Security Solutions Today

March / April 2014

MANUFACTURING & INDUSTRIAL SECURITY

Cover Focus
The Protection Of Industrial Plants

Security Feature
Smarter Ways to Help Protect Your Business & more...

In Focus
An Interview with Anna Stebleva, VP Business Development, Artec Group

Show Preview & Review
Secutech 2014
Cards & Payments 2014
CPSE 2013

Scan this code & 'Like' us on

dahua TECHNOLOGY

I ♥ HDCVI

Normal BNC Cable Transmission HD Image

CE FC VL UL RoHS ISO 9001:2000

secutech International Trade Fair for Security, Fire and Safety TAIPEI
SECUTECH TAIPEI 2014
19–21 Mar 2014 Taipei, Taiwan
Booth: NO.4141

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

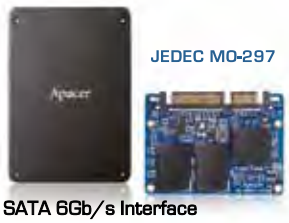
Apacer

Applications

Industrial SSD SOLUTIONS

SFD
SATA Flash Drive — SATA 3

SFD 25A-M



JEDEC MO-297

SATA 6Gb/s Interface
Capacity: Up to 256GB

SDM
SATA Disk Module — SATA 3

1U Server Series

Extended Temp. Support
(-40℃~+85 ℃)
Capacity: Up to 64GB

mSATA
SATA 3

MO-300

Capacity: SLC: 4GB~128GB
MLC: 8GB~256GB

M.2 (NGFF)
SATA 3

T42 A100-M

Capacity:
T42: 16GB~128GB
T60: 32GB~256GB
T80: 32GB~256GB

CFast 2
CFast Card

Compliant with CFast 1.0 Specification
Capacity: Up to 128GB

Industrial CF
Industrial Compact Flash

HW write-protect switch

Extended Temp. Support
Capacity: Up to 128GB

Industrial SD
Industrial SD Card

Compliant with SD 2.0 Specification
Capacity: Up to 32GB

Industrial microSD
Industrial microSD Card

Compliant with SD 2.0 Specification
Capacity: Up to 32GB

Industrial DRAM SOLUTIONS

- Fixed B.O.M. commitment
- Conformal Coating:
  dump & mould proof & corrosion prevention
- Wide Temperature range (-40°C~+95°C)
- Built-in Thermal Sensor
- Golden Finger 30u"

ECC DIMM (with Very Low Profile Option)

Data rate	Model	Capacity	Voltage	Standard Op. temp	Industrial Op. temp	CL	Layer
DDR3-1600	PC3-12800	2GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL11	240pin
DDR3-1333	PC3-10600	2GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL9	240pin
DDR3-1066	PC3-8500	1GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL7	240pin

SO ECC DIMM

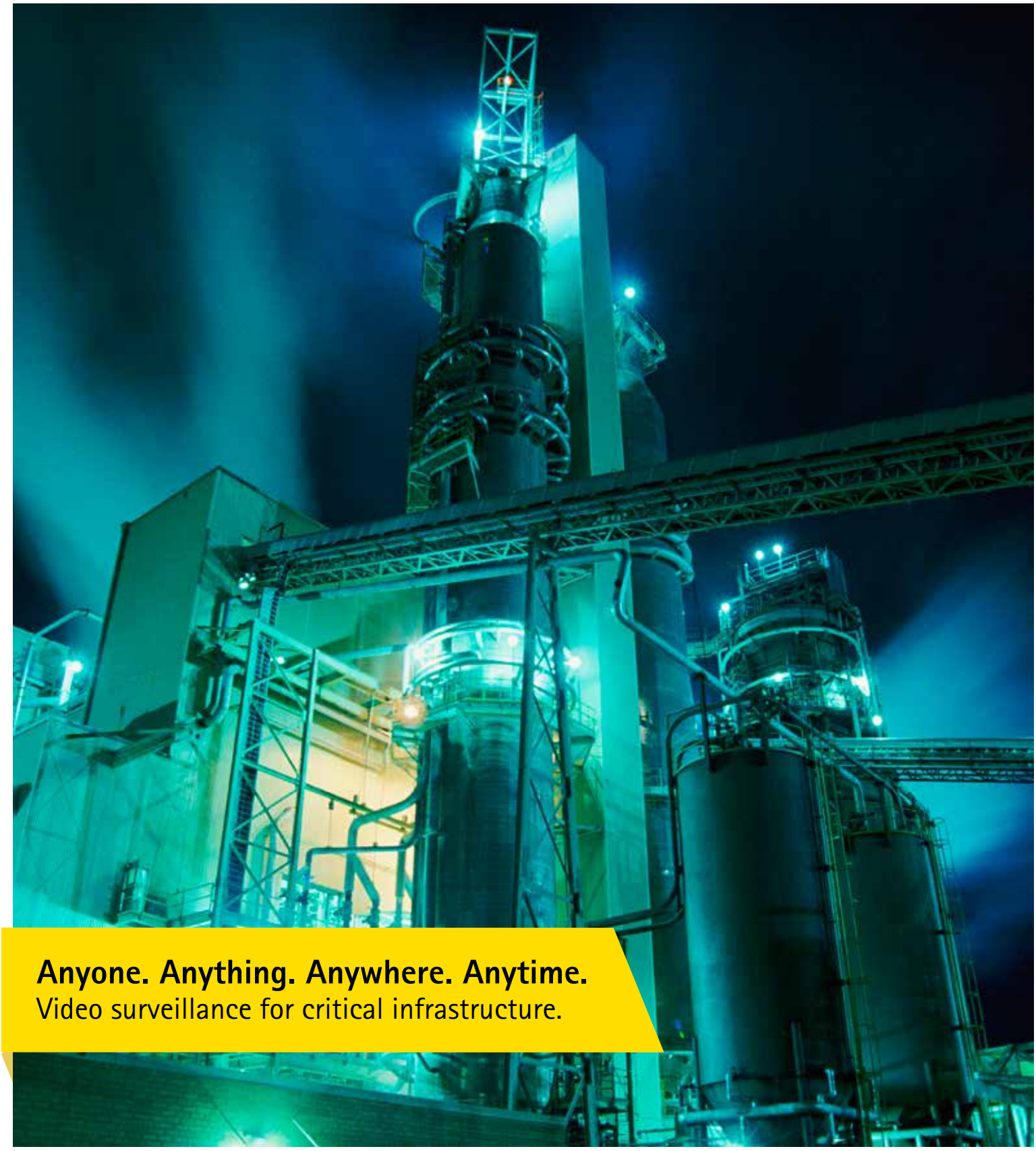
Data rate	Model	Capacity	Voltage	Standard Op. temp	Industrial Op. temp	CL	Layer
DDR3-1600	PC3-12800	2GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL11	240pin
DDR3-1333	PC3-10600	2GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL9	240pin
DDR3-1066	PC3-8500	1GB~8GB	1.5V+-0.075V	0°C~+85°C	-40°C~+95°C	CL7	240pin

Apacer Technology Inc.

Account Manager : Johnson Wen Tel: +886-2-2267-8000 Ext.5883 eMail:johnson_wen@apacer.com

CONTENTS

March - April 2014



Anyone. Anything. Anywhere. Anytime.
Video surveillance for critical infrastructure.

With threats possible from any angle, the unexpected is pretty much a guarantee for critical infrastructure. That's why Axis focuses on securing you from perimeter to core.

Our network video surveillance products help you secure your site in even the harshest conditions. Yet beyond that, we constantly work together with our partner network to bring you solutions that ensure safe, uninterrupted production that's also more efficient.

Axis solutions for critical infrastructure – covering every angle.

Visit www.axis.com/criticalinfrastructure or email contact-sap@axis.com for more info.

Scalable, future-proof solutions • Outstanding HDTV image quality • Integration of video alarms and monitoring into the SCADA system • Intelligent analysis with partner software

AXIS®
COMMUNICATIONS

CONTACTS

March - April 2014

Publisher
Steven Ooi (steven.ooi@tradelinkmedia.com.sg)

Editor
Sharon Kaur (sst@tradelinkmedia.com.sg)

Group Marketing Manager
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

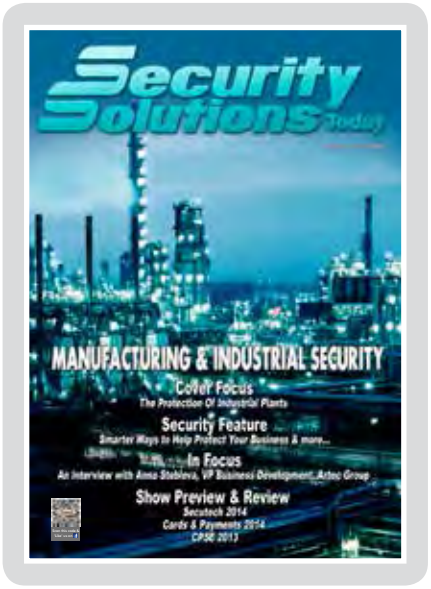
Marketing Manager
Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

Marketing Executive
Griselda Wong (griselda.wong@tradelinkmedia.com.sg)

Head Of Graphic Dept/ Advertisement Co-ordinator
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

Graphic Designer
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

Circulation
Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)



Designed by Fawzeeah Yamin
Image by: Lyondellbasell
www.lyondellbasell.com

Printed in Singapore by KHL Printing Co Pte Ltd.

Security Solutions Today
is published bi-monthly by
Trade Link Media Pte Ltd
(RCB Registration No: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399.
Tel: 65-68422580
Fax: 65-68422581
ISSN 2345-7104 (Print)

The magazine is available free-of-charge to applicants in the security industry who meet the publication's terms of control. For applicants who do not qualify for free subscription, copies will be made available, subject to the acceptance by the publisher, of a subscription fee which varies according to the country of residence of the potential subscriber in the manner shown on the right.

The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

ANNUAL SUBSCRIPTION:

Surface Mail:

Singapore	- S$40 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:

Malaysia/Brunei	- S$80
Asia	- S$120
Japan, Australia, New Zealand	- S$150
America/Europe	- S$150
Middle East	- S$150

ADVERTISING SALES OFFICES

Head Office: Trade Link Media Pte Ltd.
(RCB Reg. No: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399.
Tel: 65-68422580; Fax: 65-68421523, 68468843, 68422581.
Email (Mktg): info@tradelinkmedia.com.sg

India:
Mr. Avneet Singh
Mark Excellence Business Management
C317 / 8 Inlaks Nagar, C.H.S. 15 Yari Road
Versova, Andheri (West)
Mumbai
India
Tel: +91-22 325 81 747
Fax: +91-22 263 96 204
avneet@markexcellence.com

Korea:
MCI
Rm. 103-1011,
Brown Stone, 1330,
Baeseok-dong, Goyang-si,
Gyunggi-do,
Korea 410-907
Tel: +82 2 730 1234
Fax: +82 2 732 8899

Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: 81-3-32635065
Fax: 81-3-32342064

Italy/Switzerland:
Arch. Aldo Cacchioli
Publistein di
Galli-Cacchioli & Co.,
Via Borghese 11
CH-6600 Locarno
Switzerland
Tel: 41-91-7516910
Fax: 41-91-7517109
info@publistein.com

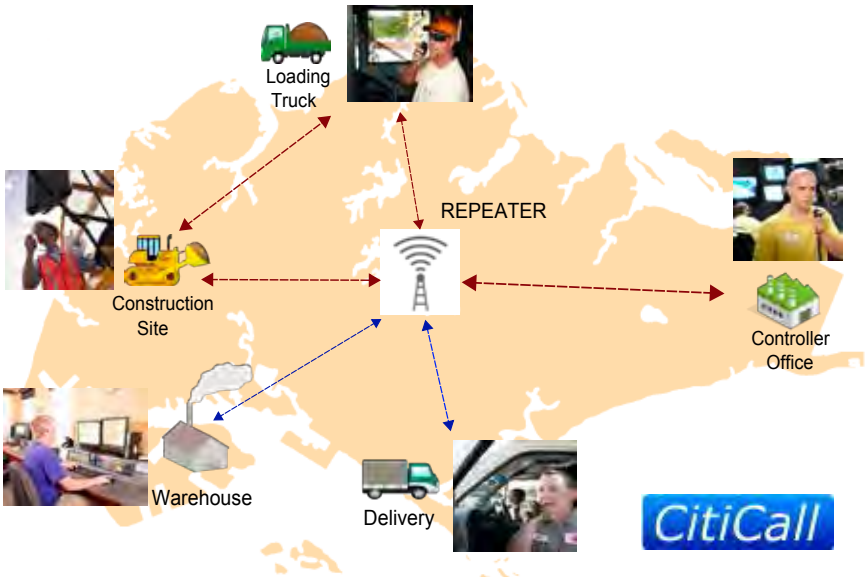
BEST PRACTICES THAT REDUCE COST AND RISK OF DEPLOYMENTS ENHANCED BY RADIO COMMUNICATION.

KENWOOD

ADVANCE DIGITAL TWO-WAY RADIO COMMUNICATION SYSTEM.

Under good and strong partnership between JVCKENWOOD and Citicall Communication Pte Ltd, Nationwide Digital Two-Way Radio Communication System is now available in Singapore! Instant and secured voice communication in many variety ways of use enables you to exchange the information of current traffic condition, delivery transition and any emergency.

Sharing information in group communication will improve the efficiency and productivity of business.



Wide Area Digital Radio Service

FOR CONSTRUCTION SITE AND MATERIALS TRANSPORTATION.

Radio Communication enables you to make wide area calls with your staffs seamlessly whether as individual or a group talk.

Especially in an emergency situation, you can instantly communicate with your staffs in warehouse, office or delivery staff to share updated information.

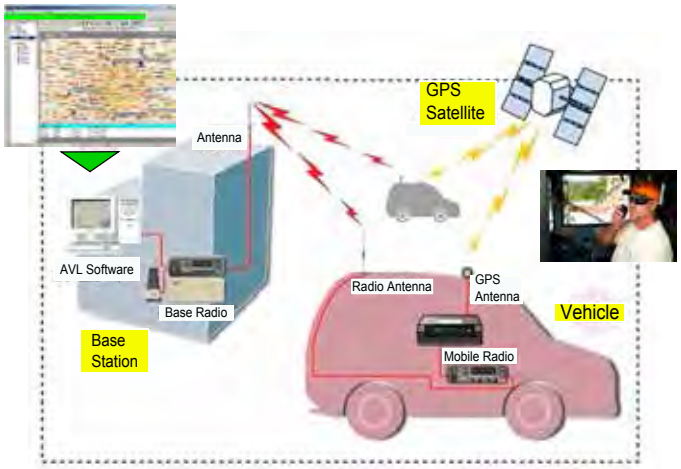
And at the same time, you are able to response quickly to meet and solve the critical situation all the times.

As a result, it will strengthen staffs teamwork as well as maximize productivity.

GPS INTEGRATION AND FLEET TRACKING FOR DELIVERY AND DISPATCHING SERVICES.

By adding GPS function on the Radio Communication, you can use Fleet Tracking to monitor the location of your each vehicle on the road through a map on your office PC.

