

DETEKTOR



International

Publisher's comment

New wave of acquisitions to start in 2018

Security technology market

Top video surveillance predictions for 2018

Detektor security academy

How to implement IoT and security systems successfully

Business news

Securitas kicks off 2018 with a trio of acquisitions

Product news

Hanwha launches Wisenet Wave VMS

The interview

Axis's co-founder Martin Gren: "OEM will come to an end"

Voice of the security market

How will the GDPR mandate affect physical security systems?

Security events

AI, drones and smart technology attracted 30 000 attendees to Dubai

FOCUS ON

THE ELECTRONIC PERIMETER PROTECTION

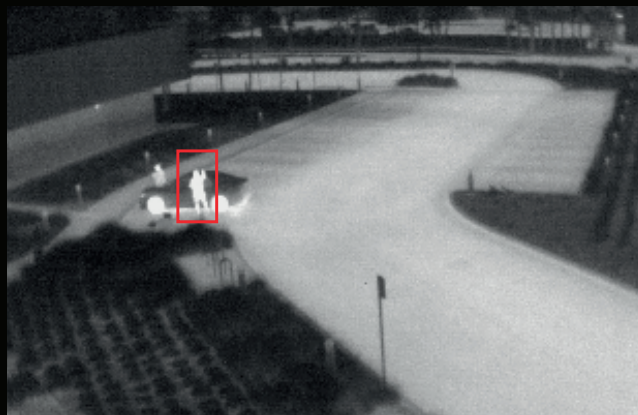
INDUSTRY LEADERS' VIEWS ON THE FAST GROWING SECURITY SUB-MARKET



ADVANCED PERIMETER PROTECTION

For any size system.

The new FLIR FB-Series ID accurately classifies humans and vehicles for fewer false alarms, even in total darkness. Get equipped with affordable, best-in-class perimeter protection from FLIR.



Learn More at
flir.com/security/fb-series





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

Head office:

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

Asia Office

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 51
+46 8 556 306 80

Publisher

Lennart Alexandrie
lennart.alexandrie@armediaint.com

Editorial Team

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

Art Director

Linn A. Maddern
linn.maddern@armedia.se

Advertisements

Carlos Cisternas
carlos.cisternas@armediaint.com

Printing

Sörmlands Printing Solutions AB, Sweden, 2018



Lennart Alexandrie, Publisher

New wave of acquisitions to start in 2018

The security industry is hot. Terror threats, the immigration situation and an expanding organised criminality are all part of today's reality in Europe. They are all examples of factors that have an impact on the demand for security products and services.

Technology development is another factor. Open platforms, scalable security solutions and decreasing price levels all demonstrate increased accessibility. These factors contribute towards, not only an increasing demand for security systems, but also towards the development of IoT solutions and business models based on security as a service, which will take the market to a new level.

For western businesses, the competition from Asia – primarily from China – has increased and accelerated the consolidation of the market.

The fragmented security market – where a large number of smaller companies operate – is also a significant acquisition factor as large scale is seen as a necessity for survival.

Let's take a look at the global market in 2017 - focusing on manufacturers / product developers in the field of alarm, video surveillance and ID/access control. According to market analysis company Memoori and their report on the global market for physical security, mergers and acquisitions of 6.2 billion dollars took place in 2017. This is only one third of the \$19.7 billion dollars realised in the previous year, but 2016 was an extreme year for acquisitions, very much affected by the Johnson Controls and Tyco merger, which almost doubled the size by value.

Now Memoori forecasts that 2017 was the start of a new wave of growth that will reach more than 7.8 billion dollars by 2022. The reasons for that belief are many.

- With so many smaller companies struggling with competition, it is inevitable that acquisitions and mergers will continue to increase over the next five years.

- Furthermore, the European and American manufacturers in the video surveillance industry are working on reaching volume and on a large scale. The easiest way is through acquisitions, and they need to take action quickly, as Chinese players are rapidly taking larger shares even in more developed markets.

Memoori also provides some examples of major acquisitions (over 100 million dollars) in 2017/2016 which they believe will strengthen the market for physical security.

- Flir's acquisition of Point Gray Research for \$ 253 million.
- Advent's (Oberthur's) purchase of Safran's Card System and Identity divisions for 2.4 billion Euros.
- Gemalto's acquisition of 3M's identity management business for \$ 850 million.
- Flir Systems' acquisition of Prox Dynamics AS for an estimated \$ 134 million.
- HID Global's acquisition of Mercury Security for \$ 250 million.

Memoori also mentions the bid of Taiwan's video surveillance company Vivotek from Delta Group from the same country. Delta Group has an annual turnover of \$ 8 billion. This business can also affect the security market.

An interesting acquisition is also that the American investment company Bain sold the Chinese video surveillance company Uniview to the Chinese company Hangzhou Jiaozhi Technologies Co. for 535.6 million dollars. It shows the Chinese companies' financial strength. The fact that it was a Chinese company that acquired Uniview confirms the cautiousness of Western companies when it comes to making acquisitions in China. After all, the buyer of Uniview, is presented with access to the world's largest local market for video surveillance equipment.

Having said that, it may be appropriate to confirm that business acquisitions across borders have a general downward trend. In 2017 these stood at 32 percent, compared to 48 percent in 2016, 42 percent in 2015 and 50 percent in 2014. According to the Memoori report acquisitions are not simply about expanding geographically and more about buying leading technology and innovative products.

It will be interesting to follow the development of the security market in 2018.

PS: The report "The Physical Security Business 2017 to 2022" can be ordered at www.armediaint.com



Jiaqi Gao, Dahua, Joe Grillo, Vanderbilt, Martin Gren, Axis, Pierre Racz, Genetec, Boudewijn Hak, Bosch, Peter Kim, Idis, William Ku, Vivitek, Tim Biddulph, Hanwha,

The electronic perimeter protection

Terrorism is the main driver in the perimeter protection market. Detektor met up with some of the leading physical security manufacturers to find out more about this market and to hear about the most efficient technologies for securing perimeters.

Page 20

3 Publisher's Comment. New wave of acquisitions to start in 2018.

8 Voice of the Security Industry. How will the GDPR mandate affect physical security systems?

10 Security Technology Market. Top video surveillance predictions for 2018.

12 Detektor Security Academy. How to implement IoT and security systems successfully.

16 Business News. Securitas kicks off 2018 with a trio of acquisitions.

20 Electronic Perimeter Protection. Industry leaders' views on the fast growing security sub-market

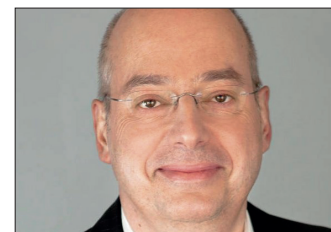
22 Product News. Axis launches palm-sized PTZ smart home camera.

27 Interview. Martin Gren, Axis co-founder: Cyber security and the end of OEM.

28 Security Events. AI, drones and smart technology attracted 30 000 attendees to Dubai.

30 Security Buyers Guide. The directory of important suppliers of security products & services.

30 Security Events Calendar. The international overview of scheduled security shows.



How will the GDPR mandate affect physical security systems?

Philippe Deby, Genetec's Business Development Director for Europe

Page 8



Security Technology Market

Top video surveillance predictions for 2018

Page 10



Detektor Security Academy

How to implement IoT and security systems successfully.

Page 12



"OEM will come to an end"
Martin Gren believes cyber security will continue to be the industry's biggest trend in 2018.

Page 27



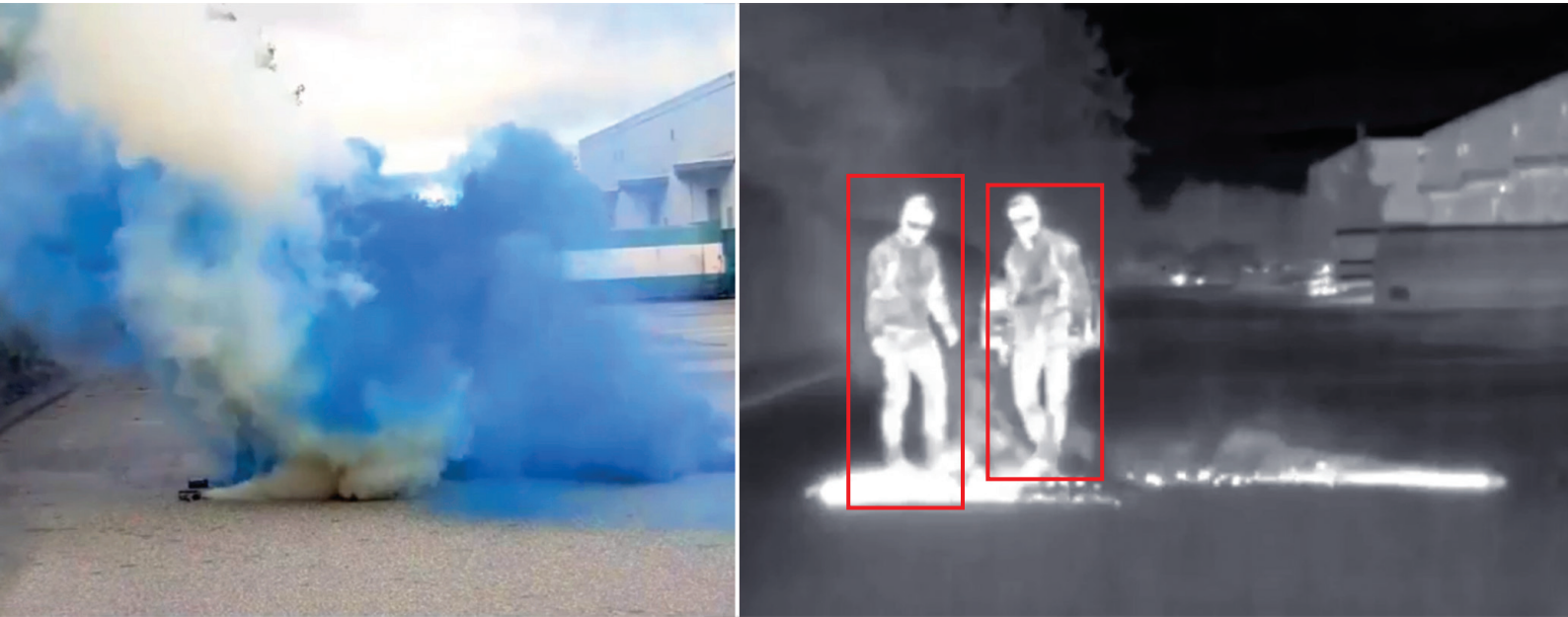
AI, drones and smart technology attracted 30 000 attendees to Dubai

This year's first major event – Intersec – took place on 21–23 January, attracting 29 522 visitors from 129 countries to the Dubai International Convention and Exhibition Center.

Page 28

Seeing Beyond What's Visible

The H4 Thermal Camera



Operating beyond the visible spectrum, the Avigilon H4 Thermal camera is designed to detect the movement of people and vehicles even in areas with poor visibility, challenging lighting conditions, absolute darkness and partly camouflaged scenes.

Avigilon Control Center (ACC) software integration

Seamless analytics configuration and alarm notifications

Patented Avigilon self-learning video analytics

Helps operators detect, verify, and act on events

HDSM SmartCodec[™] technology

Helps to reduce camera bandwidth, maintains exceptional image quality, and lowers storage requirements

IP66 environmental and IK10 vandal resistance certified

To help withstand challenging climate conditions



[avigilon.com/h4-thermal](https://www.avigilon.com/h4-thermal) | asksales@avigilon.com

Dahua Technology launches ePoE IP System

Dahua Technology Co. Ltd has launched a system of extended Power over Ethernet (ePoE) devices including cameras, network switches and network recorders. Dahua ePoE IP system supports up to 800 metres between the ePoE camera and the ePoE network switch or ePoE NVR with embedded switch. It overcomes the limitation of traditional Ethernet and POE (both restrict cable distances to 100 metres (328 feet) between network ports) and eliminates the need for Ethernet extension devices or additional network switches.

