and not choose those applications where there must be 100 per cent accuracy. Public transportation companies dream about being able to detect people laying on the tracks. For

room for error."

Chinese companies, especially Hikvision, are growing very quickly and offer IP cameras with low price. How do you compete with them?

"In essence, we have similar manufacturing costs as the Chinese. What differs is the cost of the service, support, training and quality."

Is Hikvision starting to enter markets where you have been dominating?

"There is no doubt that Hikvision is becoming one of our biggest competitors. I obviously think Axis products are much better with a higher quality. Hikvision has very small, very low cost solutions. And if you only look at price, they are an option."

Will you become more service-oriented in the future?

The trick is to start looking at the market need, and not choose those applications where there must be 100 per cent accuracy.

most people, it sounds trivial to tell the difference between a human and a train, but when conducting image processing, you realise that there are huge demands on reliability. In retail, it is not crucial whether the video analytics says that there are seven or eight people standing in a queue, but that there is a long queue that must be addressed. In security applications there is no

"It is something that we are looking into and we have taken a few steps towards that direction. But we can not talk about it yet."

Is this a strategy in order to tackle the threat of low price products from China?

"Well, I would rather focus on what the customers want and we know that they want services and therefore, we need to be able to deliver them."

Marc Handels, co-founder of Salto

“Mobile access and cloud access have crossed the line from buzzwords to reality”

Mobile access, cloud based solutions and more doors with access control are the main trends in the access control market according to Salto Systems co-founder Marc Handels.

“In the next ten years I think electronic locks will penetrate virtually every type of building”, he says.

By Henrik Söderlund

Founded in an apartment in the northern part of Spain in 2000, Salto Systems has now grown organically to become a 115 million Euro company with 29 offices around the world. Today only 5 per cent of the business is domestic.

Marc Handels, co-founder and Vice President Marketing and Sales, stresses that the company’s biggest markets are very much linked to the sizes of the markets.

“Before that was not a key driver, but now when electronic locks are all over the place, you see that the size of the market is basically driving how important it is for us”, he says.

What is the biggest trend in the access control market?

“I think mobile access and cloud access are two tendencies, which have crossed the line from buzzwords to reality, and they are here to stay. Professional end users like retail often do not have the capacity to dedicate IT resources to keep access control updated in local shops, and to keep the servers and the networks secure. Management of the access rights is perhaps not down on the local level but probably somewhere else, and here cloud really makes sense. And of course, to put access control on all doors, not only the exterior doors.”

What about access control as a service?

“We have actually just launched a product called Salto KS Keys as a Service. We see a great potential here – at the moment mostly for small and medium sized enterprises. It will take longer until the

cloud becomes standard for larger projects, like governmental projects, large university projects and large hospitals. Those are end users that have the capacity to make sure their systems are secure and well protected, and updated, all the time. They do not have an absolute need to have access control in the cloud and therefore, we need to provide other network solutions.”

What is your view on biometrics like fingerprints and eye scanners?

“In Asia this is bigger, partially because there are less privacy concerns there than in other markets. This is a technology that will not go away. We have to be able to provide such a solution and integrate these products into our systems, but for the moment we are not making them ourselves. We focus on electronic locks.”

What is your view on smart buildings and access control?

“We believe very much in it and we are working on solutions there. We think that the door – or an access point, which probably is a better word – actually is at the centre in smart buildings, smart cities, smart home – smart everything. We believe in giving access to buildings in a clever way to keep them as open as possible, so users going into these buildings have the feeling they can move wherever they want to, but still in a controlled way.”

And the Internet of Things?

“It is intimately connected to smart buildings. IOT is happening as we speak, but obviously there is



Mobile access, cloud based solutions and more doors with access control are the main trends in the access control market according to Salto Systems co-founder Marc Handels.

a big challenge and that is security. We believe that the success of IOT comes from a trust that consumers and end users have that manufacturers are really taking care of them. Most end users can not know if the products are safe, they can not test them themselves. Here, the manufacturers have an enormous responsibility to keep their IOT systems and cloud systems secure.”

control or a mechanical solution.”

How secure are cloud solutions?

“There are not many companies selling these products today. We have taken many precautions and only keep necessary elements in the cloud.

We call that distributed security. Even in the extremely unlikely case of a hack of our cloud, nobody would be able to open let us say

” Our systems are well designed, well protected and well encrypted.

How do you handle security?

“We take this very seriously and sometimes we are more cautious than our sales team would like us to be, as it leads to longer development times. IOT is a fantastic opportunity, especially for the locking world, to drive business and to interact with customers.”

What is the risk for an access control system getting hacked?

“Our systems are well designed, well protected and well encrypted. However at the end of the day, access control security also depends on how secure your own network is, something that we do not have control over. However, the most common way to break in is still through a physical door or a window, no matter if it has access

1,000 doors, because the authorisation of opening the door is partly locally activated. The more popular cloud access becomes, the more questions will be asked about security, which is good and why it is important to be one step ahead.”

What is your biggest challenge for the future?

“In the next ten years I think electronic locks will penetrate virtually every type of building. It does not matter whether it is a commercial building, a residential building or a healthcare building, everyone will look at electronic locks. The growth of the market is almost guaranteed. The challenge for us is to make people think of Salto first, and to take an important share of the growth of the market.”

Siemens Head of Fire, Mario Kahlert, on the future of the fire detection market:

"IP cameras will not replace fire detectors"

The fire detection market has traditionally been slower in adopting new technologies such as IP and the cloud. Detektor met up with Siemens Head of Fire, Mario Kahlert to find out more about where this market is heading.

"Not everything that is technically possible makes sense in a business where life safety is crucial", he says.

By Henrik Söderlund

While products for video surveillance and access control have been extensively developed and have moved through a technology shift from analogue to IP during the last 10-15 years, products for fire detection are lagging behind. Mario Kahlert, Head of Fire Safety, stresses that the market for fire detection is growing and that the trend is steady. The growth rate is about 3 per cent and is closely linked to the construction market. In Europe there is not so much new construction as for example in China and the Middle East where the market is growing faster.

Digitalisation still unsettled

There is much talk about digitalisation within the industry and according to Mario Kahlert, the industry is still trying to figure out the best way to approach it. He believes it is very important to keep the balance between what is technically possible and what is allowed according to industry regulations. He considers digitalisation and how products can be installed and serviced easier as the main trend in the fire detection market.

"I think that the general trend of connection and digitalisation is here to stay. A major issue is how we bring digitalisation without risking anything in the life safety area. But the general trend of digitalisation is something we want to pick up and really drive forwards, either with remote connectivity, with service ability and also with BIM (Building Information Model) for our products", he says.