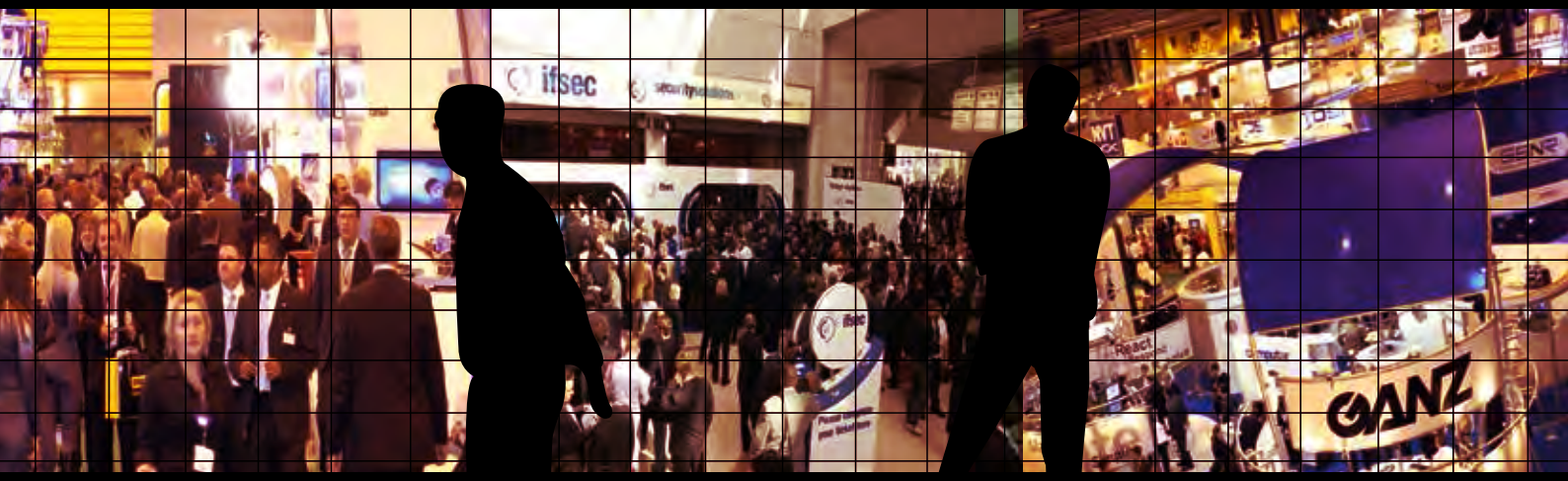
Operator is able to grasp the location of each vehicle instantly through the system. And then, dispatch arrangement will be smoother, timely and more efficient.
Voice communication between each vehicle and between the operator and each vehicle is also available for route guidance, emergency call, exchanging information of the current traffic conditions, etc.



JVCKENWOOD Singapore Pte. Ltd.
1 Ang Mo Kio Street 63, Singapore 569110
Tel : (65) 6496 4500 Fax : (65) 6496 4501/509
Email : comsales@sg.jvckenwood.com
Website : http://www.kenwood.com/sg/com/

Citicall Communications Pte Ltd
51 Goldhill Plaza #07-10/11
Singapore 308900
Email : sales@citicall.net
Website : http://www.citicall.net

Calendar Of Events



Secutech Taiwan 2014

Date: 19 – 21 March 2014
Venue: Nangang Exhibition Centre, Taipei Taiwan
Contact: Echo Lin
Organiser: Messe Frankfurt New Era Business Media Ltd.
Tel: +886 2 2659 9080 ext. 761
Email: Echo.lin@newera.messefrankfurt.com
Website: http://www.secutech.com

Safety & Security Asia 2014

Date: 28 – 30 April 2014
Venue: Marina Bay Sands, Singapore
Contact: Chloe Tan
Organiser: Conference & Exhibition Management Services Pte Ltd (CEMS)
Tel: +65 6278 8666
Email: chloe@cems.com.sg
Website: http://www.safetysecurityasia.com.sg

Asian Securitex 2014

Date: 7 – 9 May 2014
Venue: Hong Kong Convention & Exhibition Centre Hall 1
Contact: Karina Yu
Organiser: Hong Kong Exhibition Services Ltd.
Tel: +852 2804 1500
Email: exhibit@hkesallworld.com
Website: http://www.asiansecuritex.com

Secutech Thailand 2014

Date: 3 - 5 July 2014
Venue: Bangkok International Trade and Exhibition Centre
Contact: Tina Chang
Organiser: Messe Frankfurt New Era Business Media Ltd.
Tel: +886 2 2659 9080 Ext. 665
Email: stth@newera.messefrankfurt.com
Website: http://www.secutechthailand.com

Secutech Vietnam 2014

Date: 20 - 22 August 2014
Venue: Bangkok International Trade and Exhibition Centre
Contact: Sandra Chen
Organiser: Messe Frankfurt New Era Business Media Ltd.
Tel: +886 2 2659 9080 ext. 761
Email: Sandra.chen@newera.messefrankfurt.com
Website: http://www.secutechvietnam.com

IFSEC Southeast Asia 2014

Date: 11 - 13 September 2014
Venue: Kuala Lumpur Convention Centre
Contact: TJ Tan
Organiser: UBM plc
Tel: +6-03-2176 8788
Email: tj.tan@ubm.com
Website: http://www.ifsecsea.com

Security China 2014

Date: 28 - 31 October 2014
Venue: China International Exhibition Centre (New Centre)
Contact: Tony Lee
Organiser: China Security and Protection Industry Association
Tel: +86-10-51920615
Email: bizcspia@yahoo.com.cn
Website: http://www.securitychina.com.cn

never been easier

It's Easy to Install, Operate and Maintain - It's HUS-NVR-1032!

Feature-rich. Simply Easy. The latest HUS-NVR-1032 is designed with a number of user-friendly functions that enhance operation efficiency and video management experience. The Setup Wizard and One-Click Import functions reduce installation time by 60%. Its intuitive user interface, Timeline and Video Export functions save operation and management time, minimizing human resources. The HUS-NVR-1032 is also easy to maintain with advanced Hot Swap technology and front panel HDD slot design. Featuring high definition recording at 1080P (8 channels), 720P (16 channels) and D1 (32 channels), the HUS-NVR-1032 is ideal for real-time video/audio live view and playback. It can be used as a standalone solution for mid-scale installations, while for more complex system architectures, it can also be integrated with HUS (Honeywell Universal Surveillance) smart IP security integration platform.

HUS-NVR-1032 – Redefining Simplicity.

Honeywell

ONVIF
Driving IP-based physical security through global standardization

Australia: 1300 234 234 China: 400-8800-330 Hong Kong: (852) 2405 2323
India: (91) 124 497 5000 Korea: (82) 2 799 6114
Singapore: (65) 6355 2828 Taiwan: (886) 2 2245 1000
For more information, visit: www.asia.security.honeywell.com
Email us: security.ap@honeywell.com

Editor's Note

Dear Readers,

Welcome to SST's March/April Issue. This issue explores Manufacturing & Industrial Security.

Our cover story by Franz Köbinger, Marketing Manager Industrial Security, from Siemens, focuses on Industrial Security (pg. 18). There are three great Security feature articles in this issue, which discuss smarter ways to help protect your business, the uses of thermal cameras for pipeline security as well as the advantages of integrating a smart focus system into surveillance cameras (pg. 30). In addition to our usual product showcase section, you can look forward to a brand new addition to SST called "Product Spotlight" where we feature the latest product launches from companies including, Dahua Technology, Axis Communications, Vivotek, Sony and Bosch Security Systems (pg. 82).

This issue also includes an exclusive interview with Anna Stebleva, VP Business Development, from the Artec Group (pg. 80). Our Pundit Perspective section features exclusive viewpoints from security professionals from Mobotix, Milestone Systems, Vivotek, Axis Communications and Dahua Technology who discuss the threats that Manufacturing environments face in the 21st century (pg. 26).

The potential impact of security-related incidents to manufacturing can be devastating. Therefore it has become more important than ever for manufacturers to implement a proper security strategy that protects while enabling access and integration, in order to remain efficient.

Have a great read!

Sharon Kaur
Editor

Panasonic

Making the invisible visible

6 Series

i-PRO SmartHD Solutions

ONVIF S

SD Super Dynamic

Enhanced Super Dynamic imaging technology (Dynamic range: **133dB**)
Low light high sensitivity with combined MOS sensor and Multi processing Noise Reduction technology
Zero-lux image capture with IR-LED
Double SDXC/SDHC/SD Memory card slots

Outdoor

NEW
WV-SFV631L
FULL HD 1080 60p | Vandal Resistant | IP66 standard

NEW
WV-SFV611L
HD 720 60p | Vandal Resistant | IP66 standard

Indoor

NEW
WV-SFR631L
FULL HD 1080 60p | Vandal Resistant

NEW
WV-SFN631L
FULL HD 1080 60p

NEW
WV-SFR611L
HD 720 60p | Vandal Resistant

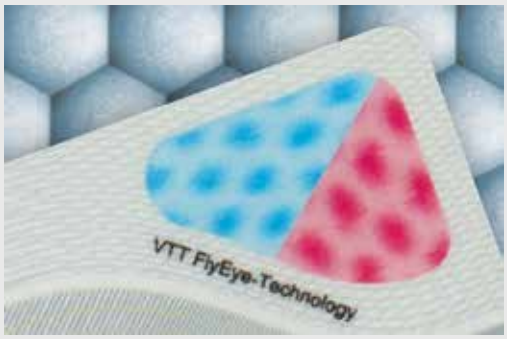
NEW
WV-SFN611L
HD 720 60p

Panasonic Security Product Library Download
http://panasonic.net/pss/security/library/products.html

Like us on facebook for more updates
http://www.facebook.com/PanasonicNetworkCamera

Panasonic Systems Asia Pacific
2 Jalan Kilang Barat, Panasonic Building Level 7, Singapore 159346 Tel: +65 6270 0110 Fax: +65 6276 0330 E-mail: biz.prod@sg.panasonic.com

VTT Verschleissteiltechnik Gmbh Recognized As Finalist For The Sesames Awards At Cartes Paris 2013 With VTT Fly-Eye Technology



VTT Verschleissteiltechnik GmbH, with headquarters in Langenhagen near Hanover (Germany), is a global leader in the production of lamination plates for passports, driving licenses, national ID's, bankcards, smart cards and health insurance cards with integrated security features. They deliver the complete solution for cost-effective manufacturing of high-quality cards. They have been selected as a finalist for the Sesames Awards at Cartes Paris in the category "Manufacturing & Tests" which refers to printing and manufacturing techniques, materials, personalization, validation test tools and suites. The Sesames Awards competition rewards the industry's best innovations every year. The jury is composed of experts from the industry. The VTT Fly-Eye Technology offers a wide range of options for different applications with one card as the hardware in the category "Manufacturing & Tests". The idea behind the new lens technology with its hexagonal lenses is to recreate the structure of a real fly eye. The fly eye consists of several single eyes on each side of the head of the fly. The fly develops a picture of its surrounding thanks to single-image dots.

Several millions of lenses can be applied on one single card. These vast numbers of lenses create a 3D and floating effect. The size of the lenses is a few microns, barely visible to the naked eye. This VTT Fly-Eye Technology allows a full-size and partial image to be moved. The viewer will observe a sort of floating-effect from all sides and three dimensional effect of the depth, despite thin card material. "It is great to be recognized as an innovator in lens technology since we already developed other lens technologies like MoveID and MLI/CLI lenses. With Fly-Eye Technology a large number of variations such as form, composition, size, resolution, coloration(printing) and radius are possible." commented Harry Post, ceo of VTT Verschleissteiltechnik. "The result is a solid and forgery-proof credit card, ID card, smart card and passport". SST

Arecont Vision Announces New Hire

Arecont Vision, industry leader in IP-based megapixel camera technology, recently announced the appointment of Matthew McCoy as the Company's new director of Strategic Accounts. McCoy is a 25+-year veteran in the security industry, where he has developed and refined his skills with companies such as ADT/Tyco, Convergint and most recently with Avigilon.

"Matt has been a pioneer in identifying and aligning clients' emerging technology needs with products and services," said Carole Dougan, vice president of North America Sales, Arecont Vision. "His expertise in this area will be a great asset both to our customers and to Arecont Vision as we intensify our focus on raising the standard of IP video surveillance with megapixel camera technology."

As director of Strategic Accounts, McCoy will be responsible for driving sales at Arecont Vision's select national systems integrators. His strong relationship building skills and ability to plan and conduct sales initiatives will help him to take advantage of opportunities and to expand sales of the company's industry leading megapixel camera technology. SST

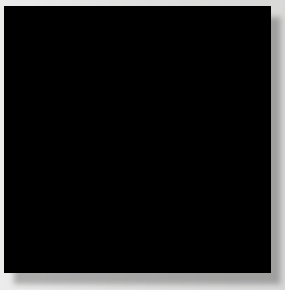
FLIR

Safety is not expensive it's **priceless**

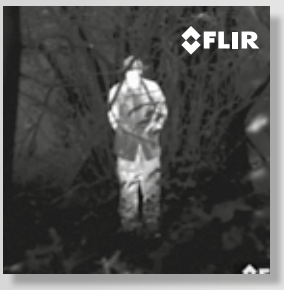
FLIR FC-Series S

Extremely affordable, network-ready fixed mount cameras

FC-Series S thermal security cameras let you see intruders and other threats to your facility clearly in total darkness and in bad weather. Fully enabled for control and operation over digital and analog networks, FC-Series S thermal imaging cameras are available in 320 × 240, and high-resolution 640 × 480 formats.



Normal vision



Thermal image

ONVIF

If you want to have more information about the FLIR FC-Series S or any other FLIR thermal imaging camera please contact:

Asia Pacific Headquarters
HONG KONG
FLIR Systems Co. Ltd.
Room 1613 -16, Tower 2,
Grand Central Plaza,
No. 138 Shatin Rural Committee Road,
Shatin, New Territories, Hong Kong
Tel : +852 2792 8955
Fax : +852 2792 8952
Email : flir@flir.com.hk

www.flir.com

HID Global Improves Classroom Attendance At Dayton Public Schools While Increasing Campus Security And Safety

HID Global®, a worldwide leader in secure identity solutions, recently announced that the company's secure ID card issuance solutions, combined with solutions from Plasco ID, a leading integrator and provider of card-based ID systems, has enabled Dayton Public Schools (DPS) in Dayton, Ohio to increase classroom attendance through improved student tracking, while enhancing campus security and safety by including new visual security elements on multipurpose ID cards. With over 30 buildings and special centres housing approximately 15,000 students, Ohio-based DPS needed to standardize and simplify ID card creation while expediting the previously manual process of checking in tardy students. Their new solution implemented by PlascoID, includes the company's automated student behaviour tracking system, PlascoTrac and HID Global's FARGO® DTC4500 card printer/encoder plus its non-technology ID cards and AsureID® Enterprise card personalization software, which is used to create customized student ID cards with high-quality photos and other visual security elements. This integrated system has achieved DPS' goals while also enhancing the security of students and visitors. "Now that we have sped up the time it takes to create IDs and process tardy individuals, our students are in class more and therefore have a greater chance for achievement and success," said Richard Melson, director of The Office of Information Technology at DPS. Today, both K-12 schools and higher education colleges and universities must combat growing security threats with shrinking budgets. This has created demand for multi-functional smart cards that provide schools with more versatile and efficient secure ID solutions. Thousands of educational institutions around the world have adopted HID Global's secure issuance solutions to create, use and manage campus ID cards that can be utilized for physical access to buildings, logical access to networks, library checkout and other services, as well as cashless and debit card transactions on and off campus. SST

Genetec Releases Security Center 5.2 For Integration

Genetec™, a leading provider of unified IP security solutions, recently announced that the latest service release of Security Center (5.2 SR4) provides integration with over 80 new video devices from 13 technology partners, including many new models from Arecont, Axis Communications, Samsung, Sony and Vivotek. The release follows the launch of new Security Center plugins for partner solutions including Software House C•CURE 9000 access control, Barco CMS video wall, Southwest MicroPoint perimeter detection devices and DSC PowerSeries intrusion panels. Available now for download to all Security Center 5.2 customers and to those with an active software maintenance agreement (SMA), this service release provides customers access to new software updates and feature options, with support for many of the latest edge devices on the market.