Product features

Dahua provides the complete solution for the ePoE IP System including IP cameras, NVRs and Network switches. The system has the following features:

1. Extended PoE transmission: 800m, 10Mbps, 13W or 300m, 100Mbps, 25.4W
2. Automatic set up, plug & play
3. Perfect for analogue to IP migration: IP video, audio, control & power (4 in1) over coax cable; with LR1002 ePoE to BNC adaptor

ePoE Series Network Cameras

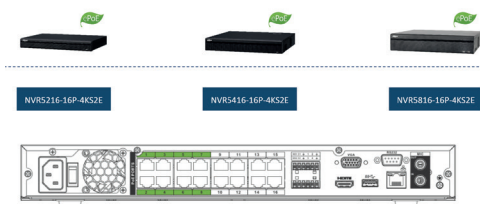
The ePoE series IP cameras cover resolutions from 1080P to 4K, and have rich selections of camera form factors (box, bullet, dome, eyeball) and lens types (vari-focal, fixed lens), which can meet most surveillance requirements. In addition, as a sub-category of the Eco-savvy 3.0 series, they inherit all the software features of Eco-savvy 3.0 series products, such as Smart Video Detection (Tripwire, Intrusion, Abandoned/Missing detection), Face Detection and Smart H.265+ encoding. They are a good choice for installers with long-distance transmission needs.

ePoE Series Network Recorders

The ePoE series network recorders have 8 green ePoE ports that support

long-distance PoE transmission (300m@100Mbps/800m@10Mbps/EOC) when connecting to ePoE cameras. There are 3 models with 2/4/8 SATA ports respectively for different storage capacity. An advanced H.265 chipset is deployed to support 4K & H.265 decoding at a performance up to 16ch@1080P or 4ch@4K live view or playback. As a sub-category of the Pro series NVR, they inherit all the software features of NVR5000-4KS2 series products, such as Smart Video Detection, Face Detection, Smart H.265+ decoding, ANPR, POS and custom split. It is compatible with standard Ethernet or PoE cameras and switches, perfect for migration of existing systems.

ePoE Series Network Switch



8 Green ePoE Ports.

The ePoE network switch PFL2106-4ET-96 has 4 ePoE ports that support long-distance PoE transmission (300m@100Mbps/800m@10Mbps/EOC) when connected with ePoE cameras. It supports plug and play and no is configuration required to realise long distance transmission. Additionally, the ePoE series network switch adopts an industrial grade design with wide operation temperature range (-30°C~+65°C) and high level lightning protection, which further saves cost by eliminating the need for an equipment room. In addition, it is also compatible with the non-ePoE IP cameras (100m@100Mbps).

Application Scenarios

For surveillance of large spaces such as big warehouses, parks, gardens and outdoor parking, camera loca-

Power over Coaxial Extender LR1002

- 1*10/100 Mbps Base-TX + 1*BNC
- RG59 coaxial cable: 400m/100 Mbps, 1000m/10 Mbps
- High level lightning protection
- -30°C~+65°C

tions that are dispersed and far from the control centre, usually longer than 100 metres. The conventional approach is to add repeater devices to extend the transmission distance. However, this would increase cost of equipment and installation. A power supply and junction box will be required to install the repeater. It also makes it harder to maintain and increases the risk of product failure. Alternatively, a fibre



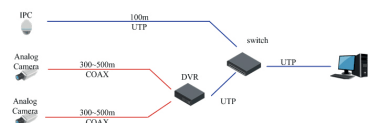
optic transceiver for long-distance transmission is also available.

However, fibre optic cable has to be installed and it requires a power supply at the camera side to power the

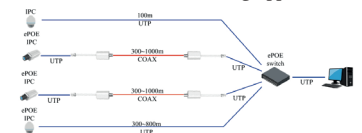
fibre optic transceiver as well as the camera. This is quite a big problem if you have a few installation points over a large space. The Dahua ePoE IP system offers a very simple and effective solution. Dahua ePoE supports up to 800 metres via the traditional Cat5 ethernet cable. It greatly simplifies the network construction as only one cable is required to connect from the front-end to the back-end devices, which results in higher reliability and lower installation and maintenance costs of the whole system.

For migration of analogue surveillance system to IP, reusing existing coaxial cable can largely reduce the installation cost. A proper solution needs to address 3 issues:

adapt the IP video signal and RJ45 connection to coaxial cable, support the length of coaxial cable as it is, transmit power over coaxial cable. Dahua ePoE IP system addresses all of them and makes it easy to reuse existing coaxial cable to run IP video. Power over Coaxial Extender LR1002 connects to an Ethernet port at the IP camera or network switch on the one end and connects to the BNC connector of the coaxial cable on the other end. Dahua ePoE IP system supports transmission up to 1,000 metres over RG59 coaxial cable at 10Mbit/s bandwidth, and delivers a PoE power to the IP camera. This is a simple and effective solution that delivers seamless plug and play solution. It can significantly reduce the cost of analogue to IP migration.



Traditional Mixed Networking Application



Dahua ePoE IP system solution

Summary

The ePoE technology of Dahua adopts advanced 2D-PAM3 coding modulation from the physical layer, and realises full duplex transmission over 800 metres at the speed of 10Mbps, or 300 metres at the speed of 100Mbps via Cat5 or coaxial cable media. Dahua ePoE technology offers a new way to accomplish long distance transmission between IP camera and network switch. It allows more flexible surveillance system design, improves reliability and saves construction and wiring costs.

About Dahua Technology

Zhejiang Dahua Technology Co., Ltd. is a leading solution provider in the global video surveillance industry. In 2016, Dahua was ranked 4th in "Security Top 50" by A&S international. Dahua is committed to providing the highest quality product with the latest technology to enable our customers to perform their business successfully. The company has more than 6,000 R&D engineers and technical staff working on cutting-edge technologies in camera lens, image sensor, video encoding & transmission, embedded processor, graphic processing, video analytics, software reliability, network security and other technologies.

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

IPC-HFW5831E-ZE	IPC-HDBW5831E-ZE	IPC-HFW4831E-SE	IPC-HDBW4831E-ASE	IPC-HDW4831E-M-ASE
IPC-HFW5631E-ZE	IPC-HDBW5631E-ZE	IPC-HFW4631E-SE	IPC-HDBW4631E-ASE	IPC-HDW4631E-M-ASE
IPC-HFW5431E-ZE	IPC-HDBW5431E-ZE	IPC-HFW4431E-SE	IPC-HDBW4431E-ASE	IPC-HDW4431E-M-ASE
IPC-HFW5231E-ZE	IPC-HDBW5231E-ZE	IPC-HFW4231E-SE	IPC-HDBW4231E-ASE	IPC-HDW4231E-M-ASE

*-ZE/Z12E lens optional for bullet and dome

Beyond Video Surveillance

HDCVI-IoT integrates temperature, humidity and alarm info with video

HDCVI 4.0 IoT



HDCVI-IoT enhances the efficiency of agricultural systems, once temperature & humidity exceeds a set threshold, the system can sound an alarm and trigger regulators, ensuring optimal production conditions.

- Temperature & Humidity Camera: Video with real-time environmental info overlay enhances monitoring efficiency.
- Gateway Camera: Connects wireless alarm devices and transmits alarm signal through coaxial cable to the XVR.
- MotionEye Camera: Motion detection & embedded PIR combine with up to 4MP video for visual alarm verification.
- HDCVI-IoT Recorder: Provides centralized IoT management with friendly UI and data reports.
- Easy HDCVI system deployment without extra wiring – saving equipment and labor costs.

Recommended Models



DH-HAC-LC1220T-TH
2MP HDCVI Temperature
and Humidity Camera



DH-HAC-LC1200SL-W
2MP HDCVI
Gateway Camera



DH-HAC-ME1400B/ME1200B
4MP/2MP HDCVI
MotionEye Camera



DHI-XVR7000-4KL
HDCVI IoT Recorder



DH-PFM871A-N1
HDCVI IoT USB Dongle



Philippe Deby, Genetec's Business Development Director for Europe

How will the GDPR mandate affect physical security systems?

There has been a lot of content published already on the EU GDPR, which becomes enforceable on 25th May 2018. Yet, given the unique challenges involved, surprisingly little action and preparation has taken place to prepare for the ensuring compliance required for operating video surveillance, access control and other physical security systems, writes Jean-Philippe Deby, Genetec's Business Development Director for Europe.

Any public or private organisations using CCTV to monitor public accessible areas, for example, should be concerned, because the clock is ticking. Under the terms of the GDPR, monitoring the public on a large scale is by default considered a high-risk activity. Per several market research studies, many organisations have only recently begun taking the steps of reviewing the new regulations and making the changes required to meet the obligations. Over the years, many organisations have created 'self-defined' corporate standards for their physical security systems based around IT standards and technologies. These should be in a better state of readiness as the regulations calls for standardised processes, common organisational approach and technology.

However, a lot of legacy security systems or disparate systems are still out there that may still have been entirely commissioned and operated by location-specific security teams. Regardless as to where your organisation stands in terms of technology, it is important to participate in the GDPR review with a greater sense of urgency.

"All businesses will remain accountable for ensuring data is classified correctly, encrypted, and shared responsibility for managing users and end-point devices"

In the UK, for example, Surveillance Camera Commissioner, Tony Porter, should be commended for his vocal efforts to make security system operators aware that their activities will be subject to the GDPR and to signpost them to relevant guidance from the ICO. For those who don't wish to be caught out, his organisation's independent third party certification is a good place to start. However, with a little over three months until the regulation comes into force, it is still a race against time to see if his organisation will be a position to confirm that it can sufficiently demonstrate compliance with the EU GDPR.

So, what more can operators do in the interim to ensure they are well prepared?

1. Get Involved and start evaluating your current systems

If you or your security and privacy team have not been invited into a GDPR discussion, proactively initiate it with your legal team and ask for guidance. Conduct a gap analysis to identify what works and what might require improvement in accordance with the new regulation. Then engage your consultants, integrators and manufacturers, who should be able to advise appropriate solutions and steps to take. In the vast majority of cases it should be possible to upgrade ones' existing system rather than "rip out and replace".

2. Adopt Privacy by Design

Even though in Sweden, national privacy regulation is stronger or equivalent to the terms of the EU GDPR, data captured by any business or government entity, must be anonymised or pseudonymised to be low-risk. The appropriate use of encryption and automated privacy protection tools is therefore a pragmatic move to assure compliance. For example, video redaction that blurs out the faces of all persons recorded on video, unless there is a legitimate reason to reveal their identity, can minimise the dangers of having security cameras deployed in public spaces. Seek out certified and sanctioned organisations, such as the European Privacy Seal group 'EuroPriSe', a professional organisation whose purpose is to ensure companies meet the 'GDPR-ready' privacy compliance standards—fostering certified trust and reliability.



Jean-Philippe Deby, Business Development Director, Europe, Genetec Inc.

"...three months until the regulation comes into force, it is still a race against time..."

3. Consider cloud-based services as a short cut to compliance

Owners of on-premises video surveillance, access control or ANPR systems are responsible for all aspects of EU GDPR compliance, including securing access to the systems and servers storing the information.

However, by working with an approved cloud provider, it is possible to offload some of these responsibilities.

For example, Genetec partners with Microsoft Azure to offer these systems and encrypted storage 'as a service'. This pathway significantly reduces the customer's scope of activities required to ensure compliance, and is highly cost effective. Yet it is important to realise it isn't a full abdication of responsibility. All businesses will remain accountable for ensuring data is classified correctly, encrypted, and shared responsibility for managing users and end-point devices.

Jean-Philippe Deby,
BDD, Europe, Genetec Inc.

GDPR + Video Surveillance

What is GDPR?
The General Data Protection Regulation (GDPR) is a set of rules for personal data processing operations on EU residents. The risk-based approach to data protection will ensure that organizations do not compromise the fundamental rights and freedoms of individuals as applied to their data.

This is the biggest change to European data protection since 1995.

What do you need to know?

- Under the regulation, data controllers must:**
 1. Assess the level of risk posed by their processing operations against the fundamental rights and freedoms of individuals.
 2. Mitigate their data protection compliance accordingly.
- By the end of 2018, more than 80% of companies affected by the GDPR will not be in full compliance with its requirements.** - Gartner
- Fines can reach 4% of annual turnover or €20 million whichever is greatest.**
- Personal data includes:**
 - Name
 - Home address
 - Photos
 - Bank details
 - Social networking posts
 - Medical information
 - IP address
 - Mobile device ID
 - IoT collected data

How GDPR affects video surveillance

Large scale public video surveillance is considered to be a 'high-risk processing operation'. Data controllers performing video surveillance in the EU will have to comply with the provisions in the GDPR relating to privacy, data protection, and the identification, management, and mitigation of risks.