Mario Kahlert stresses that cloud solutions support a business model that makes the customers

more productive and efficient. But there is always an issue about how much data the customer wants to share and that data has to be used for the right purposes.

"Nobody wants to die because someone hacked into a system and shut it down. I think there is a thin line here; we have to make progress in this area, but also make sure that we are not endangering what the industry stands for. It is all about life safety", he says.

Integration with other systems

Another main issue is how fire detection systems can be integrated in other security systems.

"In the end, as an operator or as an end user, you want to combine different functionalities. Our solution brings fire together with HVAC (Heating, ventilation and air conditioning) and other functions into a management station. It is an open platform that we want to develop further", Mario Kahlert says.

An interesting question for the future is how solutions for fire detection and fire safety – with all its regulations – can be part of the 24/7 connected Internet of Things society. Mario Kahlert has a twofold perspective on this: on the one side, IoT is a general trend that cannot be stopped and players need to find out how to participate and how to develop and shape their portfolios and offerings over time to fulfil market needs.

"It can be via remote access, visualisation and remote information and we are already offering this to our customers. And there is more to come. However, not everything



Detektor met up with Siemens Head of Fire, Mario Kahlert to find out more about where this market is heading.

that is technically possible makes sense in a business where life safety is crucial. You do not want to fail with detecting or alarming because the server was down or because the device just did not connect. This will never be accepted, you have to be careful", he says.

ogy (Aspirating Smoke Detector) will grow in importance.

"We are constantly looking for what other technologies there are on the market and evaluating what will work on a mass market where the customer gets a very good product for a reasonable price."

"Nobody wants to die because someone hacked into a system and shut it down."

New fire technologies

IHS recently claimed multi-criteria detectors, which combine multiple detection technologies, have become more common in the fire detector market and that the market is expected to grow by a compound annual growth rate (CAGR) of 6.6 per cent between 2015 and 2020. During the last couple of years, new solutions of how to detect fire have been launched on the market. One example is cameras with video based fire detection combined with intelligent video analysis for early flame and smoke detection. However, Mario Kahlert thinks that the basic principle of today's detectors will remain and that ASD technol-

He does not think that cameras will replace fire detectors even though more functions can be added to detectors in the future.

"They are two different systems. The detector must live up to a standard while the camera does not. That is also why I see a limited value in the camera replacing the detector. The interesting thing here is to integrate them: the detector can send an alarm to the management system and then the operator can have a look at the camera and see if there is a fire."

Privacy is another issue, most people will not accept having a camera in their hotel room, but a fire detector is perfectly fine.

Video analytics review

Where is the market for video analytics heading and will deep learning and AI break through? Detektor has talked to some industry specialists

about market demand, technical trends and future applications. They all seem to have a strong belief in the future of video analytics.



Willem Ryan, Senior Director of Global Marketing at Avigilon.



Milestone System's Regional Sales Manager Nordics, Lars Wilson



Anders Karlsson, Product Marketing Manager for Bosch in Northern Europe

The market – recovering and ready for analytics 2.0?

Video analytics has been growing consistently although not developing as fast as expected and has faced challenges such as causing too many false alarms.

Now, deep learning and applications for business intelligence are expected to increase growth.

By Henrik Söderlund

The market analysis company IHS Markit thinks that 2017 will be a step up for video analytics. Previously, the market has suffered from high expectations that have not been met, but now IHS expects that market confidence will be boosted by a new generation of video analytics, which will be powered by deep learning, big data analysis and high performance computing.

Lower costs

Avigilon is one of the companies to claim that the video analytics industry has reached a tipping point.

Willem Ryan, Senior Director of Global Marketing at Avigilon.

He also stresses that the costs for video analytics have been driven down and its performance has increased tremendously.

Milestone System's Regional Sales Manager for the Nordic markets, Lars Wilson, also thinks that the market for video analytics will grow.

"Definitely, when I started working for Milestone nine years ago we had 50-60 video analytics partners. Today we have 800-900 and that is a clear indication of a growing market."

He thinks that the algorithms

transportation, and what kind of problems they can solve. I think we will see a lot more of this and there will be more vertical specialists in the market, who will know a lot about the challenges within their area of expertise", he says.

Lars Wilson believes that retail and transportation are the most interesting verticals for video analytics. Willem Ryan stresses that all verticals will grow and there are analytics in a lot of applications today: retail, hospitals, transportation, airports, ports, critical infrastructure, health care, education and more.

Analytics were too demanding

Anders Karlsson, Product Marketing Manager for Bosch in Northern Europe, says that the biggest challenge for the industry is to restore trust among end users and show that today's security cameras are good enough to conduct video analytics.

"The kind of video analytics that was used a few years ago demanded hands-on, continuous updating and adjusting in order to make it work. Those who did not

have the time or expertise to do that thought that video analytics were not good enough", Anders Karlsson says.

Both installers, monitoring centres and end customers had bad experiences. Some of them decided to only use video analytics together with thermal cameras.

"To be honest, it is perhaps only since the beginning of 2016, that the industry has reached a level where the detection is reliable both for indoor and outdoor video analytics. And now, we are facing the challenge to prove that surveillance cameras are good enough."

More analytics at the edge

In the dawn of video analysis, server based analytics was the preferred way of conducting the analysis. However, during the last couple of years, camera-based video analytics at the edge has increased. According to IHS, the market for server-based analytics decreased by 39.4 million dollars in 2014, but analytics as a whole still grew because of a strong growth in analytics at the edge. However, the demand for

"We think we are at a defining moment in the industry where artificial intelligence and deep learning has radically started to change our ability to apply video analytics into video surveillance."

"We think we are at a defining moment in the industry where artificial intelligence and deep learning has radically started to change our ability to apply video analytics into video surveillance", says

are more mature today and that the market for video analytics will become more vertical.

"For example, a lot of customers look at the benefits video analytics bring to retail, or to

high-end server based analytics is expected to remain.

Lars Wilson thinks that video analytics at the edge will grow faster than server-based analytics.

"It is cheaper to do the analysis in the cameras and you might not add analytics to all your cameras. We support both solutions,

but we can see it is has taken off stronger at the edge", he says.

Providing business intelligence

Video analytics applications can basically be split into three categories: detecting someone or something while it is happening, for example,

search for information after an incident has taken place and finally using video analytics in order to generate business intelligence data.