Security Center 5.2 SR4 provides support for a number of new encoders, including the Axis M7016 and P7216, offering analog customers highly cost-effective 16-channel encoder options. The release also integrates with a large number of new megapixel IP cameras from Genetec technology partners, including support for additional models of Arecont SurroundVideo® panoramic cameras.

The number of Security Center technology partners also continues to grow with the addition of a number of new and updated third party plugins. The recently updated Software House C•CURE 9000 access control plugin for Security Center provides bidirectional integration between the two systems, enabling operators to monitor C•CURE alarms, and other information within Security Center, and view access control events with their associated video as well as video Security Center video from the C•CURE workstations. A new Barco CMS plugin provides the seamless management of Barco video walls from Security Center, allowing operators to display and remotely control tile layouts and cameras on video walls through simple drag-and-drop. Integration with Southwest Microwave INTREPID MicroPoint Cable and MicroPoint II perimeter fence detection systems offers customers a field-proven interface enabling operators to receive alarms from perimeter fences and monitor surveillance video associated with events from Security Center. Security Center also adds support for a new intrusion detection partner, the PowerSeries 1864 intrusion panel from DSC. SST

MicroEngine®

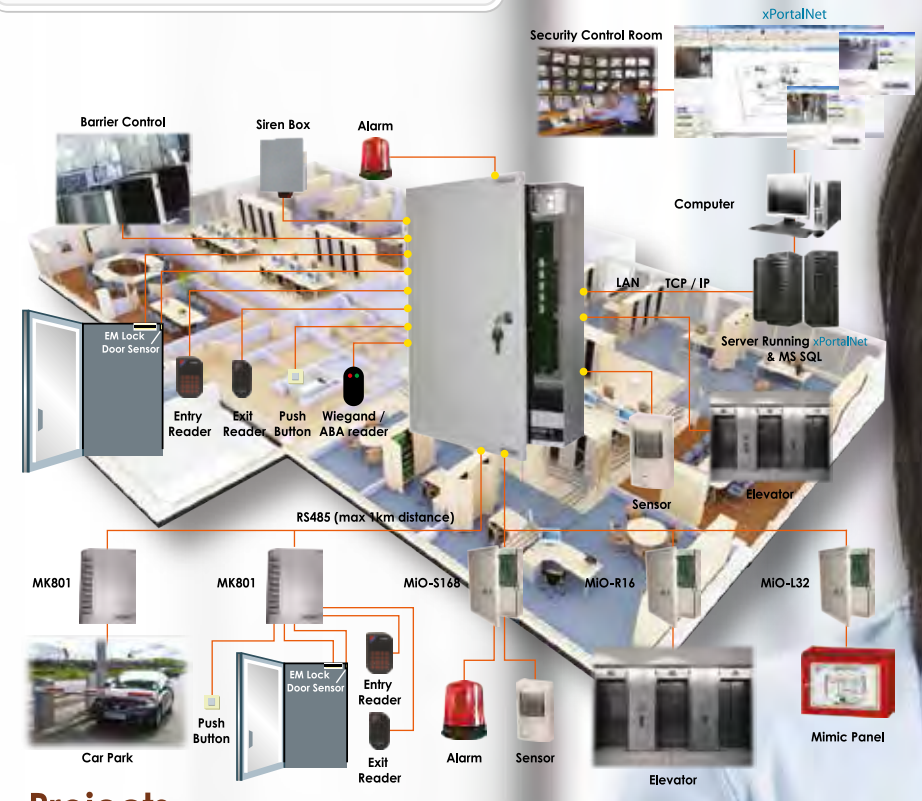
Integrated Security Systems

The Trusted Brand in Security Solutions

P1000i
PoE Controller

We have a strong track record in delivering projects even though the system requirement was changed

- PoE Controller in DIN Rail Mount Ready Casing
- CCTV Integration with Selected International Brand
- OPC Integration Module
- DesFire Reader



Projects

Commercial / Complex

Factory

Condominium

DesFire Reader

Dual Redundancy Module

Plato Reader - Slim Card Reader

600+ readers ward access & security system on SQL Server for hospital and many more ...

enquiry@microengine.net

www.microengine.net

Our Office

REG No. 44831281647

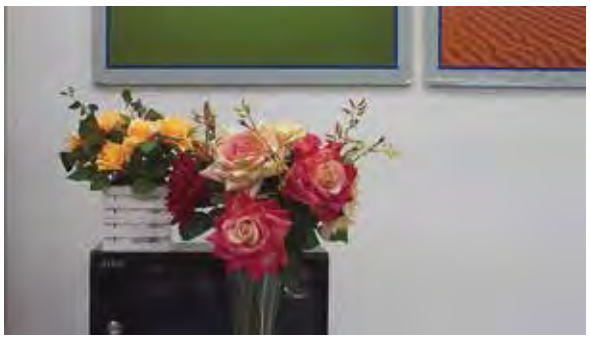
Uniview IPC Acquires The UL2802 Certificate

Uniview, the leading manufacturer of China IP video surveillance, recently became the first manufacturer to gain the UL2802 certificate in the Asia-Pacific region. UL2802 was published in October, 2013 for testing cameras' performances, including resolution, grey level, dynamic range, sensitivity, distortion, maximum frame rate, relative illumination, veiling glare and bad pixel count. It provides a more direct and more accurate standard, which helps to identify cameras' qualities. The UL2802 certificate was awarded to Uniview after two of its cameras: the HIC5421DE and HIC5401DE cameras passed rigorous tests and were confirmed to have industry-leading performances, especially in WDR and low illumination. In other aspects, for example, in grey level, bad pixel count veiling glare and sensitivity, the HIC5421DE and HIC5401DE cameras also did exceptionally well.

To guarantee every IP camera's high quality, Uniview has developed many unique technologies. By strictly selecting each sensor, Uniview ensures the highest sensitivity and the lowest bad pixel count. To exploit a sensor's maximum ability, each IP camera is equipped with algorithms to enhance low illumination and high resolution. Uniview IP cameras can provide sharp images with accuracy in colour reproduction and resolution even under harsh lighting conditions. Through high frame rates, Uniview's cameras have better-performing WDR effects. More detailed images can be presented even under great lighting contrast. Besides, the up-to-date environmental adaption algorithm enables cameras to present more clear images. SST

Comparisons between Uniview HIC5401DE camera and other company's IP camera:

Grey level, resolution:

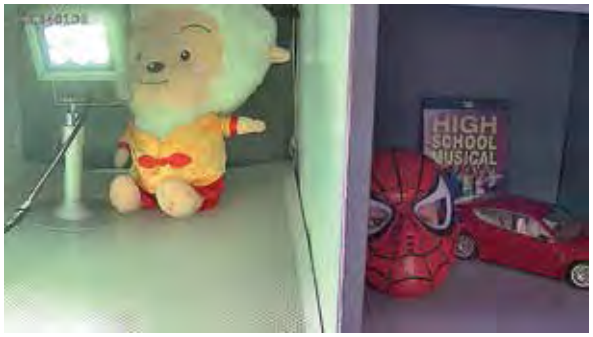


IP camera from another company

Uniview HIC5401DE camera

WDR:

IP camera from another company



Uniview HIC5401DE camera

Customized Solutions and Seamless Integration of Systems by Bosch at **The Star**, Singapore

BOSCH
Invented for life

- *Seamless integration of systems enables better synergy for security operations throughout the premise.*
- *Flexibility of systems provides ease of use and maintenance.*
- *Customized solution effectively provides time and cost savings*

The Star is an integrated hub with a Civic and Cultural Zone comprising a 5,000 seat auditorium named – The Star Performing Arts Centre, and a Retail and Entertainment Zone named The Star Vista.

This iconic multi-purpose development combines a world-class retail experience with a collection of visually stunning performance spaces. The Star Vista occupies 6 levels and is owned and managed by CapitaMalls Asia while Rock Productions Pte Ltd owns and manages The Star Performing Arts Centre that occupies the remaining 9 levels of the 15-level development.

This integrated hub serves the needs of over 400,000 residents, students and office workers in the vicinity. As an award-winning architectural landmark, The Star had to ensure effective communication and security within the zone.

They required an effective security system to monitor, control and deliver 24/7 surveillance of the premise and a public address system that can produce high quality background music, crisp voice announcements and emergency evacuation messages. Since The Star is operated by two separate entities. This meant a higher level of integration throughout the building would be required to ensure efficiency. In addition, the systems had to blend in with the building's architecture and design.

While working closely with the installer – InfoCom & Security, and the consultant, a customized solution was provided. This included the installation of the Bosch Building Integrated System (BIS), which allows seamless integration of the Bosch AUTODOME and FlexiDome cameras, Video Management System with decentralized recording, Public Address and Access Control Systems.

The solution from Bosch provides better coordination and synergy between the two operators and increased ease of use and maintenance of the building's security systems.

---

*The Bosch **FlexiDome** and **AUTODOME** cameras deliver image excellence, color reproduction and more detail in low-light conditions. Open Network Video Interface Forum (ONVIF) conformance ensures the cameras are easy to install – integrating seamlessly with third party solutions. Producing more pixels per target object, Bosch cameras make it easier to improve situational awareness. From analog to IP, standard resolution to HD, indoors or out, there's a FlexiDome or AUTODOME to meet the requirements of a wide range of applications.*

For more information, email us at:
apr.securitysystems@bosch.com or visit
www.boschsecurity.asia.

Exacq Launches Advanced VMS Solution In Asia Pacific

Leveraging the global marketing power of Tyco Security Products, Exacq Technologies, the leading developer of open architecture, cross-platform, Video Management System (VMS) solutions for video surveillance applications has launched a full series of exacqVision hardware and software in the Asia Pacific region, including exacqVision Start, Professional, Enterprise and Edge VMS software. The solutions are scalable from a single camera to an enterprise-class system with thousands of cameras, and run on Windows, Linux and Mac platforms, with the open architecture suitable for customers' various needs.

The exacqVision VMS cross-platform, scalable solution has an intuitive and user-friendly interface, and can be easily connected to cameras. The other powerful functionalities include mapping, audit trail, smart search, event surveillance, exacqReplay, digital PTZ control as well as integration with third party IP cameras and access control systems. In addition, the live and recorded video can be accessed via the free exacq mobile app on iPhone, iPad, Android, Kindle fire, Blackberry Playbook.

The newly launched exacqVision Edge VMS software runs directly on an IP camera or encoder without the need for a separate, central server and loads onto any compatible IP camera through the camera's web page app loader. The full functionality and performance of exacqVision Pro and exacqVision Enterprise is available on a single IP camera running the exacqVision edgeVMS application, including Active Directory, Integration, Video Wall, Mapping, Digital PTZ, third-party integration and more. The exacqVision software includes one to three year Software Subscription Agreement. Users can receive quarterly software upgrades for all the latest advancements as they are released. SST

AVer's IP Cameras Now Supported By Nuuo

AVer, a major global provider of presentation/education solutions, security surveillance solutions and video conferencing solutions, recently announced that 24 of their IP cameras have just finished integrating into NUUO's NVR system.

Nuuo was founded in 2004 and focuses on NVR and hybrid solutions. To date, over 110 brands and 2500 IP camera models have been integrated into their systems. AVer will continue to be a main solution provider in the global surveillance market by cooperating with companies such as Nuuo, which offer an open platform policy of multi-brand integration and a product line, which offers complete video surveillance solutions for all types and sizes of installations.

A wide selection of AVer's IP cameras have been integrated into Nuuo's systems, including models from their Rugged, Bullet, Dome and Box Series. Several models from Aver's Rugged Series have been integrated into Nuuo's systems, which are renowned for being able to handle anything you can throw at them and are operable in the harshest environments and working conditions, including the following: FB2028, FB2028-T1, FB2028-T2, FB2028-TM, FB3028-RT1, FB3028-RT2 and FB3028-RTM. SST

secutech

March 19 – 21, 2014
Taipei, Taiwan

www.secutech.com

Secutech offers triple value to global buyers

(HD Solutions) + (SMAhome) =

New Exhibitors, New Technologies, New Applications

- Source the latest HD solutions: **analogue HD, IP HD, HD-SDI**
- SMAhome: First-ever smart home area showcasing product line-ups for home security, monitoring, automation and entertainment.
- Over 85% exhibitor will release yearly launch at Secutech 2014

your first sourcing stop in Asia!

Mar. 19-21, 2014

Download the apps & sync with us!

Contact Us!
Messe Frankfurt New Era Business Media Ltd.
Sandra Chen
E-mail: sandra.chen@newera.messefrankfurt.com

messe frankfurt

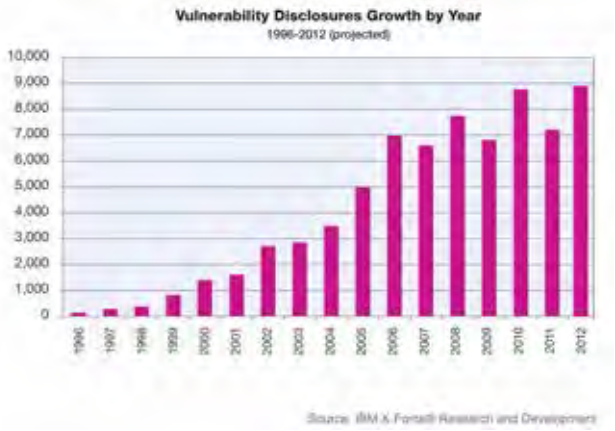
INDUSTRIAL SECURITY – SECURITY CONCEPT FOR THE PROTECTION OF INDUSTRIAL PLANTS

By: Franz Köbinger, Marketing Manager Industrial Security,
Siemens Industry Automation Division

Introduction

Cyber attacks on companies, associations and government centres have made it clear that the so-called "cyber war" has become a reality. More and more, industrial concerns and plants are being targeted, which is made clear by the increasing number of security incidents across the world in recent years. The targets and tactics of the attacks have changed. Attacks are becoming increasingly more aggressive and the tools are becoming more effective. This change in the threat situation requires a fundamental re-think of information and access protection measures, as well as the procedures for establishing security concepts. The attackers are upgrading – and both the manufacturers and operators of automation systems must counter these threats.

Headlines about industrial security feature prominently on the front page and in the news. Reports of cyber attacks



are already on the daily agenda and we have to face the fact that more and more weak spots are discovered each year. In 1996, there were just a handful of reports about gaps in security that had been discovered. That number then rose exponentially to several thousand in recent years. The actual number of the existing weak points is probably several times higher.

The fact that these weak points can be exploited and that the risks are real has been shown by investigations, such as the one by ICS-CERT, which found and investigated 198 attacks on control computers in the USA from October 2011 to September 2012 alone.

One reason why more and more weak points are being discovered is the fact that in industrial automation and control engineering, standardized hardware and software components are increasingly being used that also allow end-to-end networking among themselves and furthermore with office IT systems and the internet. These open systems simplify the integration of the individual components and reduce the dependency on certain suppliers, since, as a result, interoperability is significantly improved or even made possible in the first place. This speeds up production, allows a better overview and reduces development and production costs. Overall, the aim is for better efficiency to maintain or even improve competitiveness.

These advantages, however, involve risks since open systems are also more susceptible to attacks, manipulation, sabotage, and industrial espionage. Hackers naturally expend the majority of their resources targeting technologies that have the greatest worldwide

presence, and the decreasing number of proprietary systems in favour of more open standards makes it easier for attackers and malware to gain access to automation systems.