- Right to access:** Provide individuals request access to their self-surveillance system with direct access to their information.
- Right to be forgotten:** Individuals can ask for their data to be erased, object to processing, or restrict the processing of their data.
- Breach notification:** Data breaches must be reported within 72 hours after the data controller first becomes aware.
- Privacy by design:** Encryption and anonymization of video footage should be built into the system in any system design.

Genetec | Read our comprehensive white paper at genetec.com/GDPR-white

Join the global security conversation.

As of 2018, it is IFSEC's commitment to become the place to facilitate every member of the security profession in creating a safer world.

More than just a prominent trade show, IFSEC will foster the global security conversation, set and carry the agenda and be the platform to broadcast the safety and security dialogue.

2018 will be the inauguration year of a transformation of IFSEC's 40 year heritage as a physical security show into a high level security summit and integrated security event.

This is not IFSEC as you've ever known it before.

IFSEC
INTERNATIONAL

19-21 JUNE 2018
EXCEL LONDON UK

Secure your place at:

WWW.IFSEC.EVENTS



IHS Markit has presented their prediction for the global video surveillance market.

Top video surveillance predictions for 2018

London, UK

From artificial intelligence and deep learning to advances in privacy protection, far-reaching video-surveillance innovations are cropping up around the world. New trends continue to change the way consumers, businesses and machines interact, while also spurring the next revolution in security industry growth, according to a new white paper from IHS Markit, a world leader in critical information, analytics and solutions.

IHS Markit analysts were asked to provide their informed predictions for the global video surveillance market in the new year. The major trends to watch in 2018, as identified in this IHS Markit white paper, are as follows:

1. Artificial intelligence and deep learning

Driven by the research-and-development investment from chip vendors, software startups and major video surveillance vendors, deep learning video analytic algorithms have been developed into fully deployable products, with user-friendly interfaces and scenario-focused solutions. For example, deep learning face-recognition algorithms are now available in search-engine applications designed to find missing people from video footage. Vendors that market vertically-focused deep learning applications aligned with their own existing portfolios should have good opportunities to grow.

2. Privacy and GDPR

In 2018, there will be an increase

in the wider discussion about privacy and how the video surveillance industry protects the data it gathers. Much of this discussion will stem from the new European Union (EU) General Data Protection Regulation (GDPR) which will become law across EU member states (including the UK) in May 2018. GDPR will replace each EU member state's own version of data protection law and is likely to increase public awareness about the rights ordinary citizens have regarding their own personal data protection. With a wide-ranging scope covering many industries, GDPR also has specific coverage for video surveillance data.

3. China versus the rest of the world

China is forecast to account for almost half (46 percent) of global professional video surveillance equipment revenue in 2018. However, the Chinese market has some unique characteristics that differ from other regional markets. Essentially, there are two markets

for video surveillance equipment: the Chinese market and the rest of the world.

4. Drone detection technologies

Consumer drones are readily available for just a couple of hundred dollars and flown by anyone, with no prior training and without a license. Thus, the problem of drones in restricted air space has become an increasing concern. Given the large physical area these restricted air spaces cover, simply being able to identify a nearby drone has proven challenging. Recent developments in drone detection technology mean that anyone wanting to secure a perimeter in 2018 will have to take into account the threat from above.

5. Video surveillance fault tolerance

Compared to the IT industry, the video surveillance industry is often viewed as having a relaxed approach to many aspects of failover and redundancy. However, as the multiple uses and perceived value of video surveillance data increases,

we can expect to see increased demands for greater failover, redundancy and backups from end-users.

6. Forensic video analytics as a service

Forensic video analysis has been available for some time, yet the improvement in accuracy provided by deep-learning technology over the past two years has been instrumental in delivering a level of competency reliable enough to assist human analysts. We can expect to see increased convergence in post-recording video repositories, where multiple video sources are brought together and investigated using deep-learning video analytics.

7. The Xue Liang programme

The Xue Liang programme aims to connect all the video surveillance cameras installed in Chinese districts, towns and villages to a central surveillance platform at the county and national levels -- and build a comprehensive mechanism for video data sharing across law enforcement, emergency services and other government agencies. More traditional video surveillance vendors are expected to add data centre-ready hardware and cloud-enabled offerings to their portfolios, in order to meet the technology requirements of this programme.

Market drivers for the IoT defined

London, UK

Driven by the need for intelligent connected devices in industrial and commercial applications, the number of connected Internet of Things (IoT) devices globally will grow to more than 31 billion in 2018, according to new analysis from business information provider IHS Markit.

In its latest IoT Trend Watch report, IHS Markit identifies four key drivers and the trends that will impact the IoT this year and beyond:

Innovation and competitiveness

The IoT opportunity has attracted numerous duplicative and overlapping wireless solutions such as Bluetooth, Wi-Fi, 5G, NB-IoT, LoRa and Sigfox. Standards consolidation lies ahead, but confusion and fragmentation will dominate in the near term.

Enterprises are leveraging the location of data as a competitive

advantage — and as a result, a hybrid approach to cloud and data centre management is taking hold. More and more companies will employ both on-premises data centres and off-premises cloud services to manage their IT infrastructure.

Business models

5G builds upon earlier investments in M2M (machine-to-machine) and traditional IoT applications, enabling significant increases in economies of scale that drive adoption and utilisation across all sectors of industry. Improved low-power requirements, the ability to operate on licensed and unlicensed

spectrum, and better coverage will drive significantly lower costs across the IoT.

Cellular IoT gateways, which facilitate WAN connectivity, will be integral to edge computing deployments. 2018 will bring increased focus on compute capabilities and enhanced security for cellular IoT gateways.

Standardisation and security

Cyber security is a leading concern for IoT adopters. IoT deployments face critical cyber security risks because there are potentially many more IoT devices to secure compared to traditional IT infrastructure devices, presenting increased risk to traditional communications and computing systems, as well as physical health and safety.

Despite the promise it holds, blockchain — a technology for securely storing and transferring data — is not a panacea. Initially,

IoT applications for blockchain technology will focus on asset tracking and management.

Wireless technology innovation

IoT platforms are becoming more integrated. Currently, there are more than 400 IoT platform providers. Many vendors are using integration to compete more effectively, providing highly integrated functionality for IoT application developers and adopters.

Significant innovation will occur when IoT app developers can leverage data from myriad deployed sensors, machines and data stores. A key inflection point for the IoT will be the gradual shift from the current “Intranets of Things” deployment model to one where data can be exposed, discovered, entitled and shared with third-party IoT application developers.

VARIO2 Go The Distance



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

Part 1

IoT & security systems: ID and access control

What implications does IoT have for ID and access control and how can it strengthen the end-users' business? How can you address the security issues that come with IoT?

Detektor IoT Academy had a closer look at how ID and access control and IoT can create business opportunities for vendors and provide major benefits for the end-users.

If digitalisation was/is the latest paradigm shift in access control and ID verification, then Internet of Things is the next. And it has already begun, not least in the consumer market with a lot of "smart" online products which are part of the smart home. That market is driven by convenience – it is easy to control your thermostat, security cameras or unlock doors from your smart phone. The corporate market on the other hand, is driven by efficiency and the potential to save money. Sensors can detect when machines or devices differ from the norm and thanks to an increased information flow, companies can react proactively and avoid expensive shutdowns. Another example is that sensors can detect if rooms are empty and if so, ensure that the lighting is not on.

Some advantages with IoT-based ID and access control:

- Increased convenience for the end customers
- Much more detailed information – for example, continuous minute information and status control
- Provides the opportunity to act more proactively
- Cost-effective – requires fewer service visits and it is more environmentally sustainable
- Greater flexibility – easy to issue and change access and access levels
- The ability to use workplaces more efficiently through ID information, which knows where people are and where they are empty spaces

Risks and cyber security

The Internet puts new demands on security, and it applies even more to IoT. The more things and devices that are connected, the greater the security challenges. Systems and components are exposed in a different way, and physical and logic access are increasingly merging. The IT security level of computers is relatively high, but almost non-existent for smart home products. Even access control systems are lagging behind, several of the most popular cards have been hacked a long time ago, but they are still being sold.

Cyber security in practice

There is an increasing demand on manufacturers of security product to give each product a unique ID already from the start. For ID verification, it has become clear that only username and password are not sufficient.

Two-factor authentication, such as the Bank ID – which requires two different factors to log in: a mobile app and a pin – have become more common. Another method is adaptive authentication, which means that the circumstances determine what the user needs to do in order to login. If the user is in the office, perhaps only the password is required, but if the system can use geo-positioning to determine that the user is at another location, or if the login is made from another device, the system may require two-factor authentication to ensure that it is not someone else that is trying to get access.

Traceability is a key word for increasing cyber security: By assign-

ing unique ID's to all

devices and users, security can be significantly improved and actions can be derived and tracked

both in real time and afterwards. It brings clarity to who is responsible for what, something that often is a weakness in a IoT system.



Detektor and Securityworld-market.com has produced a series of educational articles on IoT and security systems in collaboration with some leading players within different security technology fields. Here are part 1–3.

CHECK LIST FOR MANUFACTURERS, DISTRIBUTORS, SYSTEM VENDORS AND END CUSTOMERS

MANUFACTURERS:

- Security should be a basic component already at the design stage of a product or a service and throughout the process
- Consider providing all devices with some kind of transport ID, which is an ID that can be further used in the future
- Stop making readers with old and already hacked technology, such as EM and Mifare readers

DISTRIBUTORS:

- Dare to demand requirements regarding standards for communication between card readers and above in order to secure a chain of encrypted communication
- Do not sell old systems with non-secure card readers

SYSTEM VENDORS:

- Find out what end customers really need. What features make their business smoother and safer and how can the solution contribute to increased profitability?
- Package services and create a suitable business model based on the above
- Consider security when connecting the devices and who is going to access the information
- Do not install a security system that lacks secure access management. This requirement can be put on the system owner/end customer
- Suggest/require the use of two-factor authentication and logs
- Select a manufacturer that fulfils the above

END CUSTOMERS:

- Select a proper ID and access control solution with good security
- Make a risk analysis before purchasing a solution
- Stronger identities provide better traceability
- Use digital signatures or multiple layers of security to secure identities – it is much better than passwords
- With signed logs (that can show who gave permission at a certain time) it becomes difficult to question whether something has happened or not and who was responsible
- Avoid manual processes for access – it should be done dynamically and automatically, for example when an employee quits and his/her access should be deleted

Source of information: Detektor has used expertise from Nexus Group – a Nordic market leader and IT security specialist in Public Key Infrastructure (PKI) and Identity Management – as a source of competence.

Part 2

IoT & security systems: Alarm communication

Internet of Things opens up a world of opportunities, but also a number of new security risks. Detektor IoT Academy had a closer look at how secure IoT communication can make business more efficient for companies within the alarm industry, and how IoT creates opportunities for selling services and offering benefits to end customers.



Society is undergoing digitalisation and everything that can be connected will eventually be connected. This applies to all businesses, including the alarm industry. Analogue alarm transmission will be phased out and the development is driven towards IP-based communication. With the help of IoT, companies can make their business more efficient and reduce costs. The technology makes it possible to remotely monitor and control alarm equipment and it creates conditions for offering new digital services.

Advantages with IoT-based alarm communication:

- It is future-proof and you will be updated to society's digitalisation – analogue technology is about to be phased out
- Cost-effective – streamline operations through, for example, status control, remote monitoring and remote service and reduce the number of dispatches
- Convenient for the customer as well as the ability to manage and control devices
- Automatic data retrieval – big data can create better processes for the end customer
- It creates possibilities for offering more services

Secure IoT communication provides great opportunities. You can collect data, manage, control and get information from your connected devices. Imagine a detector in an intrusion alarm system in the countryside (or far away from the person responsible for it) stops working. In the old analogue world, the only solution was to send out a technician who had to drive there and check the detector,

something that took a lot of time and did cost a lot of money. In an IoT system, you can check the control panel remotely, analyse and troubleshoot and see if it is possible to fix the problem without having to send out a technician.

The same principle applies if there are camera images being sent. Instead of picking them up, you connect to a server and download the images. Users can analyse large amounts of data, known as big data, and thus create processes and better offerings to their customers.