Lars Wilson believes that video analytics for business intelligence will grow faster with applications like people counting and conversion rates and Anders Karlsson agrees:

"Business intelligence applications will probably grow faster and become bigger than the other two, perhaps not this year or next year, but soon. However, the other two will grow too, because the technology will become cheaper and personnel guarding more expensive."

– Will deep learning bring a revolution?

By Henrik Söderlund

Deep learning and artificial intelligence are the new buzzwords within video analytics.

"A lot of challenges that seemed unsolvable are being unlocked because of artificial intelligence and using deep learning with GPU processing", says Avigilon's Senior Director of Global Marketing, Willem Ryan.

The market analysis company IHS Markit has listed deep learning as one of the major video surveillance trends in 2017. IHS describes deep learning as the fastest-growing field in artificial intelligence. Deep learning is a training process where machines can improve the accuracy of pattern analysis or classification automatically over time by receiving massive amounts of data. The technology learns what the typical activity is in a scene and alerts the operator when non-typical activities occur.

A critical mass

Avigilon is one of many video surveillance manufacturers that has great belief in deep learning and recently showcased its deep learning video analytics at ISC West in Las Vegas. Willem Ryan, Senior Director of Global Marketing at Avigilon, claims that the industry has reached a critical point, or a critical mass.

"We continue to grow the industry providing solutions that enhance performance, better surveillance, more storage, more cameras, high resolution, and this has created an imbalance between the desire and need for more video information and the lack of human attention to actually focus and view that data that are continuously collected and stored in our system", he says.

The emergence of GPUs (graphics processing units), which provide the deep learning infrastructure to cameras and recorders,

has made deep learning possible.

Willem Ryan claims that the analytics becomes part of the system without the user having to set up or calibrate it. He says: "GPUs allow us to create even more powerful analytics that are changing the way that we interact with the video surveillance system. Some of the new advancements that are now being leveraged through GPU capabilities and artificial intelligence, are bringing a new wave of analytics to the industry."

Believes in combined analytics

Milestone System's Regional Sales Manager for the Nordic markets, Lars Wilson, also believes deep learning and artificial intelligence will improve video analytics, at least when the technology becomes a bit more mature.

He says: "Self learning and artificial intelligence are misused concepts, but I believe in these kinds of solutions. You want to achieve reliable results and that the system does not only react on the information that you are interested in."

Lars Wilson believes that video analytic systems will develop greater reliability and become more intelligent. He also thinks that analytics will be combined to a greater extent than it is today.

"If you look at video analytics in retail, you should combine heat mapping – which gives you movement patterns of how customers move in a store under a certain

time frame – with for example people counting."

More cloud services

Anders Karlsson, Product Marketing Manager for Bosch in Northern Europe, sees two main trends within video analytics: deep learning and more additional services in the cloud.

"Deep learning is perhaps not a big trend yet. But the systems will become more self-learning and a lot of manufacturers are working on this right now. The second trend is to split the analysis: let the cameras and products generate metadata, and then supplemental analysis is conducted

Processors must be better

Willem Ryan believes deep learning will provide a more efficient user experience and allow the user to search for critical information even in live video, while video analytics runs in the background.

He says: "We are going to get more advanced object recognition and detection so you will be able to detect people in crowded areas and detect faces really well. You will also be able to detect vehicles and distinguish between different types of vehicles."

Anders Karlsson says face recognition in real time is still quite hard because it requires very big databases. He also stresses that

"Deep learning is perhaps not a big trend yet. But the systems will become more self-learning and a lot of manufacturers are working on this right now."

via cloud services rather than through a standardised server", he says.

Anders Karlsson is not sure whether deep learning will revolutionise the physical security industry, but he is convinced it will provide a lot of additional services in the future.

"Deep learning does not have any limits. Things that users need to tell the system 10-12 times – this is right, this is right, this is wrong – before the system understands, will not be needed in the future because it will be self-learning", he says.

most facial recognition is done afterwards.

Except for generating too many false alarms, video analytics requires quite a lot of processing power. Anders Karlsson believes it is one of the biggest challenges for video analytics.

He says: "The better processors, the more we can do. It also means that you can increase the resolution of the analysis algorithm, how many pixels it can use. And then, you can perform a lot better and do a lot more video analysis since there is more information."



Attendees packed the hall when ISC West Expo opened with the Grand Opening ceremony.

Report from ISC West

Electronic perimeter security under the spotlight in Vegas

ISC West was held from the 5th to the 7th of April. It was a great manifestation of how technology can make a difference to help companies and other organisations to fight crimes and other unwanted events through technology that either prevents those crimes or alerts operators before the crime or the fire even starts.

By Lennart Alexandrie

Proactivity is for sure a buzzword, not least as a consequence of the increasing use of video analytics, which was also a key focus at the show.

Radar technology was a hot topic

Perimeter protection solutions, based on electronics, have become increasingly interesting for the security market. This trend was obvious at this year's ISC West in Las Vegas.

Thermal cameras were on display on many stands. More surprisingly was that several exhibitors promoted radar surveillance techniques and that Axis was one of them.

Bandwidth effective video surveillance

In the video surveillance field there were many exhibitors placing emphasis on solutions for lower bandwidth use and effective storage of images. Multi-sensor IP cameras,

new VMS software and additional features for existing VMS platforms were also launched during the show.

Biometrics on the rise

In the access control field there were several exhibitors showing their solutions with bluetooth and NFC technology. Biometrics was also a major element, especially solutions for fingerprinting and not least face recognition.

Cyber security

Another key issue highlighted at the show was cyber security, a concern the security industry has recently woken up to in the light of the ongoing Internet of Things process which is being embraced by security technology providers from all over the world. But how to ensure that the security product does not become a component

that is used by hackers for network attacks? Cyber security was also the theme of the conference on day 2.

Protection against terrorist attacks

The threat of terrorist attacks was of course also something that was discussed at the show, not least on the very last day of the show because of the terrible events in central Stockholm – news that was also somewhat overshadowed by the USA's airstrike on Syria.

Gave a trend insight

Overall the exhibition was well attended and the standard of the exhibitors was equally good, with a mix of small, medium-sized and large companies. And it certainly gave an insight into what we can expect from the remainder of 2017 – both in terms of trends and products.

ISC West product overview

Strong and interesting mix to solve all kinds of security threats



ISC West in Las Vegas is a very important yearly security exhibition for North America, just like Ifsec in London is for Europe and the biennial security exhibition CPSE in Shenzhen is for Asia.

Detektor was of course present at the Sands Convention Center on the 5th to the 7th of April to pick up on trends and to see what the exhibitors had to show this year.