However, when establishing security concepts, the situation in the automation environment looks very different from that in the office environment. Securing automation networks presents a huge challenge, because it comes into conflict with other important requirements such as performance capability, availability and user-friendliness. In addition, securing a network or system requires constant attention to detail and adaptations, and the job is not finished with a one-time installation the way it normally is when setting up an automation system. Even after the acceptance inspection, threats must be assessed and responded to with adaptations and updates if necessary, to ensure that the system remains secure. If you are protecting your own systems, it is important to have a reasonable awareness of the risks. It is just as important, however, to be able to trust your own security precautions and to be able to believe in the reliability of your employees. Too little security is negligent and too much security is not cost- effective. In this area of conflict, one should use the right sense of proportion, based on need, when implementing measures, which are adapted for industrial systems.

Overview of the Industrial Security concept from Siemens

The decisive question is: How can potential risks be significantly minimized and how can adequate, but affordable security be achieved in industrial automation?

Unfortunately, there is no standard solution that can always be applied because each system has individual boundary conditions, risks and protection goals. But there are proven procedures and a reasonable number of conceivable measures, which must be taken into consideration for an efficient security concept. On their own, individual security measures always have gaps and are therefore insufficient. An individual measure is easier to by-pass than several in succession.

It is also true that multi-faceted threats must be countered with a variety of measures. For example, viruses cannot be effectively countered with firewalls and unauthorized accesses cannot be countered with virus scanners. On their own, technical protective measures cannot cover all of the protection goals, which means that accompanying supporting organizational measures are indispensable. Thus, only one overall concept can minimize all of the risks and provide effective protection. Consequently, the Industrial Security concept from Siemens corresponds to a multi-layer defence, the so-called "defence-in-depth" concept. This concept provides both all-round protection and in-depth protection for an automation system. On the one hand, this means that various, mutually complementary protective mechanisms are in place in order to be able to meet the various threats (all-round protection) and, on the other hand, that there are several barriers, which must be overcome by a potential attacker. The concept contains the important components of system security, network security and system integrity (see Figure 1).

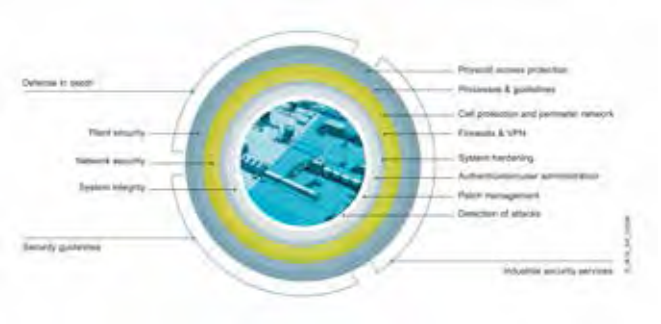


Fig. 1: Defence in depth: Multi-layered concept for protecting production systems

Plant security

Plant security ensures that technical IT security measures cannot be by-passed in some other way. This includes physical access protection measures such as fences, turnstiles, cameras or card-readers and organizational measures, particularly a security management process, which ensures the long-term security of a plant.

Physical access protection

The following items can be categorized here:

- Measures and processes that prevent unauthorized persons from gaining access to the premises of the plant
- Physical separation of different product areas with different access authorizations
- Access protection for critical automation components (e.g. securely locked control cabinets)

The guidelines for physical access protection measures also have an influence on the required IT security measures and their extent. If, for example, only select personnel have access to an area from the beginning, then the network access interfaces or automation systems do not have to be secured to the same extent as would be the case for publicly accessible areas.

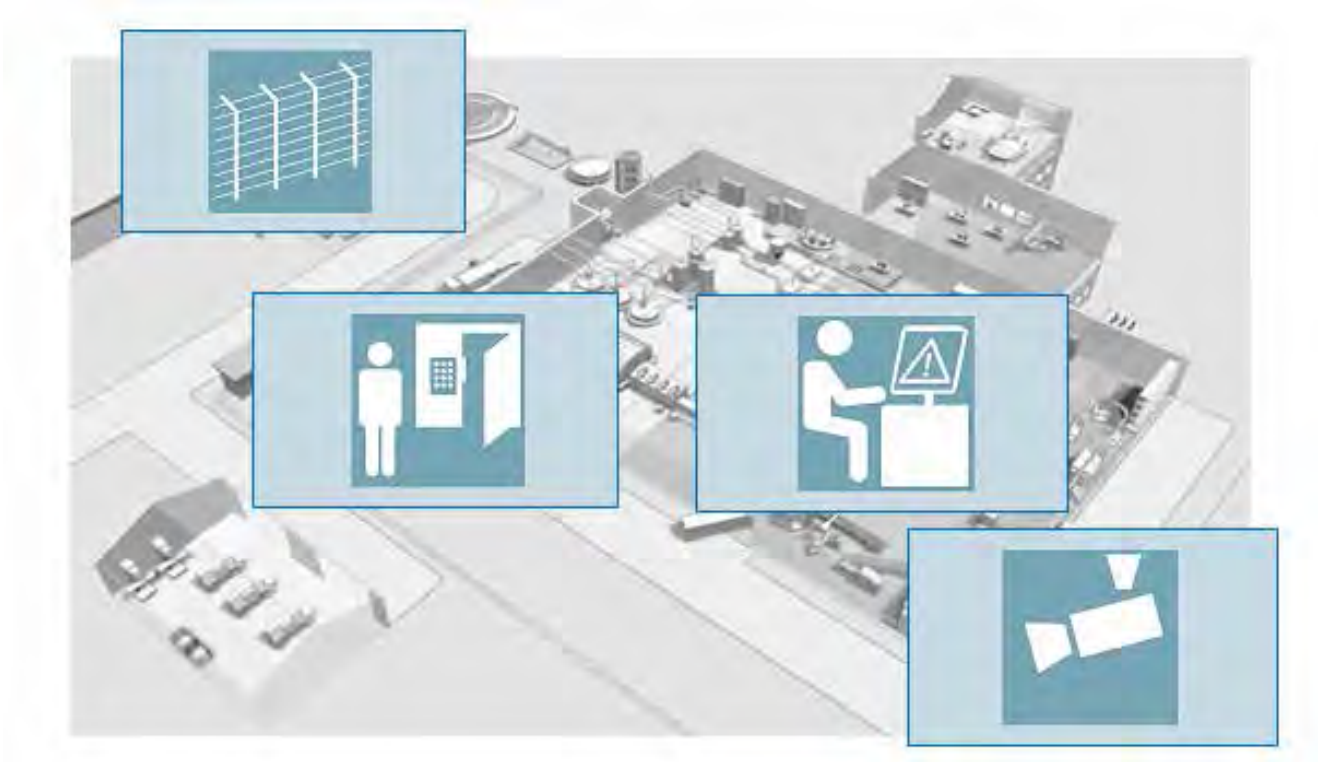


Fig. 2: Physical protection against unauthorized access to production areas

Security management

Organizational measures and the introduction of security processes are an indispensable component of plant security. Organizational measures must be closely tied in with the technical measures and they must be mutually supportive. Most protection goals can only be achieved by combining the two types of measures.

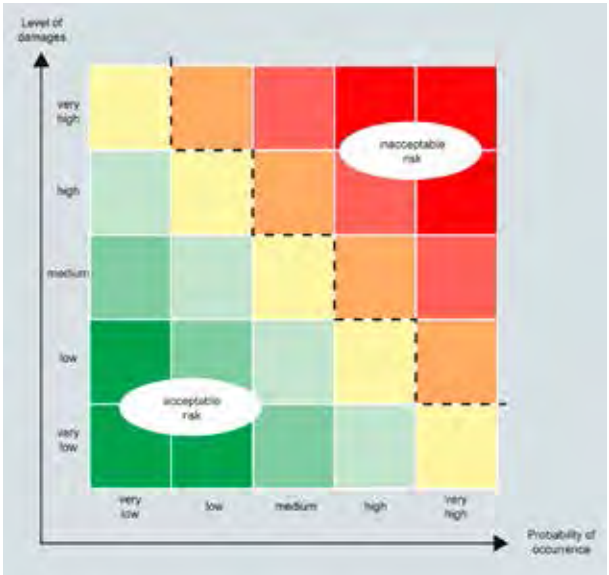


Fig. 3: Decision-making table for assessing and regularly checking risks by means of a plant-specific risk analysis

One organizational measure is to establish a security management process. In order to make well-founded decisions on which measures make sense, you must first analyse which concrete risks cannot be tolerated. Both the probability of a risk occurring and the possible extent of any damage play a role in this (Figure 3). If the operator neglects to perform a risk analysis or does not determine the protection goals, there is a considerable risk that unsuitable, overly expensive or ineffective measures will be taken and many weak points will not be detected or remedied.

The protection goals are derived from the risk analysis and serve as the basis for concrete, organizational and technical measures. The measures must be checked after the implementation. The risk must be assessed again from time to time, or if there have been changes, because the

Fig. 4: The four security management process steps to be continuously executed

threat situation may have changed in the meantime. The process then starts over from the beginning (Figure 4).

Network security

The central element of the Industrial Security concept is network security. This includes the protection of automation networks from unauthorized access and the checking of all interfaces to other networks, such as an office network and particularly remote access to the internet. Network security also encompasses protecting communications from interception and manipulation, i.e. encryption of the data transfer and authentication of the respective communication nodes.

Securing the interfaces between the company and plant network

Transitions to other networks can be monitored and protected by means of firewalls and by setting up a DMZ, if necessary. "DMZ" stands for "demilitarized zone", which means a zone that is secured or shielded. The DMZ is used to provide data for other networks, without granting direct access to the automation network. Typically, a DMZ is designed in such a way that it is also not possible to access or connect to other systems from it, i.e. even if a computer in the DMZ has been taken over by a hacker, the automation network remains protected (Figure 5).

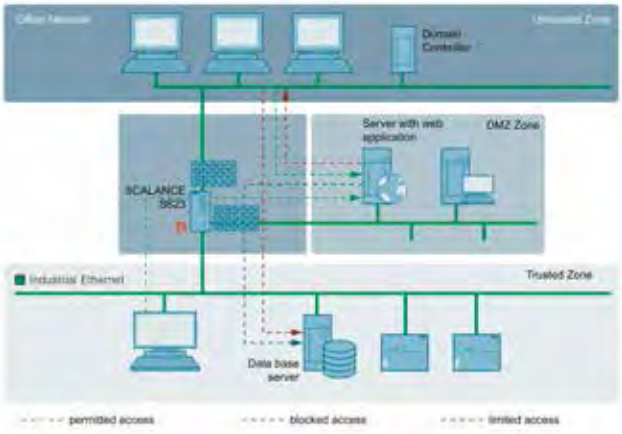


Fig. 5: Use of a "demilitarized zone" for transferring data between the company and plant network

Network segmentation and cell protection concept

The secure segmenting of the plant network into individually protected automation cells minimizes risks and increases security even further. This means that parts of a network, e.g. an IP subnet, are protected by a security appliance and thus the network is secured by segmentation. Thus, devices within this 'cell' can be protected from unauthorized access from outside without affecting the real-time capability, performance or other functions.

The firewall can now control the access to the cell, which allows the operator to define which network nodes can communicate with one another and what protocols they will use. This not only denies access to unauthorized persons, but also reduces the network load, because rather than allowing all forms of communication, only the desired and required forms of communication are allowed. The cells are divided and devices are assigned according to the communication and protection needs of the network stations. Furthermore, data transmission to and from the cells can be encrypted by the security appliances by means of a VPN as required. It is thus protected from data espionage and manipulation. This authenticates the communication nodes, and authorizes them for access where necessary. For example, the cell protection concept can be implemented and communications can be secured using "Security Integrated" components such as SCALANCE S Security Appliances or Security CPs for the SIMATIC S7 automation system (Figure 6).

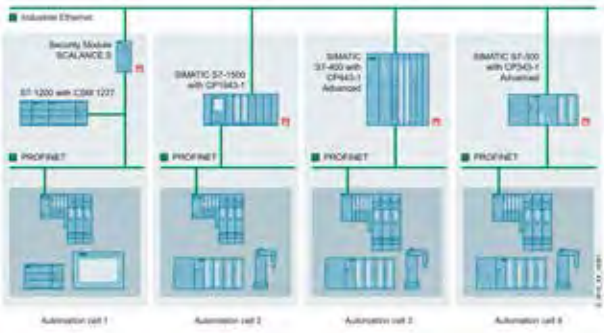


Fig. 6: Network segmentation and cell protection with Security Integrated products (see red padlock symbol)

Secure remote access

More and more plants are being connected to directly via the internet and remote plants are being connected to via mobile networks (GPRS, UMTS, LTE) for remote servicing, remote applications, and for monitoring machinery installed around the world.

Securing access is especially important here. With the aid of search engines, port scanners, or automated scripts, hackers can easily find unsecured access points without any great effort. This is why the authentication of the communication nodes, the encryption of the data transfer, and the integrity of the data must be ensured. Especially if you are dealing with infrastructures that are critical to the plant. Access by unauthorized persons, the reading of confidential data, and the manipulation of parameters

or control commands can cause considerable damage, negatively impact the environment, and endanger personnel.

VPN mechanisms, which precisely provide authentication, encryption and integrity protection, have proven to be especially effective as protective functions for this. The internet-capable security products from Siemens Industry support VPN connections and can thus securely transfer data via the internet or mobile networks as well as control access. Normally, devices are authenticated as trustworthy by means of certificates and IP addresses or DNS names are used in the firewall rules in order to block or allow access. The VPN appliance and SCALANCE S firewall use user-specific firewall rules to also give the capability of linking access rights to users as well. In this case, users log onto a web interface using their name and password and special firewall rules are assigned to each authorized user so that he or she can be granted access according to his or her access authorization. The advantage here is that you can clearly track who has accessed the system at a specific point in time.

The SCALANCE S623 variant with three firewall ports also provides a way out of a dilemma, which system integrators, OEMs and end users often have to face. On the one hand, machine builders should be able to access their machines at the end user's location for maintenance purposes, but, on the other hand, end user IT departments only grudgingly allows outsiders into the network to which the machine is connected. With the SCALANCE S623, the machine can be connected to the plant network and the firewall can be connected to the internet using the third port. This allows the machine to be accessed from the Internet, but access to the plant network from the Internet can be denied. Thus, it is possible to remotely access the machine from the internet for servicing without having to give the service technician direct access to the plant network (Figure 7).

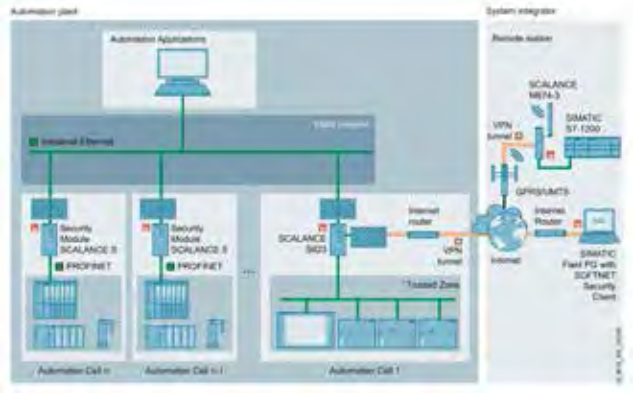


Fig. 7: Secure remote access to plant units without direct access to the plant network with three-port firewall.

System integrity

Securing a system's integrity should be regarded as the third pillar of a balanced security concept. This means using automation systems and controller components, SCADA and HMI systems, which are protected against unauthorized access and malware or that meet special requirements such as know-how protection.

Protection of PC-based systems in the plant network

Just as office PC systems are protected against malware and any weak points that are discovered in the operating system or in the user software must be eliminated by installing updates and patches, industrial PCs and PC-based control systems in the plant network also need corresponding protective measures. Many of the protection systems that have proven themselves in office environments can also be used here by using such things as virus scanners. Since virus scanners cannot detect all viruses and are powerless to stop new viruses before the pattern update, alternatives should be considered, if applicable, particularly because software cannot always be updated in a timely manner in an automation environment if no maintenance window is available, e.g. during twenty-four hour a day, seven day a week operations.