In order for a system vendor to develop its business and learn how to package and offer services instead of just selling products, it is important to try to get into the mind of the end customers and ask oneself what they really want. Why do people buy an intrusion alarm? Well, to avoid intrusions that costs money. The essence here is to stop worrying and be able to sleep well at night – to get “peace of mind”. This is the service that the system vendor should offer.

Risks and cyber security

As the number of connected devices is increasing, security risks also increase. Hackers often attack the interfaces between a device and the communication itself because that is where the weakest spots normally occur.

An advantage of secure communication is that you can notify/send an alarm when something differs from the norm – for example if the amount of data sent greatly increases or stops. Then you can locate the problem before it gets worse. If you have unprotected IoT devices connected via a 3G or 4G mobile phone subscription, it can become very costly if they

get hacked. If a device is used in a DDoS attack, it can generate multiple gigabytes of data, which can result in very expensive bills for your business.

In the autumn of 2016, a lot of companies and organisations were struck by the Mirai botnet. A massive amount of hacked IoT devices were used to carry out the attack and recently it has been reported

that there are signs of a new, larger attack with an army of hacked IoT devices that may take place soon. If you do not want your IoT devices to participate in attacks like that; protect them. The most important thing to do is to make sure that the devices are not visible on the Internet at all and a minimum requirement is to make sure you update software.

CHECK LIST FOR MANUFACTURERS, DISTRIBUTORS, SYSTEM VENDORS AND END CUSTOMERS

MANUFACTURERS:

- Do not sell products with technology that will be phased out soon
- Educate system vendors and end customers in cyber security
- Communicate the necessity for end-users to always install the latest version of software and firmware

SYSTEM INTEGRATORS:

- A good supplier has extensive knowledge and educates the customer in what is required in order to maintain a good level of security
- Demand secure, robust communication solutions
- Critical systems must have backup and redundant transmission paths
- Develop your business and become a service provider: get paid for the functionality offered by the solutions, not just for the products themselves
- Ensure that the right people have access to the communication
- Invite end customers to update their software

END CUSTOMERS:

- Make sure the communication solutions you use work and that the communication does not fail without you receiving a message or a warning
- Have a discussion with vendors of secure solutions and ensure that the services you have purchased had security built-in from the start
- Replace the default password in your IoT device: use lower-cases, capital letters, numbers, and special characters
- Close unused ports and services in devices and servers
- Be sure you always install the latest versions of software and firmware
- If you consider it to be necessary: demand alarms when there are abnormal changes in transmitted data
- In order to protect a device from unwanted traffic, it is important to use a firewall and/or IP filtering.

Source of information: Detektor IoT Academy has used Addsecure, a company that works with securing alarm communications and other critical communication – as a source of competence

Part 3

IoT & security systems: Video surveillance

Security cameras have all the capabilities to play a central part in the Internet of Things since they not only deliver images, but also can gather and analyse large amounts of data. Detektor IoT Academy takes a look at how video surveillance and IoT can create business opportunities for vendors and provide end-users with major benefits.

There are many factors that drive the development towards IoT in video surveillance. Not least, it is about business and customer benefits.

Some advantages of IoT-based video surveillance:

- Convenience for the end customer
- Cost-effective and more environmentally sustainable
- Greater end-user functionality and integrators can enhance their service offer
- Great opportunity to use and analyse data
- It provides the opportunity to work proactively

Surveillance cameras should be seen as sensors that can solve problems and generate data and statistics (through video analysis) that others, other than security managers can benefit from. Instead of being used as a retroactive tool, for example in order to identify a shoplifter afterwards, cameras can be used proactively to detect if someone enters an area at night or calculate how many people pass a certain point. IoT systems also contribute with cost-effectiveness and create added value, for example, the end customer can check status and take measures remotely. In addition to saving time and resources because of less staff call outs, it can also mean energy savings and a reduced ecological footprint.

What delays the development of IoT?

The share of IP-cameras versus analogue cameras varies in different places in the world. If there are a lot of analogue cameras, it is hard to be part of an IoT world. It is said that the physical security industry is being "ITfied", but the security industry is far behind the

IT industry where for example patches and software updates have been natural for a long time. Many people have installed their security cameras on dedicated networks and may not dare to adapt to an IoT world. In addition, they may not have enough knowledge about network infrastructure.

Risks and cyber security

Security cameras and video surveillance are the part of the physical security industry that was first digitalised – Axis Communications launched the world's first network camera in 1996 – and has long been part of a connected system. At the same time, security cameras have been used in several major cyber attacks in recent years, including DDoS attacks against sites such as Twitter and Spotify. These hacker attacks have increased the manufacturers' awareness of cyber security and they are focusing more and putting more resources on securing their cameras.

Cyber security in practice

Cyber security is a time-consuming process – not a product. Some end customers may think the risk is not big enough compared to the time it takes to secure their networks. Security cameras are almost always part of a larger system and the IT security is no better than the system's weakest link. It may be a camera but it might as well be the ventilation system. Securing IoT-based video is thus no guarantee to avoid hacker attacks. Everyone must take their responsibility.

There is no obvious training or standard for network access in many countries in the physical security industry today. Security cameras are usually only a small part of the end customers' network

and there are often other things in the network with higher priority. Therefore, it is important for camera suppliers to listen to how end users are using their networks.

The physical security industry has long enjoyed high margins on hardware, while the IT industry created business models based on service and updates many years ago. In the future, the physical security industry is expected to follow and then, the entire life span of a security camera will

become more important.

What will happen in two or five years? One important question to ask is how a camera system will be updated and that is absolutely crucial for cyber security. Software and firmware updates may also be the single most important thing in the camera manufacturers' hardening guides, which are often also about not using open ports, using good, secure passwords and demanding additional authentication if the devices are being attacked.



CHECK LIST FOR MANUFACTURERS, DISTRIBUTORS, SYSTEM VENDORS AND END CUSTOMERS

MANUFACTURERS:

- Cyber security should be a factor already in a product's design stage
- Listen to how end users are using their networks
- Notify how loopholes should be secured
- Train distributors, integrators and end customers in cyber security

SYSTEM VENDORS:

- Make sure you have extensive knowledge about network infrastructure
- Tell end customers to update their camera systems
- Find out what the end customers really need. What features make their business smoother, and safer and how can the solution contribute to increased profitability?
- Offer services and create a suitable business model based on the above
- Have an active dialogue with the manufacturers, as many of them have various types of technological possibilities to create a service offering together with you

END CUSTOMERS:

- Consider what problems the camera system can solve and what added value it can create
- Demand training in cyber security – not least considering the EU data protection regulation GDPR, which will come into force in May 2018
- Read the manufacturers' hardening guides and spend time on securing the network
- Update your camera system
- Choose an open system so you have the option to change supplier

Source of information: Detektor has used expertise from Axis Communications for this article.



Exhibit Hall: April 11-13, 2018
SIA Education@ISC: April 10-12, 2018
Sands Expo | Las Vegas
www.ISCWest.com

**COMPREHENSIVE
SECURITY FOR A
SAFER, CONNECTED
WORLD**

REGISTER FOR FREE TODAY!

ISC WEST is THE largest converged security event in the Americas. At ISC West you will have the chance to network with over 30,000 physical and IoT security professionals through forward-thinking conference sessions and countless networking events, plus the opportunity to meet over 1,000 exhibitors and brands featuring the newest products revolutionizing the security industry.



Discover the latest security products, technologies & solutions - featuring a NEW Emerging Technology Zone, and more!



Direct access to 1,000+ leading exhibitors & brands that are transforming the security industry.



Enhance your knowledge at 85+ SIA Education@ISC Sessions covering cybersecurity, intelligent physical security, IoT and more!



Build your network and share experiences with 20,000+ Physical, IoT and IT Security buyers.

FEATURING:



&



www.iscwest2018.com/Detekor-International

BUSINESS PEOPLE



Daniel Lee joins Genetec in new executive position, as APAC MD

New APAC MD for Genetec Montreal, Canada and Singapore

Genetec Inc. has appointed Daniel Lee as Managing Director for its Asia Pacific (APAC) region. Lee will be in charge of managing sales and strategy to bring the company's unified IP security solutions to broader APAC markets.

Lee's responsibilities will include leading a growing team of sales, support, training, and marketing professionals to achieve continued growth and innovation across the APAC region and expand into new markets.

Lee is a seasoned IT industry entrepreneur, CEO, angel investor, and board member. For 19 years, he grew his own IT and Physical Security services distribution business called Lan 1, which was acquired by Hills Limited, Australia, in 2012. Lee joined Hills as an advisor to the board and served as Head of Product Practice until 2016.

Lee will be based in the Genetec Singapore office, traveling extensively throughout the APAC region.

"Daniel brings many years of experience and a fresh determination and drive to expand Genetec solutions for security, intelligence, and operations to the APAC market," says Guy Chénard, Vice President, Global Business Development and Sales at Genetec.

Securitas kicks off 2018 with a trio of acquisitions

Stockholm, Sweden

Securitas is already strengthening its global position in 2018 with the acquisition of three electronic security technology companies, S ddeutsche Bewachung in Germany, Automatic Alarm in France and Johnson & Thomson in Hong Kong.

Firstly in Germany, Securitas has acquired all shares in the security solutions company S ddeutsche Bewachung with an enterprise value estimated at MSEK 80 (MEUR 8.2).

S ddeutsche Bewachung has annual sales of approximately MSEK 95 (MEUR 9.6) and 300 employees. The company offers on-site, mobile and remote guarding in the Rhein-Neckar area in the south-west of Germany, with headquarters located in Mannheim. The company has a very solid customer portfolio, comprising many customer segments. With this acquisition, Securitas strengthens its position in this area of Germany.

In France, Securitas has acquired all shares in the electronic security company Automatic Alarm at an enterprise value of approximately MSEK 430 (MEUR 44).

Automatic Alarm is a nationwide system integrator and installer of electronic security solutions, including intruder systems, video surveillance and access control, with multiyear maintenance contracts. The company, with 250 employees, has annual sales of approximately MSEK 370 (MEUR 38).

"The acquisition is in line with our Group strategy to integrate electronic security into our on-site and mobile security solutions offerings. This major acquisition positions Securitas as a significant player within electronic security and it strengthens us as the market leader in France", says Securitas President and CEO Alf G ransson.

And Finally, Securitas has acquired the technology and installations company Johnson & Thompson in Hong Kong. With this acquisition, Securitas strengthens its position to deliver value added security solutions to



Securitas President and CEO Alf G ransson.

customers in Hong Kong. The enterprise value is estimated to MSEK 46 (MHKD 43).

Johnson & Thompson is a monitoring, maintenance and installation company focused on the retail and mid-sized corporate market in Hong Kong. The company has 22 employees and annual sales of approximately MSEK 17 (MHKD 16). With this acquisition, Securitas continues to strengthen the ability to optimise security solutions, covering a combination of on-site guarding and remote guarding, mobile, monitoring and electronic security services to its customers in the AMEA region.

Dahua 2017 revenue growth reaches new high

Hangzhou, China

Zhejiang Dahua Technology Co., Ltd. or **Dahua**, has released its unaudited preliminary earnings estimate for 2017, indicating that the revenue reaches CNY 18.852 billion, a year-on-year growth 41.44%.

In 2017, Dahua achieved a gross revenue of CNY 18,852,104,991.81 (approx USD 2.89 billion) representing a year-on-year increase of 41.44%. Total profits reached CNY 2,633,776,603.92 (USD 403.08 million), a year-on-year growth 30.88%. Net profit attributable to shareholders of listed companies reached CNY 2,378,228,515.67

(USD 363.97 million), growing 30.30% year on year.

In referring to the charts on the right: The data in the upper chart is completed based on the company's consolidated statements; the lower chart shows the digits that Dahua calculated corresponding with accounting procedures based on matters in relation to the repurchase and write-off of certain restricted stocks during the reporting period. The total share capital of Dahua has been changed from 2,899,411,405 to 2,898,756,130 shares.

The increase resulted mainly from the following factors: the mar-



ket sentiment continued to rise; the company expanded the market and met new demands with enhanced comprehensive solutions and services; the company strengthened internal control to achieve steady growth in sales and simultaneous growth of net profits.

During the reporting period, the total company assets increased by 40.05% and the net assets increased by 27.09%, mainly due to the increase in the scale of operations and rising profits.