By Lennart Alexandrie

Product wise ISC West is very much a marketing platform where the large companies debut products that have not been released on the market yet. This year was no exception.

Here follows a review on what the ISC West event had to offer the visitors in 2017.

Perimeter security – thermal cameras and radar

A very strong trend at the show was the solutions and products for perimeter security. Exhibitors with thermal cameras and radar technology were especially well represented this year.



IndigoVision enhances range with thermal imaging technology.

IndigoVision, from Scotland, a developer of end-to-end video security solutions, has enhanced its portfolio with the addition of thermal imaging technology. At the show the company offered visitors a preview of the new BX thermal camera.

IndigoVision combines its encoding platform with un-cooled thermal sensors to enable advanced video analytics and temperature measurement analytics in a single, easy to install product. With an effective detection distance of 9,845ft/3,000m for a vehicle, IndigoVision's thermal cameras enable users to see further and more easily protect their assets.

Flir, the market leader in thermal cameras, launched the PT Series HD, which features a thermal imaging technology, new high performance 4x optical zoom thermal lens with autofocus, high sensitivity 1080p visible-light sensor with 30x optical zoom and highly accurate PT engines. All →

UP-TO-DATE security technologies



IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK

Stand F1610

We will be glad to see you!



MANUFACTURER OF SECURITY PRODUCTS

PERIMETER SHOP

www.PERIMETER-SHOP.com

- ✓ Unique character and no analogs
- ✓ One person configuration
- ✓ Accuracy and visualization of the process



→ this combined in a single, powerful perimeter protection system, capable of detecting targets in complete darkness, through smoke, dust and during the harshest environmental conditions. The PT-Series HD integrates with Flirs Unite VMS, featuring full control, proprietary dual-sensor, viewing mode, programmable presets and PT auto-tracking functions.

The American company **SpotterRF**, displayed *Spottercop*, a software that helps to monitor the condition of hundreds of sites and thousands of Spotter radars and cameras. It provides a system level view of the conditions of the perimeter security system and offers a way for the quick identification and prioritisation of health-related events in a web-based user interface.

Axis surprised everyone when they added a new product to their portfolio, namely an outdoor motion detector with radar technology. The network radar detector – *Axis D2050* – enables motion detection in a specified area and reduces false alarms. It offers cost-efficient perimeter protection and Axis claims it is a great complement to existing surveillance solutions in smaller outdoor areas, such as warehouse perimeters and construction sites, that need monitoring after-hours.

Magos Systems from Israel was also in Las Vegas to promote its *SR-500*, a radar based perimeter system for both rural and more saturated environments. It covers an area of more than 250,000

square metres with a detection range of up to 400 metres for a walker and 600 metres for a vehicle, and yet consumes extremely low power (<3,5W) with a small form factor.

Another interesting product at the show was *Hydra* from the USA-based **Thermal Imaging Radar**. Hydra provides unprecedented wide area monitoring through continuous 360 degree thermal intrusion detection combined with 360 degree targeted surveillance from a 30X zoom laser IR starlight PTZ. The thermal radar continuously scans 850,000 square metres every two seconds targeting intruders with edge-based analytics followed up with slow-to-see operation from the starlight PTZ.

A similar product was the *Aeron Searcher*, launched by **Sierra Olympics**. This environmentally-rugged outdoor video surveillance system features true thermal PTZ with an optical zoom thermal imager, zoom thermal imaging and continuous 360 degree rotation. It has IP67 class environmental protection and delivers 640 x 480 thermal core and continuous zoom thermal imaging. Furthermore the Aeron Searcher has HD and SD video options. It also offers wide, intermediate and narrow zoom and can detect a person at a distance of up to 3.4 kilometres.

Video surveillance cameras

Panasonic presented their *Aero PTZ camera*, a rugged unit for a

wide range of extreme environments, providing full HD surveillance



Aero PTZ camera from Panasonic.

images at 60fps and 30x optical zoom lens. The Aero PTZ is ideal for applications like ports, transit yards, airports, city surveillance, highways or any area or location prone to severe natural weather conditions or other factors that might wreak havoc on the operation and reliability of a typical video surveillance camera.

Pelco showcased its enhanced series of *Optera* Panoramic multi-sensor cameras with Surevision 3.0 technology in Las Vegas. The 360°, 270° and 180° 12 MP multi-sensor cameras provide completely stitched, seamless and blended

panoramic views with electronic PTZ capability across the entire panoramic image to provide superior wide area surveillance and forensic scene analysis.

The *Optera* Panoramic multi-sensor cameras capture high quality images in difficult lighting conditions where highly contrasted lighting sources exist within the same scene. An enhanced WDR of 130 dB, advanced low light performance with full colour down to 0.05 lux, anti-bloom technology, 3D noise filtering, and enhanced tone mapping for colour accuracy ensure excellent performance for virtually any application.

It also features smart compression technology, which reduces bitrate usage, resulting in up to 70% savings on storage, according to the company.

Optera Panoramic multi-sensor cameras are preloaded



Håkan Hansson, global product manager for the audio portfolio of Axis, acted as a magician during the company's press meeting just an hour before the opening of ISC West Expo. Martin Gren (to the left), the co-founder of Axis, displayed for the first time the network radar detector together with Fredrik Nilsson, Vice President for Axis in America.

One-stop service for innovative RFID products

125KHz / 13.56MHz / 433.5MHz / 915MHz / 2.45GHz



- Biometric (Fingerprint)
- Bluetooth / NFC Access Controller
- Passive / Active RFID System
- Reader / Writer Programmer for LF / HF / UHF frequency
- Car Parking System / Lift Access Control System
- Single / Multi-Door Access Controller / ESD Access Control System
- Electric Strike / Electric Deadbolt / Electromagnetic Lock
- Exit Button / Contactless Infrared Sensor Exit Button

Module Series

- Compact with **Dual, triple, quadruple** decoding by single module.
- With **multi-selectable output formats** (ABA, Wiegand, UART, RS-232, RS-485)
- **Low power** consumption modules with **sleep mode** supported.
- **OEM / ODM** available.





PONGEE INDUSTRIES CO., LTD.
www.pongee.com
pongee@pongee.com.tw
Made In Taiwan

with advanced analytics including: abandoned object, intrusion detection, camera sabotage, wrong direction, loitering detection, object counting, object removal, and stopped vehicle.

Arecont launched its new *Surroundvideo Omni G3* which is the latest member of the Omni multi-sensor and multi-megapixel series. It has all the features of Arecont's other 4-sensor Omni camera. This new camera has no-touch remote setup, making it the fastest adjustable-view multi-sensor camera on the market, according to Arecont Vision.