The use of so-called whitelisting software is an alternative to virus scanners. Whitelisting works with positive lists in which the user can define which processes or programs may run on the computer. If a user or malware then tries to install a new program, this is denied and the damage is prevented. As a manufacturer of industrial software, Siemens supports the user by testing the software for compatibility with virus scanners or whitelisting software.

Protection of the control level

It is common knowledge that PCs and networks must be protected against threats. But what measures can be taken to protect manufacturer-specific, proprietary systems? How can one protect programmable logic controllers (PLCs) and operator stations that do not use a commercially available operating system or which use an older version, because they have been in operation for years or even decades?

Third-party security software generally does not provide a solution for this. Access to the system functions of the devices is mostly not possible or only possible to a limited extent. For security solutions for protecting the control level, the manufacturers of automation hardware are asked to implement corresponding

security mechanisms and to provide users with system-specific setup options. At the same time, users are encouraged to ask the manufacturers about the existence of such mechanisms and to activate them if setup options are provided for this. The protection of the control level is essentially aimed at ensuring the availability of the controllers in the field and also to protect intellectual property, because the development know-how with regard to the machine is a big investment for any machine builder. The requirements for access protection and protection against manipulation in production plants are changing, however, as a result of increased interconnection and integration within the IT world in automation technology. This is indispensable for modern control systems and is already integrated in the next generation of controllers, SIMATIC S7-1500. If, for example, Siemens controller functions, such as password protection, block protection or copy protection are used, another essential building block for securing the plant network has been laid.

Individual function blocks can be protected, meaning that unauthorized individuals have no access to their content and cannot therefore copy or change algorithms. At the same time machine reproduction is prevented using copy protection, i.e. linking the program parts with the memory card's serial number, meaning that protected programs can only be used in legitimate machines. These functions help every machine manufacturer to protect their investment and maintain their technological edge.

Roles and rights concepts

We have seen that a defence concept that confronts an attacker with several hurdles (defence-in-depth concept) is required to defend against the various threats and to achieve an appropriate level of protection. At the same time, however, this means that authorized personnel must also overcome these hurdles. In practice, there are normally different access rights or classes of rights. Specific users may only access specific parts of the system, devices or applications for example. Many have administrator rights, others only have read or write access rights. Implementing a security concept thus not only serves to defend against attacks, but also implements a rights concept, i.e. to ensure that only authorized persons are able to access a system and even then only in accordance with the rights assigned to them. Typically, individual rights profiles are not created for each person. Instead, roles that have specific rights are defined. Users or groups of users are now assigned to the roles and thus their respective, corresponding access rights are assigned. User management is therefore an important aspect in connection with security.

A universal configuration for all of the automation components facilitates user management in this case, because the roles and rights of various persons can be defined and maintained centrally.

Consideration of attack scenarios in product development

Security measures that are implemented by operators of production plants have been described above. Manufacturers like Siemens naturally support this by providing corresponding security products that are industry-capable in every regard, and concepts, guidelines and recommendations for use of the security products are created for this. Of course, manufacturers can do even more by scrutinizing the automation systems and devices during the development process for possible weak points and eliminating any that are found. Every weak point that is eliminated makes things more difficult for attackers and reduces the overall risk.

Manufacturer processes for increasing product security

Firstly, it is important to increase general understanding of the fact that the measures for preventing weak points must exist in a systematic, universal and sustainable way even during the development process and that they must be constantly checked. Those actively involved in structuring this process – both suppliers and in-house development departments – are, among other things, laying the foundations for security certifications, for example in accordance with ISA Secure (International Society of Automation) or NERC-CIP (North American Electric Reliability Corporation; critical infrastructure protection).

Experts then examine the development processes and the internal organization and evaluate them with regard to security aspects. The goal is to find improvement measures in the relevant processes and, if required or deemed useful, to also introduce new roles and responsibilities within the organization.

The following process improvements have been introduced at **Siemens Industry** in the context of these evaluations and corresponding improvement results have been achieved:

- **Creation of a new role in the Product Lifecycle Management process**
  Product security experts monitor the PLM process following the "four eyes" principle and are responsible for the product data security.

- **Creation of programming guidelines**
  The establishing of security programming guidelines in order to prevent known and standard weak points with statistical analysis in the source code.

- **Establishing product security risk management**
  Expansion of the Siemens internal PLM process, which assesses the security risk in specific PLM steps and from which countermeasures are derived.

- **Optimizations in the development process**
  Adaptations of the development process in order to proactively increase security against development weak points.

- **Creation of security awareness in development**
  Create awareness among the developers in order to establish industrial security as a central element.

- **Expansion of the product strategy with security mechanisms**
  Introduce data integrity, data confidentiality and data availability into the products as fundamental elements.

To deal with weak points found in products that are already in the field, reactive measures are required. If weak points are found in automation components during external or internal testing, not only must they be eliminated, but the relevant target group must also be notified. To do this, a dedicated process must be introduced in which security incidents are handled with a higher priority and the required experts are available quickly. Such a process reduced the processing times at Siemens for the discovered weak points by up to 80 per cent and affected users were able to be notified within a few hours. Of course, the elimination of weak points alone cannot ensure protection against specific cyber attacks such as unauthorized access or the detection of malware. These require active protection mechanisms such as secure authentication, access control or encryption. But, nevertheless, the elimination of weak points and preventive measures is also an important and necessary component of securing automation systems. Only this combination of security-hardened products and active security measures can result in a consistent, high-performance security concept.

Security services

With the Industrial Security Services, Siemens offers its customers solutions and services that can be precisely adapted to the requirements of the automation environment.

The "Security Assessment" forms the basis for consultation. The customer is given a clear depiction of the possible threats, especially in the industrial environment. The result is a meaningful report, which contains the current risk level and recommendations for the effective and sustainable reduction of risks. This gives the customer an ideal basis for planning and implementing targeted measures. On the basis of the "defence-in-depth" concept, Siemens works with the customer to implement measures, which range from the implementation of firewalls, anti-virus/ whitelisting software and system hardening to the access control systems with special signatures for the industrial environment (Intrusion Detection (IDS) / Intrusion Prevention (IPS)). The signatures are based on an analysis of the weak points of the components to be protected and ensure that they are protected.

Monitoring and managed service

To ensure that systems or machines maintain their security level over their entire lifespan, Siemens provides monitoring capabilities for the continuous monitoring or alarm notification if needed. Threats are identified and eliminated in time thanks to the monitoring and alarm notifications, before processes or systems are damaged and values are destroyed. The success of the measures is validated by means of strict, cyclically recurring checks. Many customers concentrate intensely on their core businesses. Therefore, the service line "Industrial Services and Security" can provide them with support within the framework of Managed Services in order to analyse, monitor and continually update their security architecture.

Summary: A comprehensive security concept for secure automation

Industrial Security is not only a question of technical implementation, rather it begins with an awareness of security at all levels of management and among employees. With the elements of plant security, network security and the protection of system integrity, it is possible to achieve a comprehensive and in-depth security concept, which can significantly minimize the risks that modern production networks are faced with (see Figure 8).

Within the framework of a holistic industrial security package, Siemens provides products, systems, solutions and professional services in order to be able to implement comprehensive industrial security concepts.

The Siemens solution pyramid for Industrial Security is thus comprised of the following three parts (see Figure 9):

Industrial Security Services: Comprehensive service packages over the entire lifecycle for a tailored security solution

Security management: Processes and guidelines for increasing product security in the in-house development process and recommendations and guidelines for users on using the products and systems.

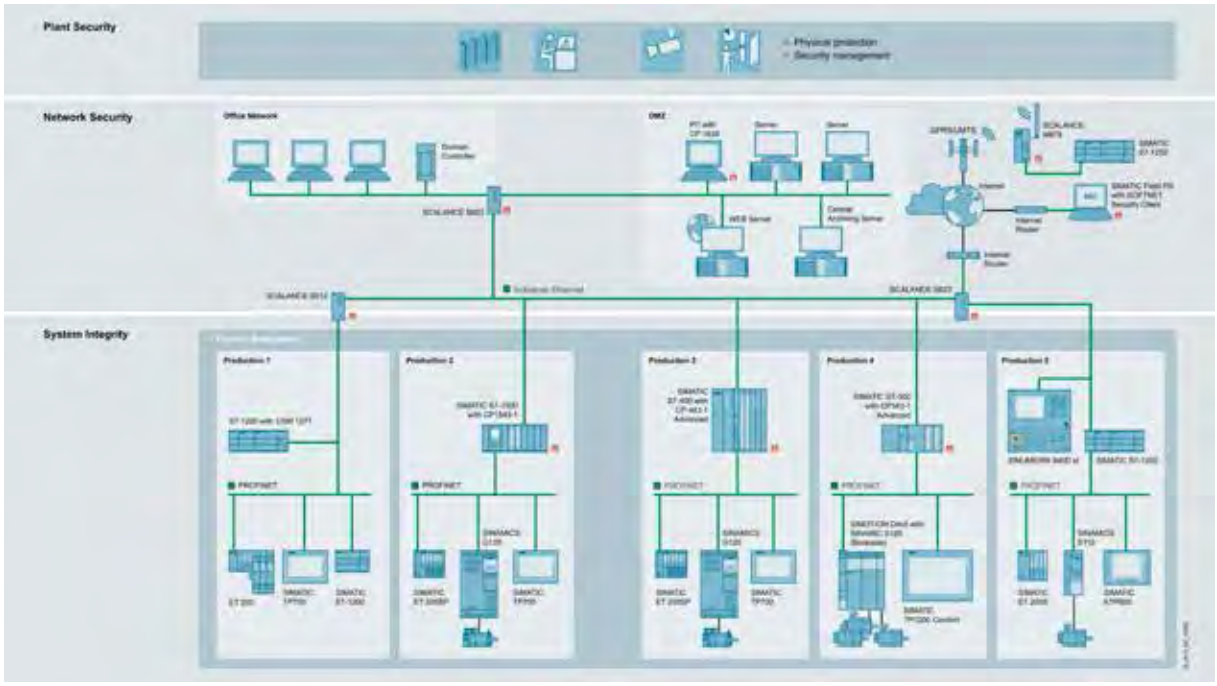


Fig. 8: Implementation of a comprehensive security concept and in-depth defence with the elements of plant security, network security and system integrity.

Fig. 9: With a comprehensive security concept for secure automation

Products and systems: Security-hardened and tested products and special security components and functions, which are tailored to the requirements of industrial automation.

This results in a comprehensive approach, which provides companies from all branches of industry with a way to a secure production network. SST

Experts' Commentaries On The Threats That Manufacturing Environments Face In The 21St Century & What More Needs To Be Done To Ensure Safety & Security

Security concerns today, of course, are important. The economic downturn has caused more thefts in manufacturing facilities. Meanwhile, raw materials like lumber, copper and steel is at an all-time high. Therefore, we see a great demand for this vertical market. Last year, we participated a forum in Bangkok which is designed for manufacturing facilities and industrial parks. It proved that many factories value their security system very much.

We believe the security system in manufacturing facilities can prevent theft, provide quality control and monitor the safety of facilities. Today, there is huge competition in every industry. Every company has their core technology to keep them ahead in their market. Therefore factories rely on high-level security to guard their core technology and raw materials from being stolen. Video surveillance can also ensure their quality. Using video surveillance, can help you control product quality as well as make the whole process faster and more efficient. Meanwhile, surveillance cameras can be placed near dangerous machinery to monitor automated processes safely, or to protect employees from harm. This has been a popular use for video surveillance cameras for years, and has grown more efficient as technology has advanced.

Manufacturing facilities are usually large-scale, so IP and NVRs are a perfect solution as people can easily fetch the video image from the control room and easily manage all cameras. This is especially helpful if you manage a large-scale factory or in multiple locations. NVRs allow security managers to perform more active security duties (e.g. foot patrols) instead of staring at a video monitor for hours at a time. In conclusion, video surveillance systems do not just protect buildings and people. They have an importance in ensuring that enterprises stay competitive in growing and fierce markets.

Tim Shen
Marketing Director,
Dahua Technology

Oh Tee Lee
Regional Director, South Asia Pacific Region, Axis Communications

Manufacturing facilities, factories and warehouses normally contain very valuable raw materials and goods that are attractive to thieves. Graffiti and vandalism that happen at night, are also often seen as an unavoidable nuisances to many manufacturing facilities. These type of crimes subsequently causes millions worth of damage that can ultimately lead to loss of revenue. Apart from just being threathened by crimes, manufacturing companies need to consistently watch every activity in the facility to manage their employees' health and safety.

The challenge that these manufacturing companies face is the ability to monitor every inch of their facility. Therefore it is important to have an efficient surveillance system that works round-the clock to ensure safety and security. Several industries have chosen Axis network video solutions to exercise capabilities like automatic alerts when someone enters the perimeter or a restricted area, night-vision and thermal images, HDTV-quality video images with exceptional level of detail real-time access to live and recorded images and easy-to install, outdoor-ready cameras. By leveraging on the the Internet, Axis' IP camera surveillance enables remote viewing and recording from anywhere and anytime. In addition, the large amount of Axis network cameras that have been deployed all over the facility can be managed, monitored and controlled from one central point.

Experts' Commentaries On The Threats That Manufacturing Environments Face In The 21St Century & What More Needs To Be Done To Ensure Safety & Security

Steve Ma
Executive Vice President,
VIVOTEK

With the increasing automation of a manufacturing industry's production line, the implementation of a well connected and intelligent IP-based surveillance system with features such as high image quality, real-time monitoring and intelligent video content analysis is becoming more vital to the business's success since the system is able to make a great contribution to the smooth operation of the entire plant and also for seamless security all over the site. From a smooth operation perspective, IP-based surveillance can monitor production lines in detail to ensure every move by the operators or machine operation is on track. With IP-based surveillance, managerial staff are able to effectively and efficiently solve any error or accident that may occur on the production line. From a security perspective, suspicious behaviours, cars, or objects can be easily recognized by the intelligent function of the surveillance system. The notification alarm will be triggered and the administrative staff or security guard is able to take immediate actions. Hence, an intelligent IP-based surveillance system can not only effectively solve the security problems and improve management efficiency, but also ensure a safer working environment for employees.

Dr. Magnus Ekerot
CEO MOBOTIX AG

Be it monitoring congestion on the conveyor belt, securing the utilities room, long-term storage of test benches or remotely monitoring production machines: Modern IP camera systems perform analysis and monitoring tasks, independently send alarm messages and enable reliable remote diagnosis. This way, it is possible to reduce machine downtimes and speed up workflows, among other things. This creates plenty of opportunities for industrial companies to save both time and money. In short, it will be difficult for companies without modern video solutions to work efficiently in the future. Both users and manufacturers of video systems have recognized the trend. Some features of security systems are required universally, such as high image quality, low power consumption, low maintenance costs and efficient network load, while use in industrial and rough conditions places additional high requirements when it comes to weather-proof qualities and stability as well as the density and corrosion protection of the cameras. Models certified according to the industrial standard IP65 guarantee full functionality, even in extreme environmental conditions. IP cameras that function without any problems under adverse conditions in temperatures ranging from -30°C to +60°C (-22°F to +140°F) significantly extend the operational scenario.

Operating in an environmentally friendly manner is increasingly topping the agendas of industrial companies. There is backlog demand in many places in the area of video security. Here, a decentralized concept offers a future-proof solution. A system like this requires lower network bandwidth, as data is processed and stored in the camera itself, meaning the high-resolution images do not have to be constantly transferred for analysis. Network cameras do not have to be connected to a PC. They operate independently and can be connected to any compatible IP interface that is connected to the network.