Acquisition extends Assa Abloy reach in ME & UK

Stockholm, Sweden

Assa Abloy has acquired Dale Hardware and Excel Architectural Hardware through its acquisition of the Progress Ventures Group ("Dale & Excel"). Dale & Excel are the leading suppliers of architectural hardware to builder's merchants in the UK.

"I am very pleased to welcome Dale & Excel into the Assa Abloy Group. Dale & Excel offer a comprehensive portfolio of architec-

tural hardware products that effectively complement and extend the Assa Abloy offering in the UK and Middle East markets," says **Johan Molin**, President and CEO of Assa Abloy.

"Dale & Excel are an exciting addition to our UK business. It offers an extensive high quality range of architectural hardware products with a strong track record of innovation. Their portfo-

lio will extend the Union offering into the commercial market in the UK", says **Tzachi Wiesenfeld**, Executive Vice President of Assa Abloy and Head of the EMEA division. "

Dale was established in 1974 and has its headquarters near Leeds. The business has approximately 70 employees and sales for 2018 are expected to reach around £19 million.



Johan Molin, President & CEO, Assa Abloy.

Addsecure continues growth strategy with new acquisition

Stockholm, Sweden

Addsecure is strengthening its Nordic presence further by acquiring the alarm communication business of Finnish Prevent 360, majority-owned by private equity firm Intera.

This part of Prevent 360 provides a range of alarm transmission and monitoring services and has

a substantial share of the market for transmission of fire alarms in Finland.

"Finland is a strong and growing market for advanced technology. As Addsecure has extensive experience within the security industry and a tradition of adapting to market needs, we see a strategic

fit. We are very pleased to combine our two businesses and leverage our collective resources and expertise to accelerate growth", says **Stefan Albertsson**, CEO of Addsecure.

Addsecure will continue with the well-established service concept that Prevent 360 has developed. As part of the transaction, the com-

pany announced that the current local Prevent 360 team will become part of the Addsecure organisation and that a new entity, Addsecure Oy, is being established.



Stefan Albertsson, CEO at Addsecure.

SIA NEW PRODUCT SHOWCASE WINNER
Network Support Solutions
KBC Networks Limited
2017 ISC WEST

KBC data delivered

Ethernet Switches • Wireless • Secure Wan • Fiber Optic • IP over Coax • Power Solutions



Industrial Switches and SFPs



Long Range IP over Coax and UTP



Gigabit Wireless



Secure Video Streaming over 4G



Extensive Fiber Solutions



UPS, Solar and Wind

KBC Networks: Transmission Solutions built to perform in non-conditioned environments

kbcnetworks.com

Axis new VP for EMEA region

Lund, Sweden

As vice president for Europe, Middle East and Africa (EMEA) Verena Rathjen will take responsibility for Axis' long-term success in the region and ensuring the strategic direction of the company's expanded solution offering in a growing market.

"The EMEA region is big and diverse, and shows a lot of opportunities. Verena Rathjen will have vital role in driving the

strategic expansion of Axis' business in this market and working together with very strong regional management teams," says Bodil Sonesson, vice president for global sales at Axis.

Previously to joining Axis, Verena Rathjen's most recent



Verena, new VP for EMEA at Axis Communications

position was as vice president at global lighting company Ledvance, where she was responsible for the global Smart business and defining portfolio and business strategies for the LED business in Europe.

"My ambition and passion is to work

with skilled and smart people to drive business growth and create value for our society. Axis' vision to contribute to a smarter and safer world is in that matter highly relevant, and the strong company values were an instant fit to mine. I am therefore excited to further develop our portfolio across EMEA to create value for our customers and all of us in our daily lives," says Verena Rathjen.

Motorola Solutions to acquire Avigilon for 1 billion dollars

Vancouver, Canada

Motorola Solutions (NYSE: MSI) has entered into a definitive agreement to acquire Avigilon (TSX: AVO) in an all-cash transaction that will enhance Motorola Solutions' portfolio of mission-critical communications technologies.

Motorola Solutions will acquire all of Avigilon's outstanding shares for CAD\$27.00 per share. The enterprise value of the transaction is approximately US\$1.0 billion including Avigilon's net debt.

Based in Vancouver, Avigilon designs, develops and manufactures advanced security surveillance solutions, including video analytics, network video management software and hardware, surveil-

lance cameras, and access control solutions. The company holds more than 750 U.S. and international patents.

"This acquisition will bring Avigilon's advanced video surveillance and analytics platform into public safety, while expanding our portfolio with new products and technologies for commercial customers," states *Greg Brown*, chairman and CEO, Motorola Solutions. "Video can play a powerful role in creating safer cities and thriving businesses. It can serve as highly efficient 'eyes and ears' for monitoring a given location, and advanced video analytics can proactively alert officials to a perimeter breach or quickly

find a person who left behind an object of interest."

As more cameras feed into public safety workflows, video surveillance and analytics will enable more public-private partnerships between local communities and law enforcement. The acquisition will also enable Motorola Solutions to extend into new segments of its commercial markets business, which provides secure, reliable communications technology to industries such as oil and gas, transportation, utilities, manufacturing and higher education. Customers will now be able to purchase advanced security and surveillance solutions as part of Motorola Solutions' portfolio of



Greg Brown, chairman and CEO, Motorola Solutions.

critical communications technology for commercial markets.

The transaction is expected to be completed by the end of the second quarter of 2018, subject to customary closing conditions, including regulatory, shareholder and court approvals.

Motorola signals more Safe City activity with Avigilon acquisition

London, UK

Jon Cropley, principal analyst, video surveillance at **IHS Markit** explores Motorola's motives for moving into the video surveillance market place.

Cropley suggests that Motorola's focus on public safety projects is likely to have been a major motivation for the acquisition. City surveillance is an important element of public safety. Professional video surveillance equipment revenue has been growing faster in the city surveillance sector

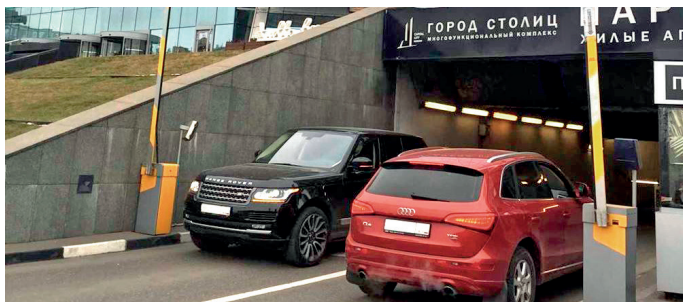
than in the rest of the market in recent years. IHS Markit forecasts this will continue, with the city surveillance sector growing at a compound annual growth rate (CAGR) of 11.1 percent to 2021 — and the total market growing at a CAGR of 6.8 percent.

IHS Markit also estimates that Avigilon was the eighth largest supplier of professional video surveillance equipment in 2016 with over 2 percent of a global market worth \$15.4 billion.

"The announcement to acquire Avigilon comes after a string of acquisitions by Motorola over the past three years," says Jon Cropley and mentions some notable recent acquisitions such as the UK Tetra operator Airwave, the US-based 911 business of Airbus DS Communications, Kodiak (a push-to-talk provider) and Spillman (a public safety software provider). Given these deals and planned acquisition of Avigilon, it's clear that Motorola is aiming to increase activity in

the wider public safety and 'safe city' market, moving beyond its emergency communications focus of the past. Traction of national public safety broadband networks such as ESN and Firstnet, which facilitate video integration, further support this strategic play."

IHS Markit estimated Motorola held approximately 7 percent of the nearly \$5 billion command and control technologies and services market in 2017, making it the largest supplier to this market.



AAM Systems and Nedap bring parking to a high security level in Moscow.

Moscow turns to advanced vehicle access from Nedap

Groenlo, The Netherlands and Moscow, Russia

Capital Group, a leading Russian real estate investor company, cooperates with the security company AAM Systems to implement a proven security concept at various buildings in Moscow.

The solutions include the most advanced systems for security, access control and parking for their newly constructed buildings. For vehicle access control in OKO Towers, Capital City Towers and Capital Plaza, AAM Systems implemented Nedap's long-range RFID platform Transit in order to ensure fast and secure vehicle and driver identification.

Capital Plaza is a modern multi-tenant business centre located in the heart of Moscow. Designed to be a high-class multi-tenant facility for companies headquartered in Moscow, Capital Group asked AAM Systems to integrate Apollo Lyrix for access control and the Nedap long-range RFID for automatic driver based vehicle access to the car park. With this integrated security solution AAM systems offers Capital Group a proven concept that manages both building and parking access control in a highly secure yet user-convenient manner.

In order to optimise vehicle access control at the entrances and exits of the parking facility, Nedap's Transit readers were installed. This long-range RFID reader identifies vehicles and its drivers up to 10 metres. Transit supports simultaneous identification of

both the vehicle and driver.

Nedap's patented Smartcard-Booster RFID transponder ensures that vehicles only can enter and leave the parking facility when the vehicle is occupied by an authorised driver. Within the Transit long-range RFID platform, the Smartcard-Booster supports reading of HID iClass 13.56 MHz smart card technology. HID Iclass is the card credential applied for access control to the Moscow Capital Plaza complex.

The Booster is the perfect solution to closely monitor all activities of vehicle and driver combinations. With the Booster onboard of the car, both the vehicle and driver are identified simultaneously. The transponder contains a unique vehicle identification number, but is also a multi-technology card reader. When the HID Iclass card is inserted in the Booster, it reads the drivers' personal ID.

"We are delighted to have the proven technology from Nedap on board. Nedap develops truly unique solutions for vehicle access control. Transit is a reliable platform for long-range and secure data transmission. The system is easy to install, commission and integrate. Additionally, under all extreme environmental conditions and weather circumstances, Transit performs accurately. Supporting reading multi-technology cards allows Capital Group to use the issued HID Iclass cards. With Nedap, we are able to bring parking to the high security level required," says Vadim Borisov, CEO of AAM Systems.

TAKEX



PRE-ASSEMBLED BEAM TOWERS

- Active Perimeter Detection +
- Up to 200m coverage +
- 2 & 3 Beam configurations +
- Pre-wired and assembled +
- Cost save on installation +

+44 (0)1256 475555
email: sales@takex.com

TAKEX EUROPE
www.takex.com

The electronic peri

Terrorism is the main driver in the perimeter protection market. Detektor met up with some of the leading physical security manufacturers to find out more about this market and to hear about the most efficient technologies for securing perimeters.

The market: “A phenomenal growth”

Research shows that the perimeter protection market is forecasted to grow at a Compound Annual Growth Rate of 12.2 per cent until 2022. The security professionals interviewed in this article also have positive views of this market.

“With the added threat of terrorism, and the atrocities that we have seen over the last few years, perimeters have become more and more important to protect”, says Axis co-founder Martin Gren.

By Henrik Söderlund

The market for perimeter security is expected to reach 196.60 billion USD by 2022 according to Marketsandmarkets. The growth of this market is primarily driven by the rise in terror attacks worldwide. Marketsandmarkets claim that the technological developments in video surveillance have fuelled the demand for perimeter security systems and services and the increased usage of the Internet of Things is also expected to contribute to this growth.

Vanderbilt's CEO Joe Grillo says: “I think perimeter protection has always been an important part of an overall integrated security system, as the perimeter can relate to a number of things, your building, your premises or your entire corporate campus or university campus or an airport or a government facility, so I think that has always been an important part of a total integrated solution.”

A phenomenal growth

Axis co-founder Martin Gren says: “Perimeter protection is very much a growing vertical, I mean,

with the added threat of terrorism and the atrocities that we have seen over the last few years, perimeters have become more and more important to protect. We have seen a phenomenal growth in that segment.”

Dahua's Marketing Manager for Overseas Business, Jiaqi Gao, also stresses there is a rising demand for perimeter protection: “I think especially in the EMEA market and in the American market, it is driven by the people's security consciousness and the safety of the people. Generally we think it is quite a big market”, he says.

Video surveillance leads the way

Today, there are many technologies that can be used for perimeter protection. According to Marketsandmarkets, the video surveillance systems segment is estimated to lead the perimeter security market to 2022. It is claimed that “the increasing use of video surveillance systems, especially in the commercial and services, industrial,



Axis co-founder Martin Gren.