Omni G3 uses the patented omnidirectional track that allows the camera to cover any angle and view up to 360 degrees, including blind spots below the camera, just like earlier models for non-stop situational awareness. The installer just puts it on a wall, ceiling, pole, corner, or emergency call box, attaches the base plate, plugs in the PoE Ethernet cable, tightens the screws, and they are done. Then, just pick a 180, 270, 360o view and the camera sets itself to that view.

The end user or installer can also adjust the camera to any other position using the same onscreen remote interface. They can also save those settings, so if used in a stadium, for example, they could choose one view for a sports event and another for a concert audience.

Arecont were also talking about their integrated advanced cyber security protection that is in every

Arecont Vision camera, which they believe is the only non-hackable-camera architecture on the market.



Dome network cameras from Vivotek.

Vivotek introduced two anti-ligature corner dome network cameras with the fixed lens *CD8371-HN-VF2* and vari-focal lens *CD8371-HNTV*.

With anti-ligature edges, the camera can provide a prevention against self-harm and even suicide. Designed to be installed in the upper corner of a cell, the corner dome cameras also allow security officers to see any event in the cells, with a wide angle horizontal FOV up to 108° and a vertical FOV up to 79°.

Moreover, each device is armed with a robust vandal-proof IK10+ rated and weather-proof IP66 rated housing, enabling the camera's body to withstand water and protect against vandalism or tampering. The cameras are also equipped with shock detection and advanced tamper detection in case of malicious attack. Thanks to two-way audio and a built-in microphone, sound can also be clearly monitored and recorded at up to 5 metres.

Offered as professional day and night cameras, the CD8371-HN-VF2 and CD8371-HNTV feature built-in 940nm IR illuminators ef-

fective up to 10 metres and which operate invisibly whilst guaranteeing security in total darkness. These cameras also support WDR Pro, which captures both dark and bright areas of an image and combines the differences to create a highly realistic representation of the original scene. Furthermore, they also deploy SNV (supreme night visibility) technology to ensure high quality images even under low-light conditions. This effective visibility further enables the cameras to deliver high-level security around the clock to areas of critical importance.



Visix V-Series 2MP from 3xlogic.

3xlogic launched a new All-in-one Multi-Sensor camera, along with a significant upgrade to the company's Vigil Software Suite, which includes Vigil Server and Client, Vigil Central Management (VCM), Vigil POS and the View Lite II Mobile App.

The *Visix V-Series 2MP* indoor multi-sensor camera has the ability to host the Vigil Server, allowing the camera to record video to the on board SD card, with full search capabilities in Vigil Client and in the View Lite II and Infinias mobile apps. Through Vigil Central Management (VCM) it becomes

easy to monitor online/offline and recording status as well as number of days of recorded footage. A true all-in-one solution, built-in passive infrared (PIR) sensors, 2-way audio with Vigil Server, and digital I/O allow the multi-sensor to be an alarm annunciator, audio system, and video recorder in one, small unit. Paired with an eIDC32 and Infinias Cloud, users can achieve a completely serverless access control and video system without having to store video in the cloud.

The multi-sensor camera was designed for quick, easy deployment, and acts as a stand-alone or integrated security surveillance solution.

A powerful all-in-one device in a tiny package, the 3xlogic multi-sensor camera provides combined PIR and pixel-based motion detection to reduce false alarms and on-board DIO for alarming and relays.

Axis Communications introduced the *Axis FA Series* with modular cameras for highly discreet, yet cost-efficient video surveillance, and three new additions to the Axis P13 Series that offer 4K resolution in full frame rate and that enable coverage of large areas with high image detail.

Dahua, from China, launched a multi-sensor 360 degrees panoramic with 2P integrated PTZ camera. This all-in-one combines eight 2MP sensors for 360 degree field of view, along with a 2MP 30x PTZ, allowing personnel to precisely track subjects in mission-critical scenarios. It provides a →

Just stay analouge. Digitise with DALM.

Analogue alarm systems need not become outdated. By digitising existing installations using our DALM security router, opportunities can be created for more security solutions with even greater flexibility.

In other words, alarm communication via the Internet opens up a world of completely new opportunities. Without any expensive investments.

Read more about next generation alarm communication at dualtech.se



→ seamless view without blind spots, plus exceptional responsiveness and situational awareness.

The new Avigilon Unusual Motion Detection ("UMD") video analytics technology was in focus for a preview on the **Avigilon** stand at ISC West. UMD is an advanced artificial intelligence ("AI") technology that Avigilon believes brings a new level of automation to surveillance. This technology is designed to continuously learn what typical activity in the scene looks like and focus the operator's attention on atypical events needing further investigation.

By continuously learning, UMD is able to automatically detect unusual events, such as a vehicle moving in the wrong direction on a road, or a crowd running in panic in a public space. This technology enables users to quickly search through volumes of recorded footage with ease, revealing events that might have otherwise been missed.

This technology is designed for Avigilon's complete line of video analytics solutions. Existing customers will be able to upgrade certain legacy products to benefit from this exciting new technology.

On the exhibition Avigilon also showcased its expanding deep learning artificial intelligence (AI) search engine: Avigilon Appearance Search technology, with two powerful new features that help users save time and effort during critical investigations.

Using deep neural networks for face analytics, Avigilon Face Appearance Search technology enables searching for a person by incorporating the unique characteristics of a face to find

similar recorded footage of that person across a site. For operators, this technology increases the speed and accuracy of investigations, by detecting and understanding that it is searching for the same person, even if items such as their clothing change over time.

Avigilon Vehicle Appearance Search technology enables users to quickly search recorded footage and find a specific vehicle across a site. This technology is designed to provide security operators critical information about where and when a vehicle might have been before and after an event.

Both Avigilon Face and Vehicle Search have been designed to be part of Avigilon Appearance Search technology, and will be integrated with Avigilon's full line of video analytics solutions. Existing customers will be able to upgrade certain legacy products to benefit from these exciting new technologies.

Theia Technologies demonstrated its award-winning family of compact 4k lenses at ISC West on Hanwha's new XNB-8000 *Wisenet* 5 camera as well as on Dallmeier's *DF5400HD-DN 4k* camera.

Theia's motorised TL1250 and TL936 lenses were shown at ISC West on Arecont's Megavideo G5 series cameras.

The motorised zoom, focus, and P-iris lenses also feature custom housings.