Experts' Commentaries On The Threats That Manufacturing Environments Face In The 21St Century & What More Needs To Be Done To Ensure Safety & Security

The common requirements in the manufacturing sector include the delivery of goods on time where JIT (Just-in-Time) is in most manufacturers' delivery philosophy. In this industry, the trend is the shifting of manufacturing plants from high-cost manpower regions to lower cost manpower areas; this will continue to evolve in the 21st century. Moving from a trained to untrained workforce has driven manufacturers to invest in video technology to help support their operations."

Video has now become a tool for manufacturing plant supervisors and managers to monitor their work force, to observe their behaviour and be able to manage them better. For example, video can help alert to and review mistakes made by operators (or proper procedures), and the video can be played back and exported as training material not only to retrain an operator but also as video for training to the general workforce.

Investing in sensors or detectors that are integrated with video can also help reduce manpower needs in production sites, for example to perform high-risk tasks that can have higher incidences of injuries to human beings. We have installations with sensors linked-up to video that can easily send video to the central Milestone XProtect® Smart Wall when there is a situation that triggers the sensors/detectors to show the video being observed in the command centre or operation centre. This provides important information whether to send in manpower to fix the issue or to wait for time to reduce the risk before human beings can enter the premise.

Sunny Kong
Sales Director, Asia,
Milestone Systems

We would like to invite Security Professionals to share your opinions and perspectives for the Pundit Perspective section in the May/June Issue of SST! This issue is centred around the Retail & Hospitality Vertical Market. The topic we would like you to comment on is this:

What security challenges do retail environments face, and what strategies should be put in place to overcome them?

Your submission must include
(A) Commentary on your perspective (not exceeding 200 words) with your Name, Current Job Title and Company name
(B) A high resolution image yourself

For Security Professionals who are keen on being featured in this section, please drop me an email with the above-mentioned details to the following email address: sst@tradelinkmedia.com.sg

Southeast Asia's Largest Security, Fire and Safety Industry Exhibition

Visit ifsecsea.com

3-5 September 2014, KLCC Kuala Lumpur, Malaysia

Meet Over 7500 security and fire purchaser from 36 countries

IFSEC Southeast Asia

COMMERCIAL & GOVERNMENT SECURITY • FIRE • SAFETY

Meet the industry's senior government and private purchasers at the region's key security, safety and fire exhibition

IFSEC Southeast Asia provides the perfect platform to:

- Conduct market research
- Develop your market entry strategy
- Establish and strengthen your supply chain by meeting existing and prospective partners
- Network and position your brand within the industry
- Launch new security and fire products to the Southeast Asian market
- Showcase and sell your solutions to senior end users from the private and government sectors

Part of:

IFSEC Global
Connecting the Security and Fire communities

Incorporating:

CYBERSEC Asia
PROTECTION • INTELLIGENCE • CYBER SECURITY

Supported by:

Ministry of Home Affairs Malaysia

Ministry of Urban Wellbeing, Housing & Local Government Malaysia

bsia
ASIS
CyberSecurity MALAYSIA

Contact Us:

MALAYSIA
Ms. Rina Fadzil
+6-03-2176 8788
Rina.Fadzil@ubm.com

ASEAN
Mr. TJ Tan
+6-03-2176 8788
TJ.Tan@ubm.com

REST OF WORLD
Mr. Kristan Johnstone
+44 (0) 20 7921 8057
Kristan.Johnstone@ubm.com

Organised by:

UBM

Integrating A Smart Focus System Into Surveillance Cameras

By: Steve Ma, Executive Vice President, VIVOTEK

Introduction

For many applications, surveillance cameras must be installed in less accessible locations high above the ground so as to prevent tampering and to ensure they have a broad, unobstructed view of the area to be monitored. It is often difficult and time-consuming to perform installation because the cameras typically used for such applications also require focus to be set manually, a process that introduces the possibility of error that will require physical access to the camera for another round of focus configuration.

Naturally, any maintenance to be performed on such cameras after their installation is equally time- and labour-intensive. This can particularly be a problem for outdoor cameras such as those used to counter vandalism or property theft, because of their exposure to large and rapid fluctuations in temperature. These extremes in temperature cause components in the camera which are constructed of different materials to expand and compress unevenly, leading to a loss of focus, which must be manually re-adjusted in the case of conventional surveillance cameras. In some situations, noticeable deterioration in focus may occur in a mere matter of days.

When a site has a large number of such cameras deployed outdoors, maintaining optimal focus to ensure reliable surveillance can result in significant overhead in terms of the additional time and labour resources needed.

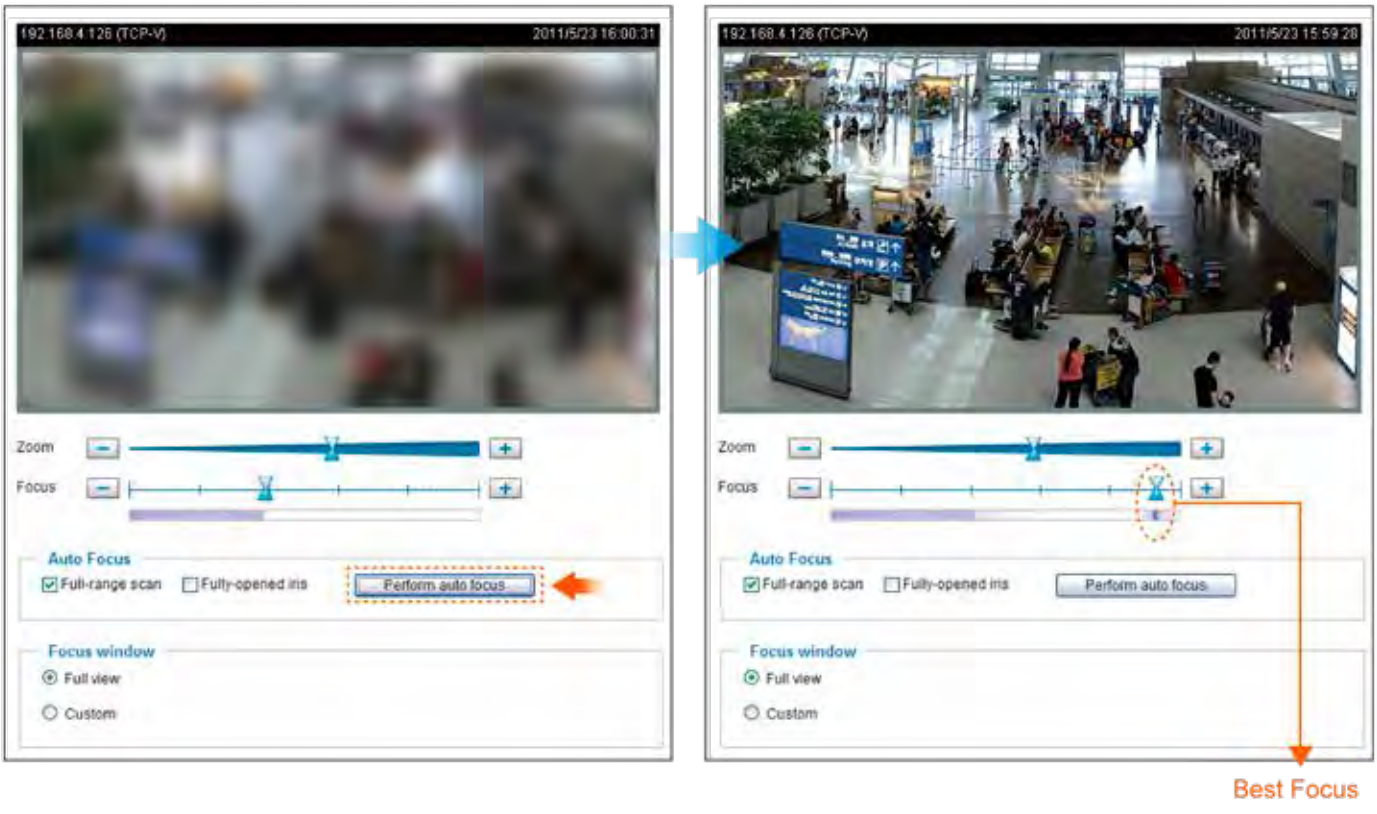
Smart focus systems

To overcome these liabilities, surveillance vendor VIVOTEK has developed a smart focus system. A smart focus system may consist of several elements. Central to such a system is a remote focus utility, which allows users to adjust camera focus remotely. With the help of a stepping motor lens, a user can make adjustments to focus without physical access to the camera.

This basic functionality can be augmented to provide additional features or enhance user convenience. For example, an advanced remote focus capability provides the flexibility to automatically maintain proper focus when zooming in or out, ensuring adequate image quality as focal length is changed or when a specific field of view is required. In addition to reducing the maintenance overhead for surveillance cameras, remote focus offers a convenient way to adjust the view of a monitored location while meeting specific resolution requirements. The flexibility that a smart focus system enables can make powerful additional functionality possible as well.

For example, a feature might be provided to allow users to define a region of interest in the camera's field of view by setting a focus window in the interface. At the user's prompting, the system can then calculate a focus value based on the dimensions of the focus window, automatically providing the best possible image quality. A different type of optimization is possible with focus assist integrated in a smart focus system. A focus assist feature adds a graphical and numerical indicator of the current focus value, making it easier to fine-tune focus. This capability is especially valuable in high-megapixel cameras because their wide field of view and high level of detail make it difficult to distinguish on a small analog monitoring screen whether an object or person of interest is completely in focus or not.

An example of a vendor moving aggressively to adopt smart focus systems in its cameras is Vivotek. Vivotek's implementation of a smart focus system includes all the elements described above—remote focus, focus windows, and focus assist.



Remote focus – lens with stepping motor iris

Vivotek's remote focus capability is available through a web browser interface. Users can manipulate a slider to adjust focus, with auto-focus options also accessible in the same window. The ability to change zoom settings is controlled with another slider positioned just above the focus slider for extra convenience, since adjustments in the two are typically made consecutively. It is recommended that the zoom multiple first be adjusted to the desired value, which will determine the focal length. Then click the "Perform auto focus" button, and the optimal focus value will be set automatically, with the focus slider bar reflecting any changes made dynamically.

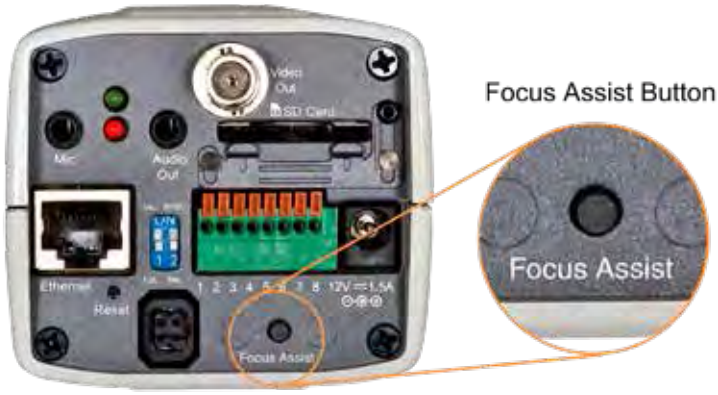
Remote focus – Define a region of interest by focus window

Users can set a focus value by scanning the entire field of view, or by defining a region of interest. If the latter option is chosen, the region can be set by either dragging out a rectangle or by entering the number of pixels for its width and height in fields provided in the web browser interface. The former provides an intuitive and quick way to define the region of interest, while the latter is particularly useful when a specific resolution is desired.

Focus assist – hardware and user interface

The focus assist functionality is enabled with a hardware button on Vivotek's cameras. Once enabled, a focus value indicator appears on-screen in the web browser interface. In addition to a graphical representation of the current focus value, the indicator provides both the actual focus value number and a number corresponding to the optimal focus value. The indicator thus provides a simple and precise way to adjust focus to achieve the best possible picture quality.

Article courtesy of Vivotek Inc.
www.vivotek.com SST



THE 13TH ASIAN INTERNATIONAL SECURITY, SAFETY AND FIRE PROTECTION SHOW & CONFERENCE

ASIAN SECURITEX 2014

www.asiansecuritex.com

7–9 MAY 2014

HONG KONG CONVENTION & EXHIBITION CENTRE

FOR ALL YOUR SECURITY NEEDS

- Meet **500** leading international suppliers
- Shop **10,000+** innovative products and solutions
- Meet and network with key decision makers
- Learn from an array of insightful educational events

Featured Event:

Asian Securitex Conference 2014

- Asia's Most Reputable Event for Security and Fire Protection themed on **"Meeting the Challenges and Opportunities – in a changing Security Environment"**
- Supported by Hong Kong Police Force and 4 leading security associations
- Get insights of the upcoming security trends and technologies that lead you to a safer world

REGISTER NOW!

www.AsianSecuritex.com

Asian Securitex Conference Advisory Panel:

ASIS International Hong Kong Chapter

Asian Professional Security Association (APSA) Hong Kong Chapter

Hong Kong Police - Crime Prevention Bureau (CPB)

Hong Kong Security Association (HKSA)

International Professional Security Association (Hong Kong) (IPSA)

Organiser:

ALLWORLD EXHIBITIONS MEMBER

Hong Kong Exhibition Services Ltd
Tel: +852 2804 1500
E-mail: exhibit@hkesallworld.com

Egyptian Cement Producer Heightens Security With Megapixel Cameras

The Customer

Suez Cement, the largest cement producer in Egypt, operates an industrial network of five cement production facilities in Suez, Kattameya, Tourah, Helwan and El Minya. The company has a long-standing history in the Egyptian market and is innovative in launching new brands and products to meet market needs. The company's five plant facilities use state-of-the-art technology to deliver quality cement to Egyptian and export markets.

The Challenge

Needing a day/night video surveillance system for its plants, Suez Cement wanted to minimize the number of cameras required for full coverage without compromising on video quality. Using fewer cameras and minimizing infrastructure would meet their objective of lowering system costs.

The Solution

Desiring to install a new video surveillance system, Suez Cement turned to G4S Egypt. The integrator leveraged the benefits of Arecont Vision's megapixel cameras to convince the customer to go with an IP system with higher megapixel resolution rather than using analog or standard resolution cameras.

"G4S Egypt chose Arecont Vision megapixel cameras to cover important areas in the factories to meet the specific needs of the cement production environment," said Ahmed Said, G4S systems director. Megapixel camera views provide license plate recognition in some areas and packing details and security standards in other areas.

Three different locations use a combination of Arecont Vision 1.3- and three-megapixel cameras, connected locally to a network video recorder (NVR) and across leased lines to a centralized location. The Arecont Vision MegaDome® AV1355DN 1.3 Megapixel H.264 Day/Night Dome Camera, an all-in-one integrated camera, lens and IP66-rated dome housing provides 1280x1024-pixel images at 32fps. For higher resolution, Suez Cement used Arecont Vision's three-megapixel Day/Night cameras providing 2048x1536-pixel images at 15fps. Each camera uses Arecont Vision's MegaVideo® image processing at billions of operations per second. Both cameras are day/night versions with a motorized infrared (IR) cut filter, which automatically switches the camera from colour to black-and-white mode at night to allow 24-hour surveillance. Other capabilities include motion detection, image cropping, region-of-interest viewing and forensic zooming. The cameras use H.264 compression to minimize bandwidth and storage requirements while maintaining real-time image frame rate. Compact camera sizes enable easy installation in outdoor housings. Power-over-Ethernet (PoE) supplies camera power on the same Ethernet cable used for data transmission.

The Benefits

"Based on Arecont Vision's diverse megapixel offering, picture quality and reliability, the project turned out to be a big success for all parties involved," commented Said.