Vanderbilt's CEO Joe Grillo.

and military and defence verticals for protecting the organisation of assets is said to be enhancing the growth of the video surveillance systems segment in the perimeter security market”. Other segments are perimeter intrusion detection systems, access control systems, alarms and notification systems, and others such as fencing, lighting, and detection devices for metals, explosives, drugs, and chemicals.

be able to detect a drone, but once you detect them you also need to take action, and I think this is still in its infancy, but it is the number one issue for many security companies and security managers.”

Jiaqi Gao from Dahua stresses that the increasing number of drones has added complexity to perimeter protection. He says: “Previously you only needed to take care of the vertical area, now you also need to take care of the

“I think perimeter protection has always been an important part of an overall integrated security system.”

According to Marketsandmarkets, the North American perimeter security market is expected to dominate until 2022. The growth will be attributed to the increasing need for security against terrorist activities, as well as government regulations for safety and security, technological developments in physical security solutions, rising illegal immigration, and increasing criminal activities.

Drones change the market

Previously, perimeter protection was all about what is happening on the ground, but today, with the booming number of drones, more and more perimeter protection applications need to consider the threat drones could pose. Martin Gren believes the increasing number of drones being used will effect the use of perimeter protection. He says: “Well, you want to

horizontal area. It has become more spatial. There are some anti-drone technologies available in the market, and especially for high security areas, like airports.”

Mission availability problem

Could drones be used for protecting the perimeter? Genetec CEO Pierre Racz is sceptical.

He says: “Drones must be properly engineered into a security system. An example of an improper engineering of drones is to expect drones to do autonomous patrols of a perimeter. A good example of the use of drones is having piloted drones to do spot inspections of roofs and other difficult to access locations.”

He also stresses that there is a mission availability problem with drones; after using them they need to be charged for a longer time than they were up in the air.



Dahua's Marketing Manager for Overseas Business, Jiaqi Gao.



Genetec CEO Pierre Racz.

perimeter protection

Industry leader's views on the fast growing sub-market

The technology: Is video analytics good enough?

Radar, thermal cameras and intrusion detectors are some of the most common technological solutions for securing perimeters. But the most heated debate is about video analytics.

"You cannot rely on video alone for perimeter protection", says Genetec CEO Pierre Racz.



Keen Yao, Vice President of Hikvision's International Business Center.



William Ku, Vice President, Brand Business Division, Vivotek.

It is a debated point as to whether video analytics should be used for perimeter protection. Tim Biddulph, Head of Product Management at Hanwha says: "The problem with video analytics is, in the real world, perimeters change. The world is not a clean environment, so increasingly, we are getting closer to the point where analytics at the edge is able to offer reliable perimeter protection."

He claims the industry has been able to use video analytics for perimeter protection in expensive systems and in really clean environments for years, but not as a general solution.

"The requirement and the cost have never really got close. But now, we are starting to get much closer to be able to implement reliable perimeter protection in the real world at a more cost effective rate", Tim Biddulph says.

Boudewijn Hak, Regional BU Marketing, Bosch Security Systems, is very positive towards video analytics. He says: "The demand is very big, and of course there are different solutions to protect the perimeter, but video analytics is now improving so much that

it is also a very reliable detection, especially using thermal cameras, where you can achieve long range detection in a very reliable way. We see a big increase in demand there."

Genetec CEO Pierre Racz is more sceptical towards video analytics.

"You cannot rely on video alone for perimeter protection. Now, in combination with other technologies such as radars or infrared beams, you can achieve much better perimeter protection but it is an illusion to think that perimeter protection can be achieved alone with video analytics", he says.

Different solutions for different applications

Vanderbilt's CEO Joe Grillo claims that the choice of technology depends on the application.

"As a company we are not focused on the sensors or the devices themselves, rather we want to make sure we can interface with all of those different types of sensing solutions, whether it is video, radar or different types of motion detection, and be able to easily integrate those into our software solutions."

Keen Yao, Vice President of

Hikvision's International Business Center, claims video analytics can now solve intrusion problems and is useful within 100 metres, while radar is useful for longer distances. He says: "It depends on the different environments, market needs and costs."

William Ku, Vice President, Brand Business Division, Vivotek, also stresses that the cost is an important factor when choosing

PIRs still widely used

Boudewijn Hak from Bosch stresses that radars are usually used for long distances and often combined with cameras: The radar controls the camera, so when the radar detects something, the camera will automatically track that object based on information from the radar. He says: "But we see that this also can be done by video analytics nowadays, for

We are starting to get much closer to be able to implement reliable perimeter protection in the real world at a more cost effective rate.

technology: "I think it depends on the scenario and it depends on the budget, so for some it will probably be thermal and video technologies, if the project has a higher budget they will probably be using radar or thermal technology", he says.

Ku also stresses it has been very hard to use video surveillance alone for perimeter protection in the past. He likes to combine thermal cameras with video analytics.

Martin Gren gives a few examples of which technologies are most apt for perimeter protection: "If it is for an airport I think a thermal camera is what you need, if it is for a car dealer, then probably network radar is a good choice, so it varies, and if the project is a transformer substation or similar, then you can definitely use a video camera with high end video analytics."

example with thermal cameras. The thermal camera detects something at the perimeter and then sends the coordinates to the PTZ camera and it can zoom in to the position and confirm what is happening there. So, there are different solutions for perimeter protection."

Tim Biddulph from Hanwha says PIR detectors are still widely used, and there are still many companies in the industry making PIR technology today, however, thermal cameras are very popular. He says: "The future is all about thermal technology and improved low light performance in optical technology as well. Where you needed thermal cameras in the past, there is now optical technology that in most cases will do the same job with good reliability."



Tim Biddulph, Head of Product Management at Hanwha.



Boudewijn Hak, Regional BU Marketing, Bosch Security Systems.

Dallmeier adds VCA to 5000 series

Regensburg, Germany

In the age of Artificial Intelligence, IP cameras are evolving from purely imaging appliances into smart modules in the context of a video surveillance system.

Dallmeier is following these developments by integrating VCA technology, also known as video content analysis, into the 5000 series of Dallmeier cameras, thereby enabling intelligent incident search in the recorded video streams.

All 5000 series Dallmeier cameras are equipped with VCA technology as standard, to allow intelligent incident searching in the recorded video stream.

Filtering of the observation situation by the camera with the aid of the preset classifications enables real-time video analysis, with which

incorrectly detected incidents can be minimised in advance and are not even transmitted for storage, while at the same time incidents that are relevant can be stored on the server together with the associated metadata. This functionality has the advantage in the next step that the user no longer has to spend long periods laboriously viewing huge volumes of archived material, but instead can find the incidents of interest more selectively and efficiently with the aid of the stored metadata. Valuable time is saved, and pertinent suspicious instances can be verified quickly and simply.

Unlike motion detection (simple detection of movement), with which this analysis is carried out on the appliance only after the

fact, consuming much time on the part of the user, VCA performs the analysis beforehand and in real time, and classifies the objects it detects. The results of the analysis are transmitted continuously to the recording system together with the corresponding metadata as an incident report.

With VCA technology, five different analysis classifications can be assigned depending on the field of application: Intrusion Detection, Line-Crossing Detection, Object Classification, Face Detection and Tamper Detection.

Besides the basic data, such as date, time and location of the incidents, further filters can be used so that a broad spectrum of information such as object class



Dallmeier integrates video content analysis into the Dallmeier 5000 series cameras

or duration of the incident can also be stored, and this in turn can contribute to a precisely targeted, efficient search and evaluation, e.g., distinguishing between and filtering object classes (such as vehicles or people). **swn**

Civintec new generation Android 5.1 Utouch

Shenzhen, China

Civintec Global, a designer and manufacturer specialised in RF 13.56MHz contactless smartcard devices for access control and time attendance, has released the new generation CN890 Android terminal, *Utouch*, with competitive and innovative new technologies for general purpose management.

The Android Utouch is an intelligent terminal for 1-2 doors access control and general purpose management, it is incorporated with fingerprint technology, 125KHz+13.56Mhz smart card and NFC/BT smart phone

keyless access credentials. It is 'wire+wireless' communication and includes device network management to build PC/web based software solutions.

The new flagship Utouch terminal has been designed with a built in 1.4GHz quad-core processor with Android 5.1/Linus OS. An equipped optical fingerprint reader supports verifications of up to 25,000 templates in less than 330ms. As it also employs dual frequency 125KHz and 13.56MHz, it is fully compatible for use with advanced secured smart cards with

Mifare, Mifare plus, and Desfire-EV1 technology.

Via NFC or Bluetooth, the user's smart phone can be turned into a mobile key as an access credential. The Utouch terminal offers versatile interfaces including 4G, Wifi, BT, TCP/IP, and USB for communication and transmission. With the built-in camera version, video resolution can be optional from 2.0 to 5.0 megapixels for crystal clear images.

The Utouch terminal is equipped with a 7" capacitive touch screen. The terminal offers

a friendly GUI, allowing software companies and partners can extend system functions to meet more applications and project requirements for high efficiency and compatibility. **swn**



Civintec Global has released the new generation CN890 Android terminal, Utouch.

Optex releases new BX Shield

Maidenhead, Berkshire (UK)

Optex has launched the new *BX Shield* (BXS) series sensor in the EMEA region. These range of curtain motion sensors are ideal for protecting windows and the immediate boundaries of a building or site.

The BX Shield series includes four PIRs, two on each side, and the detection range and sensitivity can be adjusted independently for

each side of the sensor; the detection area can be easily set up to 12m/40ft (24m/80ft in total).

The sensor comes in two standard colours: a black body and white front face plate, or white body and white face plate. Optional black and silver plates are also available.

The new BX Shield has four models: two standard, hardwired PIRs (BXS-ST) and two hard-

wired models with anti-masking (BXS-AM). There are also two battery-powered models, standard (BXS-R), and antimasking (BXS-RAM).

All are equipped with digitally-enhanced signal recognition logic known as Super Multidimensional Analysis (SMDA), which improves immunity against changes in temperature or moving trees and

vegetation.

For environments where the temperature difference between the human body and the background is very small, the extreme high detection mode increases the PIR sensitivity to prevent any missed alarms.



Hanwha launches Wisenet Wave VMS

Chertsey, Surrey (UK)

The new Wisenet Wave video management software (VMS) from Hanwha Techwin has been designed to make it almost effortless to display up to 64 high definition video streams.

Hanwha Techwin already offers an entry level free VMS called SSM and for sophisticated Enterprise level VMS projects, the company integrates with technology partners such as Genetec and Milestone. *Wisenet Wave* has been launched to answer the needs of projects in the middle ground with an emphasis on simplified user experience.

An intuitive 'drag & drop' tool makes it extremely easy for operators to set up a display of live and recorded images on a single screen or video wall, with customisable layouts and sizes. Other key features include a virtual PTZ which, with just simple clicks of a mouse, enables operators to zoom in to see close up detail of any suspicious activity, whilst motion detection

and video analytics support can be configured to generate alerts when user defined incidents occur. A wide range of smart, keyword, calendar and time-slice search options facilitate rapid retrieval of recorded video.

Wisenet Wave offers a wide range of options to allow users to choose how and where they wish to manage their video surveillance systems with minimal hardware requirements.

- **Via the Desktop:** Wisenet Wave is offered as software which can be installed onto a user's desktop running Windows, Linux or Apple/Mac. 24 to 64 live high definition video streams can be managed on 32 and 64-bit operating systems.

- **Via the Cloud:** A cloud-based service which can be remotely accessed by an unlimited number of authorised users from anywhere in the world, offers a hardware free, cost saving method way to take advantage of all Wisenet Wave functionality.

- **Via Server solutions:** Wisenet Wave is available as a pre-loaded out-of-box server or software downloadable from Hanwha Techwin's website which enables operators to view up to 64 high definition streams of live video. A supporting web-based application enables each Wisenet Wave platform to be managed as a stand alone system or as part of a larger, scalable video management solution. The application also provides an audit trail, real-time health monitoring and camera failover support, as well as reports on server health and storage status.

- **Via a Mobile:** A mobile app



Hanwha Techwin introduces its new VMS - the Wisenet Wave.

provides the opportunity to remotely access the key functions of Wisenet Wave from a smart device to enable 'on-the-road' users to view and respond to any incidents captured by Wisenet cameras.

Whilst Wisenet Wave is packed with features to make it simple and easy for users to achieve maximum advantage from their video surveillance systems, it is likely to also be popular with system integrators looking to minimise on-site time. With the benefit of an auto-discover feature, connected cameras and a wide range of 3rd party IP network devices can be addressed and set up within just minutes. 