Theia's family of compact 4k lenses in fully motorised or manual versions continues to be selected and approved by OEM camera companies including Vivotek for use on their IP9181-H camera, and by Dahua for their 4k cameras.

Video analytics solutions



Smart camera GV-VD8700 from Geovision.

by the Qualcomm Snapdragon 600 series IoT connected camera portfolio and Intellivision's Face Recognizer solutions.

With this new camera Geovision brings what it believes to be the world-first deep learning-based, 4K HEVC, intelligent video analytics (IVA) on-device smart camera, featuring on-camera face detection, tracking, recognition of up to eight faces, human detection, and intrusion detection for various security applications.

Traditionally, video analytics processing for video surveillance has been limited to server or cloud management due to CPU or GPU constraints, which are often still time lagging to properly provide meaningful and useful analytic results in real-world applications, and on time. Qualcomm's Snapdragon 600 connected camera platform and Intellivision's video analytic algorithm fundamentally changes how video is captured and analysed, to truly build a new class of "Artificial Intelligence (AI) camera", so that the camera can help to sense, gather, and analyse data. With the new platform, the GV-VD8700 can easily add deep learning capabilities with very low power requirements; reduce data streaming, and create immediate action and event alerts. Video analytics features such as facial recognition, human detection, and intrusion detection will be able to operate on multiple channels in real time.

Another face recognition solution was launched by **3M**. The *3M Live Face Identification System* (LDIS) is a software only back-end system that processes video in real time or post-event and searches against person-of-interest databases for the identification of people. It is scalable, easily configurable, cloud-deployable, and leverages the customers' choices of IP cameras and/or mobile devices. According to 3M laboratory testings the LFIS

Geovision showcased its new deep learning based smart camera GV-VD8700, powered

is more than 95 percent accurate with less than a second between capture and identification.

Other video surveillance products



WES3HTG from KBC Networks.

The latest updates in transmission solutions by **KBC Networks** was showcased at ISC West. The company displayed the new and improved *WES3HTG* wireless transmission system and some of the best in real-time encrypted video and data communication over 3G/4G networks with the new generation ThruLink.

The new *WES3HTG* wireless transmission system is marketed as one product but with three configurations - client, host or multipoint host. The new system incorporates enhanced user-selectable firmware, backhaul applications, compact design and full technical support.

ThruLink allows real-time, encrypted video, voice and data to be transmitted over public networks such as the Internet or 3G/4G/LTE. It enables users to take full advantage of public infrastructure while maintaining data security.

Hikvision's new, single-unit intelligent video management station – the *Blazer Express* – focuses on managing Hikvision IP cameras with the Windows-based NVR, using the operating system on an SSD (Solid State Drive). It has 16- or 32-camera options with 16 built-in POE inputs for IP cameras, and up to 24 TB of onboard storage; central management, with live view and playback from up to 15 remote NVRs or Blazers; and powerful video analytic searches with POS integration.

Nuuo from Taiwan presented their *NVR and VMS platform*, which work in both Linux and Windows O/S environments. Their VMWare version is engineered to be scalable and flexible with advanced functions such as, intelligent video analytics, facial recognition, license plate identification, and point of sale for retail applica-



One of the product highlights of the show was *Mission Control*, a decision support system from the Canadian VMS company Genetec. Rémi Bréval, the director of Mission Control Group, demonstrated the system for the impressed editor of *Detektor*.

tions to meet almost all sizes of system requirements from markets worldwide.



Theia Technologies displayed their 4k lenses.

Theia Technologies demonstrated its award-winning family of compact 4k lenses at ISC West on Hanwha's new XNB-8000 *Wisenet* 5 camera as well as on Dallmeier's DF5400HD-DN 4k camera. Theia's motorised TL1250 and TL936 lenses were shown at ISC West on Arecont's Megavideo G5 series cameras.

The motorised zoom, focus, and P-iris lenses also feature custom housings.

Theia's family of compact 4k lenses in fully motorised or manual versions continues to be selected and approved by OEM camera companies including Vivotek for use on their IP9181-H camera, and by Dahua for their 4k cameras.

Access Control

In the field of access control there were several exhibitors at ISC West, showing off their latest products. Different types of biometrics, bluetooth and NFC were all common among these exhibitors.

Following the 3.5" OLED touch-screen terminal, to complete their *Crystal* series, **Civitec Global** also presented a new RFID and Bluetooth reader. The



Crystal series from Civitec Global.

new Crystal keypad is equipped with a 2.4" OLED display with a mechanical keypad in a housing for outdoor applications.

As it is a 125KHz/13.56MHz RFID reader, the Crystal is able to read CSN or encrypted protected data from 13.56MHz smart cards utilising key diversification and

mutual authentication routines. It can be equipped with one or more SAM modules for secure data encryption.

The Crystal keypad is featured with a mobile key application through ISO18092 NFC and Bluetooth technology as well, with more data transmission options such as Ethernet, RS485 OSDP protocol, and Wiegand, USB.



Bio-Sign 2.0 from Suprema.

Suprema, Korean developer of biometric access control readers, decided to highlight something different this year, namely the *Bio-Sign 2.0*, a game-changing mobile fingerprint authentication algorithm, featuring what is hailed as the world's fastest matching speed.

According to the company, its latest artificial intelligence technology, means that the new Bio-Sign 2.0 algorithm yields matching speeds of up to twice as fast as the best competitor's solution while far outpacing competitors in terms of accuracy (FRR) and level of security (FAR). Moreover, Bio-Sign 2.0 offers enhanced robustness over time and extra flexibility in integration by supporting various types and sizes of sensors.

Bio-Sign 2.0 is designed to produce best performance even with low-end application processors (AP), therefore it will take the essential role for low-cost smartphones to adopt fingerprint authentications. Bio-Sign 2.0 performs a matching speed of 50ms with high-end APs and 100ms with low-end APs while maintaining the security level (FAR) under 0.0005%.

When it comes to fingerprint authentication in smartphones, due to changes in scanning habits and skin condition, current technology often results in poorer performance with use over time. Powered by a self-learning mechanism on its algorithm, Bio-Sign 2.0 gets smarter with use. Bio-Sign 2.0 learns the user's habit and conditions con-

tinuously, the algorithm self-evolves to cope with such change and results even better accuracy with use over time.

Texas-based **Crucialtrak** launched *BACS*, which stands for Biometric Access Control System. It is claimed by Crucialtrak to be the world's first multi-biometric authentication technology, providing the highest security measures by layering four different biometric authentications in to one terminal. In each BACS module, up to four biometric identification technologies are considered touchless fingerprint, iris patterns, vein patterns and facial recognition authentication. The user can customise different biometric identification layering options accordingly depending on the level of security required. The highly secured algorithms maximize accuracy and accountability of the identification process.