The cameras' H.264 codec maintains excellent image quality while keeping video file sizes to a minimum. Imaging can be magnified digitally while preserving critical image details, and moving the enlarged image area up and down and from side to side provides a virtual pan-tilt-zoom (PTZ) function. A single megapixel camera can be used in place of several analog cameras, resulting in significant time and cost savings as well as a reduction in infrastructure. Multi-streaming provides up to eight concurrent, non-identical video streams, each with a different frame rate, bit rate, resolution and image area. Region-of-interest (ROI) viewing enables an area of the screen to be viewed in higher resolution than the surrounding image, providing superior detailed images while reducing network load.

At Suez Cement, the features of the megapixel cameras translate into much greater system functionality at lower cost with a faster return on investment (ROI). SST

Chemical Products Manufacturer In Johannesburg Elevates Security With Enhanced Perimeter Protection

Background

AECI's Chemserve Systems (Pty) Ltd provides chemical products to a diverse range of industries. Their site at Chloorkop, a small industrial town just outside of Johannesburg, was being monitored by four different analog camera systems, making effective security surveillance extremely difficult. Hence, a decision was made to consolidate and upgrade the existing solution.

The Solution

Seasoned IP CCTV and systems integration provider, SLA Group, designed and installed a cohesive solution, using Axis network cameras, which offers complete perimeter coverage and extensive internal monitoring capabilities. The main entrance control room maintains centralised control of the entire system, while the IT server room records and acts as a main buffer for the whole system, thereby reducing the risk of an incident or intrusion, failing detection by security personnel.

The Result

The vacant land that borders the north and west sides of the Chloorkop AECI's site no longer poses a threat to the security of the premises. Previously this open area was responsible for continuous trespassing and the

removal of large quantities of valuable stock. Thanks to the installation of Axis thermal network cameras, even complete darkness cannot offer criminals a place to hide.

Protecting essential stock

AECI – Chempark Division's supply an extensive range of specialty chemical products and related services for industrial use across a broad spectrum of customers in the manufacturing and mining sectors, mainly in South Africa and in Southern Africa.

"It is imperative that warehouses, administrative buildings, workshops and storage tankers are under 24-hour surveillance. This ensures that our customer has complete control of the entire site at all times," remarked SLA Groups Alexandre Teixeira. "Any movement after working hours will automatically trigger an alarm that security officers can react to immediately. The Axis PTZ network cameras provide a visual of what security can expect to encounter during these responses."

A fortified boundary

SLA Group has over 24 years' experience in the design, manufacture and installation of CCTV and automation systems for the power generation, mining, iron and steel and chemical industries. This sustained involvement allows SLA Group to offer best value for money solutions without compromising on quality, reliability or long-term stability.

"We realized that AECI - Chempark perimeter was a major security issue that required careful attention and meticulous product investigation," said Alex Teixeira. "The AXIS Q1910-E Thermal Network Camera presented itself as the most intelligent option." AXIS Q1910-E uses thermal imaging to detect people objects and incidents in complete

darkness or challenging conditions such as smoke, haze, dust and light fog.

For a long time thermal imaging was too costly for any application outside of the military, however, as price is driven down by improved technology, it is rapidly becoming a force to be reckoned with in the security and surveillance industry. Creating images based on the heat that is generated by any object, person or vehicle and requiring no additional light source, thermal cameras are ideal for securing perimeters and dark or shadowed areas.

Crisp, high definition images

The main entrance to the site and the internal roads are monitored by AXIS P1344 Network Cameras. The first-rate HDTV image quality of AXIS P1344 ensures that control room personnel are able to view video surveillance of the highest possible resolution in the zones where clarity and detail are absolutely critical.

"Picture quality and ease of installation were just two of the many reasons that we selected Axis as our IP partner for this project," remarked Alex Teixeira. "Every single corridor, intersection, entrance and exit needs to be accessible by the surveillance cameras. The versatility of the Axis-based solution makes this entirely possible." SST

Spanish Security Specialist Prefers Thermal Imaging Cameras For Perimeter Protection Of Solar Parks

Background

OMEGA GROUP, based in Sevilla, Spain, offers a comprehensive range of surveillance and security services, including the installation and maintenance of systems and equipment for intrusion and fire detection, CCTV, access control, etc. One of the company's main areas of expertise is perimeter protection of solar parks. As an increasingly important provider of electricity across the globe, solar parks need to be effectively secured. The threats these installations face are the same as for any other energy producing facility: vandalism, sabotage and terrorism.

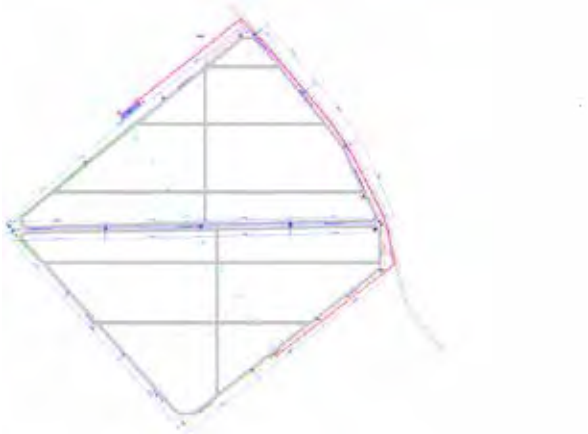
Based on a proven track record for perimeter protection projects across Spain, Omega Seguridad has also been able to offer its expertise to solar park projects in other European countries like Portugal, France, Italy and Romania.

Solar park surveillance project in Romania

For a new solar park, located in Sebis, Arad, Romenia, Omega Seguridad installed 22 thermal imaging cameras for perimeter surveillance purposes. The new park is the country's largest and also one of the largest parks in Europe.

The park has been developed by Bester Generación, a leader in the renewable energy market, specialized in the promotion, construction, operation and maintenance of infrastructures for the production of clean energy. It stretches across 200 hectares and includes some 72,000 photovoltaic panels, amounting to 15 MW of power. The new solar park is said to ensure the need of energy for around 100,000 people.

The total perimeter, including two separate confined areas of approximately 21 kilometres, could be covered with a total number of 22 cameras. On average, this amounts to approximately one thermal camera per 190 metres.



SR series

For this particular project, Omega Seguridad relied on FLIR's SR series of surveillance cameras, offering high quality thermal imaging in any night or daytime environmental conditions. More specifically they chiefly used the SR-313 camera with 35 mm lens and 320 x 240 resolution, next to the SR-324 camera with 19 mm lens and 320 x 240 resolution. The SR-Series of security cameras provide high contrast imagery optimized to get the most out of video analytics software. In this case, video analytics was provided by Spanish company Davantis.

FLIR's SR series of surveillance cameras, offer high-quality thermal imaging in any night- or daytime environmental conditions.

The SR-Series cameras provide high contrast imagery optimized to get the most out of video analytics

Surveillance technologies

Omega Seguridad usually offers two options for perimeter protection to its customers: CCTV cameras and thermal imaging cameras. Although traditional CCTV systems are effective for security and surveillance applications, they are not able to see in total darkness. As a result, they have to be complemented with additional lighting, which again allows the cameras to look at night for a certain distance.

Antonio Millán Fernández, project manager at Omega

Seguridad, explained why his company always makes an extra effort to convince the customer to choose thermal imaging cameras: "Thermal cameras can see much farther than traditional CCTV cameras and therefore you need less of them. So in short: less cameras, less issues."

Smaller investment for thermal imaging

Although a thermal camera is still more expensive than a visual video camera, the investment cost for perimeter surveillance will still be lower, since you need fewer camera units. Fewer cameras also means that there will be less required investments for all camera-related equipment (meaning: all equipment that is needed to get the camera operating properly and to get the video signal onto the control room screen).

All these additional costs need to be made per camera unit. By reducing the number of required cameras, thermal imaging allows customers to make significant savings with the camera-related equipment and civil works. On top of that, thermal imaging cameras need no lighting equipment whatsoever and will operate with the same accuracy during night and day. Last but not least, Omega Seguridad calculated that the overall power consumption of a project with traditional CCTV systems is about 50 per cent higher than the power consumption of a project with thermal cameras. This results in considerable savings in the end user's electricity bill.

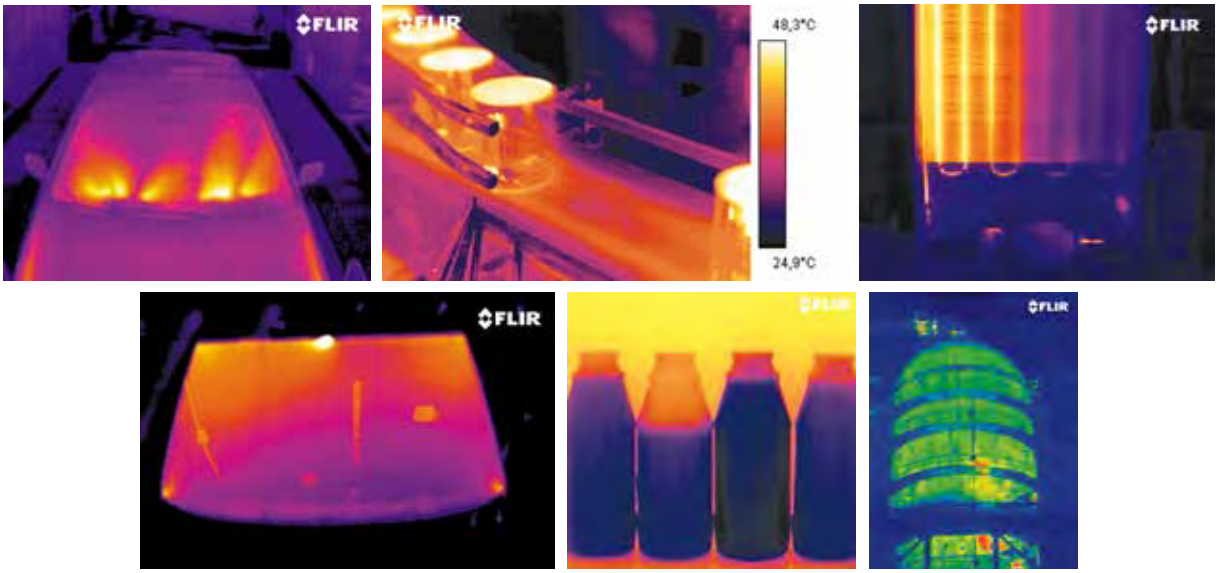
"For distances between 60 and 120 metres that would require two conventional cameras, but only one thermal camera, the cost of equipment involved in both systems would be equivalent," commented Enrique Delgado Torres, engineer and project manager at Omega Seguridad. "For distances between 120 and 180 metres where three conventional cameras would be required, the equipment associated to the thermal system becomes more economical. Longer distances will make the advantage bigger."

"The more bends and curves a perimeter has, the more camera positions you will need to have a sufficiently good view," commented Vicente Nanclares Ocio, director of the engineering department. "Luckily for us, solar parks generally tend to have straight shapes, so this allows thermal cameras to see even farther than 180 metres."

Better performance with thermal imaging

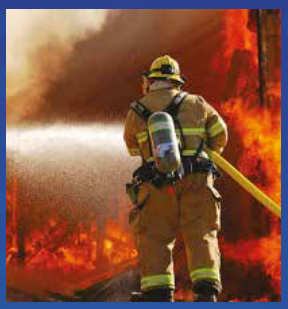
The lower overall investment is not the only reason why Omega Seguridad prefers thermal imaging for the Sebis project in Romania. Thermal cameras also have a higher accuracy and they generate fewer false alarms, which ultimately results in less frustration and a lighter workload for the control room operator.

"Obviously, we no longer experience light-related false alarms," commented Ocio. "Sometimes, car headlights can set off false alarms, but since thermal cameras are unaffected by light, they are also not disturbed by it. Thermal cameras also allow us to see better through fog. Sometimes, the fog can be so dense that traditional CCTV cameras are unable to see through it." SST



BOOK YOUR STAND NOW!

3 - 5 March 2015
Singapore

GLOBAL SECURITY ASIA 2015

International Exhibition & Conference on Counter Terrorism & Security



Be a part of Asia Pacific's Premier International Exhibition and Conference on Counter Terrorism, Internal State Security, Law Enforcement and Civil Defence

www.globalsecasia.com

Korean Cosmetics Manufacturer Uses Network Cameras For Round-The-Clock Security

Background

Amore Pacific Osan Integrated SCM (Supply Chain Management) Base is a large-scale plant built in July 2011 with the goal of becoming one of the 'Top 10 Cosmetics Companies in 2015, with sales of KRW5 trillion' and effectively coping with an ever-expanding global business. Osan Integrated SCM Base is a huge plant: the lot size is 224,400m^2 with a building area of 89,009m^2 housing environment-friendly production, logistics, and loading facilities. In addition, this world-class facility manufactures 15,000 tons annually and ships 60,000 boxes daily. Immediately after its completion, for efficient maintenance and management of this large integrated base, it was necessary to monitor the logistics and technology inside the plant and laboratory, control visitors and be alert for intruders.

The Challenge

It is not easy to effectively monitor this large facility and closely restrict access. In addition, as the plant is divided into several quarters, i.e. the main building, the design building, the logistics building and the research building, it required a solution that would be capable of simultaneously monitoring the entire plant and individual quarters.

The Solution

The need to monitor the real-time status of the plant, work situations and outsiders and to protect products and research technology was of the highest priority. To resolve this issue, Amore Pacific adopted the Siveillance Fusion system from Siemens for the purpose of monitoring key locations and managing access to the facility, and introduced an Axis network camera solution to effectively monitor a wide area and reduce costs.

The Result

The Amore Pacific SCM Base in the Gyeonggi Province installed AXIS 233D, AXIS P1311 and AXIS 216FD Network Cameras to implement a system capable of real-time monitoring and efficient access control of the entire facility. The solution with the PoE (Power of Ethernet) function transmits high-resolution images and enabled the simultaneous power supply via the network cable, thereby ensuring convenient installation and reduced costs.

In particular, Siemens' Siveillance Fusion system made it possible to effectively control and manage system users at various levels, from security managers inside the company to outsourced guards, thereby adding outstanding flexibility and efficiency to security. Combining the Axis network cameras and the Siemens Siveillance Fusion, they built a system that satisfied the technical requirements and reduced costs, ensuring perfect security for the Osan SCM Base, and helping it achieve its dream of becoming the world's best production and logistics hub.

Network cameras make it possible to quickly grasp site situations

Amore Pacific placed the greatest emphasis on sizing up situations at the site quickly and accurately in implementing the video control system at the Osan Integrated SCM Base. They needed a system that could not only effectively control outsider intrusion, but also save the images in case of an incident.

To cover the wide area of the Osan plant of Amore Pacific, they selected the effectively designed IP-based Axis network cameras that are not burdened by excessive cabling. Accordingly, they installed network cameras in appropriate locations of the seven quarters, including the logistics building, the research building and HQ to enable real-time monitoring. As the central control room conducts monitoring in real time, they implemented a system that can quickly grasp the situation at the site and take appropriate action in case of an incident.

High-resolution video data is efficiently saved and integrated

Amore Pacific installed multiple types of network cameras at the Osan Integrated SCM Base of Amore Pacific to satisfy the specific needs of each area. For surveillance of the area outside of the plant, they installed AXIS 233D PTZ Network Cameras, which have outstanding image quality and are capable of precise monitoring of objects as far away as 160m with 35X optical zoom and 12X digital zoom. Accordingly, it is possible to quickly and precisely respond to vehicles parked outside of the plant or external intruders. Also, inside the buildings and in frequently accessed areas, they installed AXIS P1311 Network Cameras, which are ideal for indoor monitoring because of their excellent image quality, along with AXIS 216FD Dome Network Cameras, which deliver outstanding professional indoor video and audio surveillance so that it is now possible to get real-time information on people entering and leaving the plant and monitor the situation throughout the site.