NOTHING MISSED

Independent left and right detection with BX Shield PIRs



Outdoor curtain PIRs, 12m/side

The BX Shield outdoor sensors are designed to protect the immediate boundary of your premises against intrusion. Not affected by small animals or by environmental changes, they are a perfect trigger for alarm systems or outdoor CCTV cameras. They provide two independent curtain detection areas (left-right) from 2.5 to 12m each. The BX Shield are available as wired, wireless, and anti-masking models.

Visit www.optex-europe.com or scan the QR code to watch the video.

INDOOR DETECTION | OUTDOOR DETECTION | TAILGATING DETECTION | PEOPLE COUNTING | ENTRANCE DETECTION

Hikvision 2-wire video intercom

Hoofddorp, The Netherlands

Hikvision has launched a new two-wire design video intercom, which includes a variety of features to provide the latest in residential security with high-definition imaging and convenient installation for the consumer market.

Hikvision's advanced two-wire video intercom includes both indoor and outdoor video intercom stations along with a distributor. When replacing outdated or non-functioning equipment, this hi-tech visual communication system uses existing wiring for simple, speedy, and economic installation.

This advanced design features vivid video synchronisation signals and exceeds power and audio transmission expectations.

Whether replacing an aging system or simply installing a new one, Hikvision's two-wire video intercom brings harmony and high video quality to consumer contexts. Users will enjoy in-home security with the latest features, such as 2 megapixel fisheye cameras with excellent night imaging and self-adapting IR light supplement; noise suppression and echo cancellation for optimum

voice audio; and the mobile Hik-Connect App so users can identify visitors and even unlock doors if required when away from home.

"Hikvision is continuously looking for innovative ways to develop our products and solutions for a better user experience. Apart from the professional video surveillance industry, Hikvision has also been committed to providing more services and technologies for end-users in community and home security," said Keen Yao, VP of Hikvision's International Business Centre. 



Hikvision's advanced two-wire video intercom includes both indoor and outdoor video intercom stations along with a distributor.

Flir releases thermal camera development kit for self-drive cars

Wilsonville, Or (USA)

Flir Systems, Inc is introducing a high-resolution *Thermal Vision Automotive Development Kit* (ADK) featuring the high-performance Flir Boson thermal camera for automakers, tier-one automotive parts suppliers, and innovators of advanced driver assistance systems (ADAS). The new Flir ADK allows developers to add an affordable, long-range thermal camera to their ADAS development vehicles to help advance reliability and redundancy required for self-driving cars.

As the auto industry's only automotive-qualified passive

infrared sensor currently in production, Flir sensors are offered today on numerous vehicles from General Motors, Peugeot, Mercedes, Audi, and BMW, and as an aftermarket system. An ideal sensor technology for pedestrian and animal detection, thermal sensors can see up to four times the distance of typical headlights. Thermal imaging helps drivers and future self-driving vehicles see in challenging environments such as darkness, sun glare, fog, smoke, and haze. Given this differentiated sensing capability and intense market focus, ABI Re-

search expects annual shipments of night vision systems, including thermal imaging sensors, to grow from 200,000 in 2017 to 4.2 million in 2021.

The Flir ADK features the high-resolution Flir Boson, which is equipped with an Intel Movidius Myriad 2 Vision Processing Unit, a sophisticated, low-power multi-core vision processor that fits within a compact footprint package ideal for automobiles. The ADK is also compatible with the Nvidia Drive autonomous vehicle computing platform.

"Flir thermal imaging sensors

have played a critical role in enhancing driver safety for more than a decade, and using them for advanced driver assistance systems in self-driving cars is a natural evolution," said James Cannon, President and CEO of Flir. "With our latest high-resolution automotive development kit, automakers can develop and integrate thermal imaging technology in self-driving cars easier, faster, and with low cost of ownership."

Flir recently demonstrated the ADK on the Nvidia Drive PX2 at CES 2018 in Las Vegas. 

Videx introduces new 2 wire video entry system

Wilsonville, Or (USA)

Videx, experts in access control and door entry, have introduced a new video entry system that boasts a 3.5" hands free colour monitor, integrated optional proximity for up to 50 users, that only requires two wires to link the door panels, videophones and PSUs together.

Rob Sands, Technical Director at Videx UK, said: "The wiring of these systems is very simple, meaning installation is quick and easy, so they're a great door entry solution for houses, flats, apartments and small offices. They're very flexible

too so can be expanded to accommodate additional entrances or videophones, for example, should the need arise."

The system's features include a day and night camera with infrared illumination, call progress LEDs and an optional second camera that can be connected to each entrance for additional security. Up to four devices can be fitted within each apartment with the additional benefit of intercommunication between devices, meaning the video kit is a

great choice for residential entry.

Rob added: "The new system, which has between 1-12 call buttons and comes in our new updated 4000 series design, also provides proximity access if required, which can be integrated into the standard size door panel with the proximity reader concealed behind the name plate window. Coded keypad for entry is also available in the video kit range, which also provides a speaker unit with loudspeaker function, microphone volume controls and balance control, a lock release

delay, and 13° camera tilting. It's an easy to install, extremely user friendly but highly functional door entry solution." 



The system includes a day and night camera with infrared illumination, call progress LEDs and an optional second camera.

Axis launches palm-sized PTZ smart home camera

Lund, Sweden

Axis is releasing a new palm-sized PTZ camera with wireless I/O connectivity for communication with other devices using Z-Wave Plus standard, a standard widely used in the smart home market.

The new addition enables flexible wireless communication with supporting security devices and makes installation both easier and more cost-effective. The discreet Axis M5065 network camera comes with 5x optical zoom, auto-focus and built-in analytics.

In a security installation, the total cost for system deployment is not the security equipment alone. Additional expenses, such as cabling and labor costs, can put security investments out of reach for small business owners. Visible cables can also be a problem where interior design and esthetics are important. Axis Communica-

tions is helping to remove these barriers with the introduction of Axis M5065 and selected wireless accessories. The wireless I/O connectivity enables flexible system deployment providing high-quality indoor security surveillance, allowing business owners to keep control of their premises and assets.

Axis M5065 delivers HDTV 1080p resolution and includes analytics such as Axis video motion detection, removed object detection as well as audio volume and scream detection.

With the camera's wireless I/O connectivity, it is possible to use an on/off command to control up to six wirelessly connected devices supporting Z-Wave Plus. Thanks to the technology, business owners can easily and cost-efficiently design a tailor-made system by themselves, combining camera and accessories

based on their needs. Changes and updates to the system can be made just as easily.

Axis offers four wireless I/O compatible devices- the Axis T8344 power on/off plug; the Axis T8342 door/window sensor; the Axis T8341 PIR motion sensor and the AxisT8343 alert button.

Kent Fransson, Global Product Manager at Axis Communications explains, "At Axis we are always trying to use the latest technologies to make security less of a hurdle for business owners. By introducing wireless I/O connectivity in a security context, we allow customers to set up an agile surveillance and security system to meet their individual business' needs, without having to invest a large proportion of their budget on set-up fees. For instance, they can use an Axis M5065 wirelessly connected to a



Axis M5065 with its wireless I/O connectivity enables flexible system setup with wireless accessories, reducing cabling and installation time.

door sensor to monitor or be alerted if someone opens a door to a cabinet with expensive goods. That is just one example of how a camera with wireless I/O connectivity could make security both easier and cost-effective and we see that it being used more broadly in the future."

The Axis M5065 network camera and its compatible devices will be available in US, Canada and Japan in January 2018 through Axis distribution channels. 

 The suppliers web site is linked to the global security web portal, www.securityworldmarket.com

UP-TO-DATE security technologies

SELECTIVE
DISCONNECTION
OF SUB-BANDS



 **FORTEZA**
RUSSIA
www.FORTEZA-EU.com

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

Nedap launches slim style Mace Smart reader

Groenlo, The Netherlands

Nedap Identification Systems is launching *Mace Smart*: a slim multi-technology reader for mobile access control.

This elegant reader is the newest addition to the Mace platform, which enables the use of smartphones in any access control system. The Mace Smart reader is able to read virtual credentials on smartphones, but also reads conventional smartcards. The Mace Smart reader was revealed at the Intersec exhibition in Dubai last month, which took place from the 21st until the 23rd of January.

"We are committed to unlocking the potential of smartphones as

identification technology in access control systems," says Maarten Mijswaart, General Manager of Nedap Identification Systems. "The release of our newest reader is proof of this commitment. In addition, we are also releasing a renewed version of the Mace Admin Portal that is used to distribute and revoke virtual access control cards. This renewed version now also has an API for seamless integration with any access control system. It is our firm belief that these innovations will help our partners to realise future proof access control solutions for their clients, whether it is for buildings, parking facilities or events."

With the introduction of the Mace platform last year, Nedap responded to the global shift of smartphone credentials replacing physical cards. Mace readers support Bluetooth, NFC and QR codes to identify people using virtual credentials, which are stored in a Mace app. Mace can be used in combination with any access control system or any other system that requires the swift identification of people, such as parking management systems or registration systems.

The Mace Smart mobile access control reader supports Bluetooth, NFC and smartcards and is small



Mace readers support Bluetooth, NFC and QR codes to identify people using virtual credentials

enough to be mullion mounted. It has a slim design, which makes this mobile access control reader an ideal solution for doors that require a combination of security and convenience. 

Dahua releases its first Wifi video doorbell

Hangzhou, China

Dahua Technology is releasing its first battery powered, Wifi video doorbell – *DB10*.

Nowadays, traditional digital doorbells are becoming less helpful to residents who are often on the go. With no network connectivity and no video recording, the householder is likely to miss important visitors and information. To solve these problems, Dahua is releasing the Wifi video doorbell DB10 to enable users to answer the door from anywhere.

With an app operated via mobile phone and cloud services, users can answer the door from anywhere in the world. The app will forward

in near real-time a video call which can be controlled and reviewed even when the user is on the other side of the globe.

The DB10 supports up to a 5 month service period in a single charge and can be recharged in 3.5 hours, enabling the user to spend as little time and attention on maintenance as possible. In addition the wire-free installation and Wifi connection for the DB10 makes it easy to install and use. Requiring no cabling or punching, users can just install the doorbell themselves.

The DB10 supports up to 1080P HD video intercom with super wide horizontal field of view

(FOV=140°). These enable users to clearly see in the house via the cell phone and view who is visiting, largely reducing the risk of mistakenly letting someone unknown into the premises.

The PIR detection with 5 configurable zones enables the set up of advanced motion detection with specific detection areas, allowing for the detection of approaching visitors while greatly reducing false alarms.

The release of this first battery powered Wifi doorbell demonstrates Dahua's commitment to continuous innovation and services. 



Dahua Technology is releasing its first battery powered, Wifi video doorbell – DB10.

Avigilon launches UMD technology

Vancouver, Canada

Avigilon has released the latest innovation in video analytics capabilities with the launch of Avigilon Unusual Motion Detection (UMD) technology, available in its upcoming *Avigilon Control Center* (ACC) 6.8 video management software.

UMD is an advanced artificial intelligence (AI) technology that brings a new level of automation to surveillance and is designed to

reveal events that may have otherwise been missed. Without any predefined rules or setup, UMD technology is able to continuously learn what typical activity in a scene looks like, and then detect and flag unusual motion. This allows operators to search through large amounts of footage faster, as UMD focuses their attention on the atypical events that may need further investiga-

tion, helping to reduce hours of work to minutes.

The enhanced ACC 6.8 user interface allows users to filter their recorded video timeline and automatically review the unusual motion events. These events are displayed in an intuitive playback screen that intelligently guides users through highlighted clips.

At launch, Avigilon UMD technology will be compatible

with the Avigilon H4 box, bullet and dome cameras, expanding to other cameras in the portfolio throughout the year. Existing customers will be able to upgrade certain legacy products to benefit from this exciting new technology.

ACC 6.8 with Avigilon UMD technology is expected to be available in the first quarter of this year. 

Martin Gren, Axis co-founder, about

Cyber security and the end of OEM

Martin Gren believes cyber security will continue to be the industry's biggest trend in 2018 and that OEM will come to an end due to greater demands for faster action on cyber security issues.

Nowadays, the Axis co-founder works more with audio than security cameras.

"IP audio is about 15 years behind network video, it is still almost completely analogue", he says.