Management systems for incidents and more

B Alert IoT Security commander from **Alertenterprise** is an IoT based security incident management and response platform, built for enterprises. The goal is to leverage employees, contractors and other staff to be the eyes and ears of the organisation and report suspicious or unsafe conditions to security operators. It is the perfect "See something – say something" companion, according to Alertenterprise.

Amika Mobile was another exhibitor, launching the *Amika Mobility Server* (AMS), an intelligent and secure critical and emergency communication platform for on-premise/cloud or hybrid deployments. AMS auto-discovers active directory information and maintaining the pre-defined organisational structures. AMS alerts and receives responses over wire or mobile or any communications layer.

Most interesting though was the demonstration of *Mission Control* on the **Genetec** stand. From monitoring and detecting through to resolving and reviewing, Mission Control guides the users on how to manage any incident from start to finish. It provides organisations with the data and tools to respond to situations quickly, confidently and intelligently.

This so called Decision Support System provides organisations with new levels of situational intelligence, visualisation, and complete incident management capabilities.

It allows security personnel to make the right decision when faced with routine tasks or unanticipated situations by ensuring a timely flow of information. Mission Control empowers organisations to move beyond simple event and alarm management by collecting and qualifying data from thousands of sensors and security devices, spotting the most complex situations and incidents, and guiding security teams in their response following organisation-specific processes and compliancy requirements.



The world's largest manufacturer of video surveillance products was of course present as an exhibitor at ISC West Expo. Keen Yao, VP Hikvision International Business Center was satisfied with the response from the visitors. Finn Vu, international marketing manager, also seemed happy with the flow of visitors to the stand.

London gets ready to receive the global security industry

Europe's largest security event in 2017 – Ifsec International – will be held from the 20th-22nd of June at Excel London. By Joakim Kempe

Approximately 27,000 visitors will descend on the capital to gain access to over 10,000 security solutions covering every aspect of security, from access control and video surveillance to smart buildings, cyber security, border control and so much more.

Visitors will be given a comprehensive update on the latest innovations within the security industry and the opportunity to hear from the leading experts in the field during this three-day event.

Borders and Infrastructure

With the recent terrorist attacks still fresh in the memory and the constant ongoing threat to European cities, security concerns are clearly on the rise and many countries are increasing their

investments in security measures.

Because of the current situation with the threat of terrorism and the complex refugee situation in Europe, the organisers of Ifsec are launching a Borders & infrastructure event within the security show. The event will focus on large-scale security issues and solutions and seminars addressing other aspects of the security industry.

Firex alongside Ifsec

For the third year Firex International will sit alongside the security exhibition Ifsec. As the two industries are increasingly becoming more aligned, placing them side by side makes it easier and quicker for visitors to obtain the information, resources and

products they are looking for when they visit.

As a significant amount of the visitors represent major vertical sector end users, the organisers have made some special sections to satisfy their needs. These sectors include safeguarding and protection of transportation, national infrastructure, border and immigration control.

The Smart Zone

A growing area this year is The Smart Zone where the various technology solutions within the growing field of Internet of Things

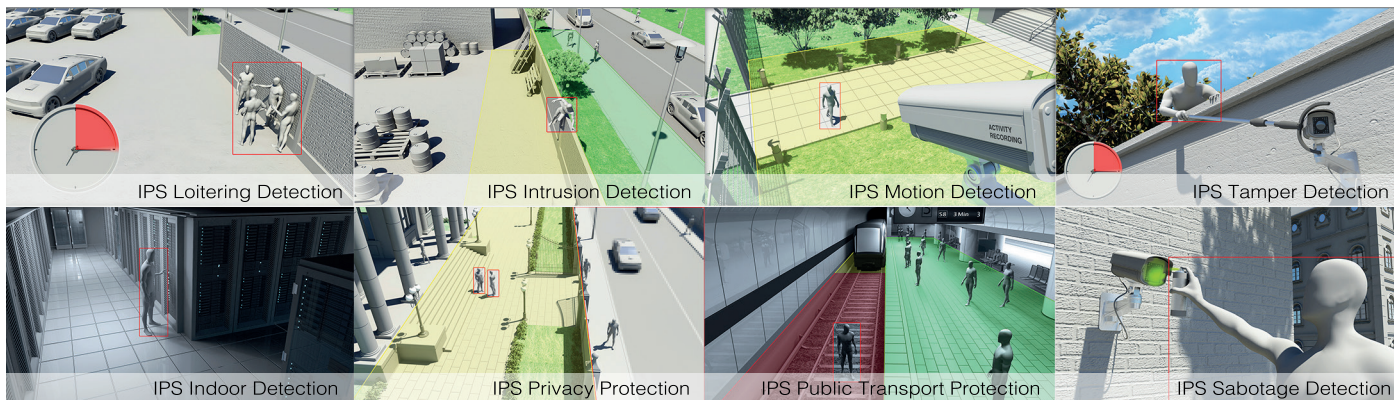
(IoT) for home and commercial buildings are presented. Following on from last years successful "Home Automation House" – a fully functioning smart home will be located in the middle of the exhibition.

600 exhibitors

Ifsec International is the largest yearly organised security event in Europe and a perfect forum for professionals to learn more about security, to find new suppliers, partners or customers. The three day-event will host over 600 global leading suppliers under one roof.



Europe's largest security event in 2017 – Ifsec International.



IPS VideoAnalytics are intelligent, software-based analytics modules operated on servers or cameras and encoders for automatic real-time detection of security related objects or events in video images. With the IPS AnalyticsManager, IPS VideoAnalytics can easily be integrated into third-party systems.

- Free choice between edge-based or server-based video analytics
- Various video analytics for different applications available
- Intuitive configuration and operation with state-of-the-art web tools
- Compatible with current video management systems
- iLIDS certified for critical infrastructures (CPNI High Class 3 Level)



Securiton GmbH
IPS Intelligent Video Analytics
www.ips-analytics.com



Intelligent Video Analytics

THE WORLD'S BIGGEST SECURITY TRADESHOW



THE 16TH CHINA PUBLIC SECURITY EXPO

Oct 29-Nov 1, 2017 | Shenzhen Convention & Exhibition Center

The 14th China Public Security Forum

The CPSE Golden Excellence Award 2017

GSIA Gold Shield Award 2017



Exhibition Area (m²)

110,000

Exhibitors

1,100

Visitors

130,000

Booths

6,000



Security Events Calendar

May



2-4 May Intersec Saudi Arabia 2017

Venue: Jeddah Centre for Forums & Events KSA
Organiser: Frankfurt Middle East GmbH P.O.
Email: intersec-ksa@uae.messefrankfurt.com
Website: www.intersec-ksa.com



3-4 May Security & Counter Terror Expo

Venue: Olympia, London United Kingdom
Organiser: Clarion Events
Email: sophie.mckimm@clarionevents.com
Website: www.counterterrorexpocom



17-18 May Security Forum 2017 - Barcelona, Spain

Venue: Centro de Convenciones Int. de Barcelona
Organiser: Peldaño
Email: info@securityforum.es
Website: www.securityforum.es



18-19 May International Police Expo

Venue: Pragati Maidan, New Delhi, India
Organiser: Nexgen Exhibitions Pvt. Ltd.
Email: ashish@nexgenexhibitions.com
Website: www.internationalpoliceexpo.com



23-25 May Exposec - Sao Paulo, Brazil

Venue: Sao Pulo Expo
Organiser: Fiera Milano
Email: comercial@fieramilano.com.br
Website: www.exposec.tmp.br



30 May - 1 June Securex West Africa - Johannesburg, South Africa

Venue: Gallagher Convention Centre
Organiser: Specialised Exhibitions (Pty) Ltd
Email: www.securex.co.za

June



20-22 June Ifsec 2017 - London, United Kingdom

Venue: Excel Exhibition Ground
Organiser: UBM
Email: info@ubm.com
Website: www.ifsec.co.uk

September



27-28 September SecurityUserExpo 2017

Venue: Bella Center, Copenhagen, Denmark
Organiser: AR Media International
Email: info@securityuserexpo.com
Website: www.securityuserexpo.co

October



9-11 October OFSEC Expo - Oman Fire, Safety and Security Exhibition - Muscat, Oman

Venue: New Oman Convention and Exhibition Centre
Organiser: Muscat EXPO
Email: marketing@muscat-expo.com
Website: www.muscat-expo.com



29 Oct - 1 Nov CPSE 2017 - Shenzhen, China

Venue: Shenzhen Convention & Exhibition Center
Organiser: Shenzhen CPSE Exhibition co., Ltd
Email: overseas_market@cps.com.cn
Website: www.cpse.com.cn

November



6-8 November Fire, Safety & Security Expo -

Venue: Palais Des Expositions D'Alger, Algeria
Organiser: New Fields
Email: jia.matthew@new-fields.net
Website: www.new-fields.com



6 Nov-9 November Defense & Security 2017 - Bangkok, Thailand

Venue: Impact Exhibition and Convention Center
Organiser: GML Co., Ltd
Email: yaowalak@asiandefense.com
Website: www.asiandefense.com



15-17 November Sicurezza 2017 - Milano, Italy

Venue: Fiera Milano (RHO)
Organiser: Fiera Milano
Email: areatecnica1@fieramilano.it
Website: www.sicurezza.it



16-18 November Secutech Thailand 2017 - Thailand

Venue: Bangkok International Trade and Exhibition Center
Organiser: Messe Frankfurt New Era Business Media Ltd, Taiwan Branch
Email: info@newera.messefrankfurt.com
Website: <http://secutechthailand.tw.messefrankfurt.com/bangkok/en/exhibitors/welcome>



21-22 November Sectech Sverige - Sweden

Venue: Stockholmsmässan
Organiser: AR Media International AB
Email: deniz.baykal@armedia.se
Website: www.sectech.nu

Detektor International takes no responsibility for any changes to the details of the above mentioned events. Please always contact the organisers in each case to confirm the dates and venues.
www.securityworldhotel.com/int/Security-Events

Security buyers guide

Alarm Communication



Tel +44 (0)1895 474474
sales@csldual.com
www.csldual.com



Nedap Security Management

Parallelweg 2, 7141 DC, Groenlo
PO BOX 103, 7140 AC, Groenlo
The Netherlands
Tel + 31 544 471 111
www.nedapsecurity.com
info@nedapsecurity.com

CCTV



Security Tech Germany

ABUS Security-Center GmbH & Co. KG

Linker Kreuthweg 5
86444 Affing (Germany)
Tel +49 82 07 959 90-833
Fax +49 82 07 959 90-180
export@abus-sc.com
www.abus.com



outdoor protection
our profession

Via Gadames 91, 20151 Milan, ITALY
Tel +39 02 380 701
Fax +39 02 308 80 67
www.sicurit.com, export@sicurit.it

Access Control



Box: 3042, 443 03 Stenkullen
Tel: 0302 680 600
Fax: 0302 680 640
Epost: info@cardkeep.se
Webb: www.cardkeep.se



Touchless Biometric Systems AG

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

Perimeter Protection



Forteza, JSC

Tilzes str. 38, 91112 Klaipeda
Lithuania
Phone +370 46 441195
Fax +370 46 412231
forteza@forteza.com
www.forteza.com



TAKEX Europe Ltd.

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

WISeNeT
SAMSUNG



WISeNeT X series
eXtreme performance

- 2X faster video processing for a supercharged performance
- 3X more memory so bring on enhanced video and audio analytics
- eXtra storage with half a terabyte on-board to pack it all in
- eXceptional WDR (150db) you'll be amazed by the world's best
- eXclusive compression improving your bandwidth up to 99%

eXperience it now www.WisenetX.com

 **Hanwha**
Techwin

HIKVISION®

CRUCIAL SAFETY IN A CRITICAL ATMOSPHERE

- ATEX & IECEx certification
- Darkfighter technology
- H.265+ smart codec, VCA functions



Hikvision's Explosion-Proof Camera Series Add Another Layer of Powerful Protection

In industries with flammable gases or combustible particles flittering through the air, every layer of protection is critical. Protect your customers and provide world-class security surveillance with Hikvision's Explosion-Proof Camera Series. The Explosion-Proof Series from Hikvision nullifies the danger of spark or combustion in hazardous facilities such as chemical plants, fueling stations and mining areas. Breathe easy in a combustible atmosphere where first-rate surveillance keeps everyone safe – every day and every way.



Hikvision Headquarters
No.555 Qianmo Road, Binjiang District
Hangzhou 310052, China
T +86 571 88075998
F +86 571 89935635
overseasbusiness@hikvision.com



IFSEC International
SECURING PEOPLE, PROPERTY & ASSETS
20-22 JUNE 2017 EXCEL LONDON UK

Hikvision Booth: E800

www.hikvision.com