By Henrik Söderlund

For a number of years, Martin Gren has been working as advisor for new products at what Axis has named New Business and he is also a member of the company's board.

He says: "IP audio products are very exciting. Unlike video, audio is still almost completely analogue. IP has so many benefits and you can do zoning, background music and all kinds of alerts and use the speakers to tell people they are at a place where they should not be."

How interconnected is your audio development with video?

"We are working to bring together entire system solutions and our horn speaker can integrate directly with all VMS, for example applications where you see someone in the frame and call the person. But our idea is to create IP-based audio solutions, it does not necessarily have to do with video surveillance. They can be used at railway stations, airports and in stores for background music and good sound quality."

What will be the biggest video surveillance trend in 2018?

"Cyber security was by far the biggest trend in 2017 and it will continue. It is in the news every day and according to IHS, the downward price pressure on security cameras has ceased because of it. Customers have become ready to pay a little bit more to make sure someone is taking responsibility for the products, not just when selling, but for several years afterwards."

Is this increase of price an advantage for you towards Chinese competitors who sell many units?

"This has to do with corporate

DNA. Openness is a core value for us, and we have shown that clearly in the last 3-4 years when security bugs have been found in our products. We have announced it, explained and quickly delivered patches. We are an open democracy and have always had this in our DNA, unlike a country that does not have freedom of opinion. I believe we have a long-term advantage there. I am sure the

” Cyber security was by far the biggest trend in 2017 and it will continue.

Chinese players will address all cyber security issues. But you have to be open when they appear, not just when they are thrown in your face."

Have your products been involved in any major cyber attacks?

"No, not that we know of. The cameras that were used in the Mirai attack were products where open ports were recommended and they had hard-coded passwords. They were really asking to be hacked. We have never had any hard-coded passwords in Axis cameras."

Your cameras are not easy to hack?

"Many years ago we had a camera that was easy to hack, but we learned a lot from it. We understood the importance of conducting all the basic tests in the early versions. I think the companies that are more new to the physical security industry also need to go through that learning phase. We began to publish our hardening



Martin Gren believes cyber security will continue to be the industry's biggest trend in 2018.

guide three years ago, and now the other players have started to do that too. We have always been very open about when being hacked."

What do you do then?

"For example, if a researcher comes to us and say they have

more common. From an Axis point of view, the radar that we launched last year is a trend and we expect to ship larger volumes of it this year."

In China, AI is by far the biggest trend.

"It is very relevant there. However, we have different cultures and social systems – here in Europe, GDPR will soon come into force and in our country of origin – Sweden – we can not even store the license plate of cars involved in gas theft (fuelling and drive away without paying). If you do not have that kind of limitation, you can do so much more. Good video analytic applications are those which do not have to be more than 95 per cent accurate. It works great to do random selection more efficiently based on data of suspicious individuals, but to conduct analytics that require almost 100 per cent accuracy is still almost impossible. And everything you do has to be according to the law and the GDPR sets limits."

When will AI be a reality?

"Much of it works already. But in spring 2017, Facebook announced that they employ 3,000 people to review content to get rid of fake news. One has to ask oneself what that says about technology. Facebook has well-organised text-only data that is directly readable, while video consists of almost grotesque quantities of data with not very well-structured data to say the least. I think that reveals what the future holds."

hacked a camera, then we usually have a month to fix it and upgrade. After that, the researcher closes the case and we will update. End customers need to know whose products they are using and that the company who supplies them can take responsibility for them."

So you believe using OEM is a problem?

"When a cyber security issue appears, the OEM skinning must be renegotiated. This means that there will be a delay and it may take three months from a bug being detected until a new OEM version has been created and the bug is fixed. For a serious integrator with a good reputation, that is definitely not good. I think cyber security issues will implicate the end of OEM."

What are the major technical video trends right now?

"The picture quality is becoming better and better. 4K is getting more common, but the bulk of all installations are 1080p. Multi imaging cameras have become



Global profile. Intersec 2018 attracted 29 522 visitors from 129 countries and 1 337 exhibitors from 59 countries.

AI, drones and smart technology attracted 30 000 attendees to Dubai

This year's first major event – Intersec – took place on 21–23 January, attracting 29 522 visitors from 129 countries to the Dubai International Convention and Exhibition Center. On site there were 1 337 exhibitors from 59 countries and a huge range of products and solutions for security purposes.

Like many other security fairs, there was a lot of attention on the opportunities that new technologies, such as drones and artificial intelligence (AI), can offer.

Automated police station

In the Dubai police exhibition stand there was a very strong focus on artificial intelligence and smart technology for a safer society. The police showcased prototypes on Robocop and also various types of smart services already in use in its fully automated police station which opened in September 2017.

Khalid Nasser Al Razooqi, Dubai police's director general of artificial intelligence, gave an overview of the government's vision toward using AI and robots for policing and protection.

"The Dubai Police has a target to be the smartest police force in the world, and we've been working on a new strategy based on AI that will ultimately increase the happiness of our residents and build Dubai to be the safest city in the world," said Al Razooqi.

"We plan to use AI to help

us not only reduce crimes, but increase our ability to predict potential crimes before they happen, along with reducing traffic accidents. We've introduced a crime prediction system as well as accident prediction system that can study the behaviours of drivers," he explained further.

"With UAE car manufacturers, we'll install sensors to study the behaviour of drivers and see how we can teach them the best way to drive. Vehicles will instruct police where they should cover based on data we have, and perhaps where there is crime," concluded Al Razooqi.

Drönare and AI

Among the new features at the 20th edition of Intersec was an indoor Drone Zone, along with two dedicated conferences on Drones and Artificial Intelligence. Greg Agvent, Senior Director for CNN Aerial Imaging and Reporting, spoke at the Intersec Drones Conference about the potential uses for drones in information gathering.

Agvent said that drones can

be effective to not only deliver new perspective of journalism and reporting, but can also be important tools for data capture that can have much wider implications:

"We're still at the very beginning of acknowledging what drones can do," said Agvent. "Right now, almost exclusively, we're working with video, but what about thermal imaging and forward looking infrared, and what context and understanding can this add to a story?"

"If we're covering search and rescue operations, what other sensors can we input? If we're doing a story on drought, can we put a hygrometer on a drone and create data that supports the video story? There're all sorts of opportunities for sensors to add new layers and context."

Intersec's seven parts

The Intersec fair is – organised by Messe Frankfurt Middle East – consists of seven sections:

- Commercial security.
- Fire and rescue.

- Safety and health.
- Homeland security and policing.
- Information and cyber security.
- Smart home and building automation.
- Physical and perimeter security.

With 483 exhibitors, the Department of Commercial security, was the largest show section.

„We're still at the very beginning of acknowledging what drones can do.“

International fair

The fact that 83 per cent of the exhibitors were international companies underlines the global profile that Intersec has achieved. There were 15 pavilions representing different countries. Canada, China, Czech Republic, France, Germany, Hong Kong, India, Italy, Korea, Pakistan, Singapore, Taiwan, UK, US and Russia.

There were also 223 exhibitors from the United Arab Emirates.

intersec

SAVE THE DATE

The world's leading trade fair for
Security, Safety & Fire Protection

January 20 – 22, 2019
Dubai, UAE

www.IntersecExpo.com



messe frankfurt

Security Events Calendar

March



6-8 March ISC BRASIL 2018 – Sao Paulo , Brazil

Venue: Expo Center Norte
Organiser: Reed Exhibition
Tel: +55 11 3060 4717
Email: atendimento@reedalcantara.com.br
Website: <http://www.iscbrasil.com.br/en/>



6-9 March Security Show 2018 – Tokyo, Japan

Venue: Tokyo Int. Exhibition Center
Organiser: Nikkei Inc.
Tel: +81 3 3512 5670
Email: tradefairs2018@smj.co.jp
Website: www.securityshow.jp/en/



6-7 March SCTX Security & Counter Terror Expo – London, United Kingdom

Venue: Olympia
Organiser: Clarion Events
Tel: +44 20 7384 7894
Email: sophie.mckim@clarionevents.com
Website: www.sctx.co.uk



7-10 March Security Expo – Sofia, Bulgaria

Venue: Inter Expo Center
Organiser: Bulgarian Chamber of Commerce and the Inter Expo Center
Tel: +359 (2) 9655220
Email: iec@iec.bg
Website: www.securityexpo.bg



14-16 March SECON 2018 – Seoul, South Korea

Venue: Hall 4 & 5, KINTEX
Organiser: SECON 2018 Organising Committee
Tel: +82-2-6715-5400
Email: global@seconexpo.com
Website: www.seconexpo.com



18-19 March Kuwait International Fire Safety Security – Kuwait, Kuwait

Venue: Kuwait International Fair Grounds
Organiser: Tafani
Tel: +968 95098204
Email: mughis@tafani.org
Website: WWW.KUWAIT-SAFETY.COM



20-21 March Securex West Africa – Lagos, Nigeria

Venue: Landmark Centre
Organiser: Montex
Tel: +44 (0) 207 886 3046
E-mail: jamie.pearson@montex.co.uk
Website: www.securex africa.com



21-21 March #TRYGGHETNU – Stockholm, Sweden

Venue: Clarion Hotel Stockholm
Organiser: AR Media International AB
Tel: +46 8-556 306 80
Email: deniz.baykal@armedia.se
Website: www.securityuser.com/se/Event
Visit AR Media at #TRYGGHETNU



20-23 March Securika 2018 – Moscow, Russia

Venue: Expocentre Fairgrounds Pavilions, 2, 8
Organiser: ITE Moscow
Tel: +7 (499) 750-08-28
Email: security@ite-expo.ru
Website: <https://www.securika-moscow.ru/en-GB/>



27-29 March SafeSecure Pakistan 2018 – Islamabad, Pakistan

Venue: Pak-China Friendship Centre
Organiser: Pagasus Consultancy Ltd
Tel: +92-21-111-734-266
Email: safia@pegasus.com.pk
Website: www.safesecurepakistan.com

April



11-13 April ISC West 2018 – Las Vegas, United States

Venue: Sands Expo
Organiser: Reed Exhibitions
Tel: +1 203.840.5602
E-mail: inquiry@isc.reedexpo.com
Website: www.iscwest.com



23-26 April Securex 2018 – Poznan , Poland

Venue: Int. Security Fair
Organiser: Poznan Int. Fair
Tel: +48 61 869 2000
E-mail: info@mtp.pl
Website: www.securex.pl/en/



25-27 April Secutech 2018 – Taipei, Taiwan

Venue: Taipei Nangang Exhibition Center
Organiser: Messe Frankfurt New Era Business Media Ltd.
Tel: +886 2 8729 1099
Email: Kirstin.Wu@newera.messefrankfurt.com
Website: <http://secutech.tw.messefrankfurt.com/taipei/en/visitors/welcome.html>

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.securityworldmarket.com/int/Security-Events

Security buyers guide

Alarm Communication



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

Access Control



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



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

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

Perimeter Protection



Manufacturer of
perimeter protection systems

Forteza, JSC

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



Manufacturer of perimeter
protection systems

Tel +7 967 445 0161
Tel +7 967 445 0162
info@forteza-eu.com
www.FORTEZA-EU.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



TAKEX Europe Ltd.

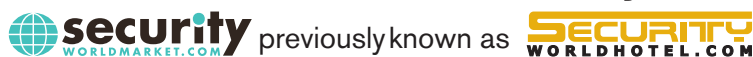
Aviary Court, Wade Rd, Basings-
toke, Hampshire RG24 8PE, UK

Tel +44 1256 475555
Fax +44 1256 466268

sales@takex.com • www.takex.com



A world-class information source for the security industry since 1998



www.securityworldmarket.com



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

HIKVISION®

PEOPLE COUNTING

Count **2005** People
Time **09:30-15:45**
Date **2017-06-18**
Location **Hangzhou railway station**



Focused on the data that matters

Hikvision's People Counting technology accurately counts crowd-traffic and reports critical data you need to see

Hikvision's People Counting technology serves critical functions in the security apparatus of crowd-centric applications. This multi-use feature records the number of people who pass through your entry ways and monitors crowd density to prevent accidents. Use loitering detection to keep visitor traffic flowing. Use alarm triggering to prevent injuries. And create reports to analyze customer activity and build revenue. Anywhere there's a crowd - tourism areas, train stations, sports venues, shopping areas, museums, and more - this advanced feature improves profits while protecting patrons.



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

www.hikvision.com