The surveillance images of the Axis network cameras are managed in connection with the Siveillance Fusion system, an integrated system from Siemens. As a result, the central control room can monitor the access control data of the Osan Amore Pacific plant, people entering and leaving the plant, and the 135 cameras at one glance so that it is possible to understand situations immediately, making more efficient and effective monitoring and management possible. In particular, the movement and voice recognition function of the Axis network cameras enable recognition of movement and noise after work. As the sound and movement are recorded only when triggered, a perfect uninterrupted security system is now available twenty-four hours a day, seven days a week. SST

Dahua Technology Takes off in Morocco

Background

Automotive Wiring System, Morocco (AWSM) is a leading provider for Volkswagen Polo, offering reliable wiring harnesses. Located in the Tangier Free Zone (TFZ), it has a mass production order demand that it has to meet each day.

To further standardize and regulate the production procedure as well as ensure the product quality, AWSM has moved ahead to adopt Dahua cameras and have them installed in its workshops and offices. The selected camera model — DH-IPC-HFW3300 is a three-Megapixel full HD network camera that not only has outstanding image quality, but also nice interoperability and compatibility for future integration.

Featuring 1/2.8 inch three-Megapixel SONY progressive scan Exmor CMOS image sensor and advanced TI DaVinci Series DSP, coupled with H.264 video compression and MJPEG image capture, DH-IPC-HFW3300 presents a wonderful full HD image quality and crisp and sharp detail reproduction.

The built-in ICR filter provides automatic day/night switching functionality, adjusting the image from colour during the day (and in low-light conditions) to monochrome at night (or in extremely poor lighting conditions) while only requiring a minimum illumination of 0.01LUX. This camera also supports C/CS auto iris lenses, which automatically adjust given the lighting conditions to get the best picture in outdoor applications where the light varies constantly. It supports 32GB SD card, PoE, and also subject to ONVIF, PSIA.

Vision

Dahua Technology values the Moroccon market due to its special geographical position and strong economy. William Zhou, the sales manager in charge of the Latin-Africa region, added: "Morocco is one of our important target areas; we will continue to work closely with our regional exclusive distributor, Country Technologie, and participate more in local projects to offer even better products and services to all clients who use our products." The general manager of Country Technologie, Anas also expressed his satisfaction the support from Dahua Technology, he appreciates excellent support from all these years and looks forward to more collaborations. SST

Hong Kong-Based Jewellery Manufacturer And Exporter Enhances Security At Trade Shows & In Offices

Background

Christelle Limited, a Hong Kong-based manufacturing jeweller, has been producing and exporting exceptional jewellery for more than three decades. Known for its unique designs and high quality materials, it participates in more than 30 tradeshows around the world each year. At these shows, and in their international offices, security and staff safety are key concerns.

The Solution

To enhance security, Christelle selected a new digital video surveillance system from Axis Communications. The system is easy for sales staff to set up and operate during tradeshows

as well as reliable and powerful enough for around-the-clock office surveillance. The system comprises of advanced and unobtrusive Axis network cameras and Axis Camera Station software. It allows monitoring of real-time and recorded images as well as remote monitoring via an authorized PC or 3G smartphone.

The Result

With this advanced Axis technology in place, Christelle can prevent theft while reducing costs in a more effective way. The cameras capture high-resolution images so that personnel can distinguish individual pieces of jewellery and more readily spot suspect behaviour. Compressed for low-bandwidth IP transmission, these images can even be accessed remotely to confirm false alarms and hence, increase the efficiency of the security team. Furthermore, staff does not need special training, and can also set up or use the new security system.

Moving to fully digital IP-Surveillance

Given the high value of its products, Christelle needs a reliable surveillance system to provide a high standard of security and a safe working environment for staff either in its offices and or in the more than 30 tradeshows it attends around the world each year.

When general manager Ken Ng decided to upgrade the company's surveillance capabilities, he wanted an efficient and easy-to-use system that would deliver the best possible image quality and improve efficiency in both of these environments.

"We had been using CCTV cameras with a digital video recorder at the backend. However, this system did not provide the image quality necessary to properly monitor high-value pieces of jewellery and this put additional pressure on our security team. The technology was also fairly maintenance-intensive and did not allow us to access our security images via the Internet," he explained. Keeping a close watch on small, high-value goods Selecting a system from Axis Communications, the world leader in network video solutions, Christelle first installed a network of about 20 AXIS M3011 and AXIS M3014 Network Cameras and wireless AXIS M1031-W Network Cameras at its Hong Kong headquarters. Each of these cameras offers superior video quality to dramatically improve image resolution—from 352x288 pixels with the CCTV system to 640x480 pixels for distortion-free images and much smoother motion.

Christelle also deployed the powerful AXIS Camera Station IP-Surveillance software to allow it to simultaneously monitor all of its networked cameras from a single PC and

access the system remotely.

The H.264 compression available with all of the innovative Axis network cameras complements the capabilities of the surveillance software. It means that surveillance images of very high quality can be transmitted for viewing and storage using minimal bandwidth, either to computers on the corporate network or securely over the Internet. Christelle personnel can even use their 3G smartphones to view real-time and archived images from an individual location or single camera.

Fast deployment and unobtrusive design

With Axis playing a major role in the deployment, the system was up and running in Hong Kong within two months. At tradeshows, the Axis system is easily set up by the sales staff manning the booth—no technicians are required. In keeping with Christelle's sophisticated image, the cameras are also all very unobtrusive. The ultra-slim profiles of the AXIS M3011 and AXIS M3014 make them difficult to spot and the compact AXIS M1031-W features passive infrared sensors for detecting movement in the dark and a white LED that activates automatically at an event or as requested by the operator.

On-going benefits and major cost savings

While tradeshow loss prevention is the most dramatic benefit of the Axis system deployment, Christelle has also achieved considerable cost savings - it has now deployed the new Axis security solution at its offices in Los Angeles and New York, with plans to use it in other overseas locations.

"The productivity of our security personnel has increased by around 100 per cent, and this has allowed us to reduce the manpower we need on the night shift. At the same time, the system is much more reliable and easy to operate and so administration and maintenance are down 50 per cent as well," said Ng. SST

Leading Chemical Company In China Strengthens Perimeter Security

The Customer

BASF is one of the world's leading chemical companies. Its portfolio ranges from chemicals, plastics, performance products and crop protection products to oil and gas. The company has been a committed partner to Greater China since 1885 and currently is one of the largest foreign investors in the Chinese chemical industry with major investments in Nanjing, Shanghai and Chongqing. According to BASF's Greater China Report published in 2012, local production enables more intensive collaboration with customers based in Greater China, and improves resource efficiency. BASF posted sales of over $6.8 billion in 2012 and employed 7,305 people.

The Challenge

Protecting BASF's chemical facilities demands high levels of security because of the nature of the operations and their potential for being the target of threats and/or criminal activities. To help safeguard people, property and assets, BASF's security management has implemented a layered security approach that starts with perimeter protection.

Fences and intrusion detection systems only provide limited protection, and false alerts create additional security issues. To provide more comprehensive and actionable coverage, BASF China needed real-time,

PROJECT QATAR

Capture World Leading Construction Opportunities

Held concurrently with:

QATAR STONETECH

HEAVY MAX

Specialized conferences:

LightingTech QATAR

HVACTech QATAR

12 – 15 May, 2014

Qatar National Convention Centre

The 11th International Construction Technology & Building Materials Exhibition

REGISTER NOW TO VISIT!

For More Information,
Please Contact:

Rawad Sleem
Project Manager

Phone: +974 4432 9900
Fax: +974 4443 2891
Mobile: +974 6600 1644
Email: rawad.sleem@ifpqatar.com

ifp Qatar

IFP Qatar, P.O.Box: 22376, Doha - Qatar, Tel: + 974 4432 9900, Fax: +974 4443 2891
E-mail: info@ifpqatar.com, www.projectqatar.com

visual monitoring of the perimeter on a twenty-four hours a day, seven days a week basis, without adding any additional lighting.

The Solution

Working in collaboration with Tyco Fire and Security China, the BASF security team selected Arecont Vision's three-megapixel (MP) AV3135 colour cameras to meet their video security needs. The dual sensor AV3135 also has a 1.3-megapixel true monochrome sensor that provides low-light performance. As the ambient light diminishes, the AV3135 switches to the monochrome sensor to deliver clear, high-resolution surveillance images for identification and recording purposes. The Arecont Vision AV3135 megapixel cameras also provide an increased coverage area for better situational awareness compared to analog or IP VGA cameras; and improved functionality including the ability to digitally zoom into live scenes and recorded video while maintaining high resolution. And because of the cameras' superior day/night capability, no expenses were incurred to install additional lighting.

Another cost-saving benefit of the Arecont Vision AV3135 megapixel cameras is that they are Powered over Ethernet (PoE) which eliminates the need to install local power sources. The AV3135 megapixel cameras are part of Arecont Vision's H.264 MegaVideo® line of cameras that offer bandwidth and storage efficiency of 10x greater on average over traditional megapixel counterparts. The proven results have laid to rest management's concerns about storage space.

BASF's corporate security team was highly impressed with the quality and coverage of the Arecont Vision megapixel cameras when images were compared to analog cameras.

"Arecont Vision megapixel cameras provide the extremely clear images that are needed for security monitoring of the facility perimeter," said Raylene Xie, global account manager, Tyco Fire and Security China. "Even BASF corporate was excited about the difference in quality between the megapixel and analog images."

The increased image quality of megapixel video played the largest role in providing superior perimeter security for the BASF facility. Expanded coverage areas and day/night capability of the Arecont Vision AV3135 cameras also contributed to a successful and effective new system. SST

Ellwood Group Intensifies Security With Megapixel Technology

Background

Headquartered in Ellwood City, Pennsylvania, Ellwood Group, Inc. (EGI) produces engineered, heavy metal sections for capital specialty equipment manufacturers in the United States and around the world. The company's nine operating business units—encompassing multiple plants in Pennsylvania, Michigan, Ohio, Texas and Canada—are dedicated to solving customers' needs for specially engineered forging steels, iron castings, forgings, and other alloy parts.

The Challenge

When making a single speciality steel product that can cost tens of thousands of dollars, it is essential to have the capability to monitor the manufacturing processes and if a problem is experienced downstream, to then have the ability to go back and find the root cause. If a manufacturer can implement process-monitoring technology that quickly, accurately solves manufacturing problems, the system pays for itself in short order.

The Solution

Ellwood Group, Inc. has installed over 250 IQeye HD megapixel cameras and growing, in order to monitor and improve manufacturing processes, in addition to meeting security needs. "We have moved from a test environment over five years ago to now having megapixel cameras deployed at about 20 different locations in our various plants," said Eugene Spadafore, senior network administrator, EGI. "We started out asking, 'How can we improve quality for process X?' Rather quickly we saw the value of closely monitoring manufacturing with the IQeye cameras and now it's a standard in our environment, we use the cameras at every facility." In what is a growing trend, EGI uses its megapixel technology 75 per cent for process control and only 25 per cent for physical security. As a result of using megapixel technology for process control, EGI has seen measureable improvements in efficiency and productivity, resulting in substantial savings. As one EGI location or division discovers the benefits of this kind of manufacturing process monitoring—both live and post-event—inevitably they, too, request cameras.

EGI stores video at each location anywhere from three days to three months, depending on the manufacturing process being recorded. The majority of the cameras are 2.1 MP IQeye Sentinel and 700-series cameras, the newest utilizing H.264 compression.

"Our growth is typically through acquisition," said Spadafore, "once a new company is acquired, the next question is, 'When can we get cameras installed?' We are quite satisfied with how the IQeye cameras have performed in meeting our sophisticated needs. As a result of using megapixel technology for process control, we have seen improvements in efficiency and productivity and that translates into real money." To successfully manage the expansion of the use of IQinVision technology, Spadafore's division has developed a de facto standard, scope of work, and set of specifications for how to successfully deploy the IQeye cameras in each new location. "To maintain consistency and best practices, we elected to be the overall project manager for camera deployment." SST

German Water Treatment & Supply Association Implements IP Security Solution To Cut Costs & Enhance Public Safety

Background

The Trollmühle water supply association in Rhineland-Palatinate (Germany) supplies and purifies water to 24 municipalities, 14,000 households and 43,000 inhabitants. Over a hundred years ago, the network of water pipes covered a mere 110 km whereas today the association has over 400 km of piping with a 2.1 million cubic-meter capacity. The Trollmühle water supply association supplies their drinking water from 25-foot-deep wells and three well shafts via 19 high-level tanks and two underground tanks. The main pumping station and central distribution plant is located in Windesheim where during peak consumption periods, up to 8,500 cubic meters of water are turned over each day. All of the association's external plants, wells and pumping stations are connected back to the central distribution plant from which they are remotely controlled.

The Challenge

Depending on the size of the plant, Trollmühle provides five to 90 cubic meters of water per hour from a depth of up to 200 meters. By way of linking the plants, the association ensures the water supply to the population even during a breakdown of one or several plants. However, because the protection and health of the population come first, Trollmühle water supply association's most important objective is to guarantee the water supply quality and to take the necessary measures to monitor the plant and deter any potential threats or contamination.

Since the 9/11 terrorist attacks, counter-terrorism initiatives have been top priority for many federal governments. This included Germany who amongst other plans, wanted to ensure the safety of its water supply. Therefore, the State Criminal Investigation Department of Rhineland-Palatinate advised all water supply

associations to inspect and evaluate all safety devices and introduce security enhancements.

Since then, the Trollmühle water supply association experienced a break-in, which after investigation, turned out to be a minor occurrence. However, this break-in became the decisive factor for the water supply association to start thinking about investing in a new security solution.

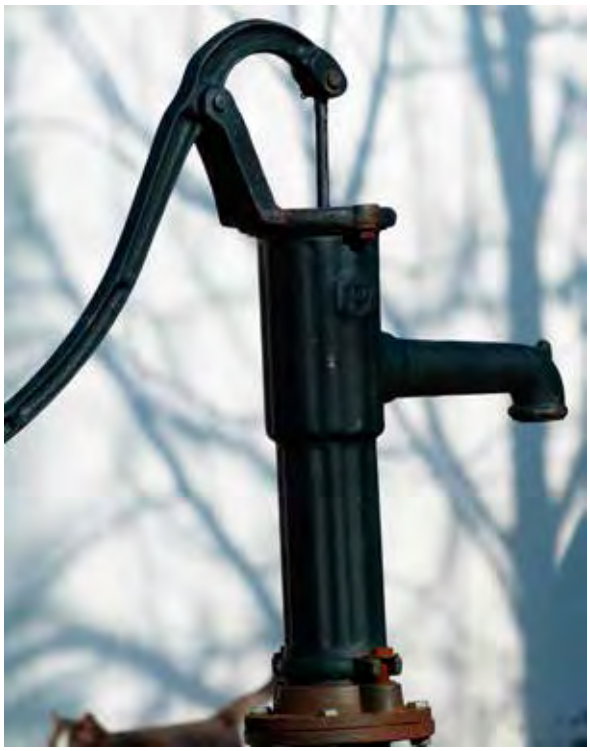
End-User Needs

As per German law, the security solution had to respect DVGW notices W 1001 and W 1002, which stated that all objects–apart from the safety devices which are already in use, such as fences, special locks, alarm systems, must be effectively protected. For this, the water supply association decided that all deep wells and water tanks should be gradually equipped with cameras and the recorded video was to be transmitted to the central control office. Although DVR technology with local video recording and storage was considered, it was deemed not suitable for this application. In the event of another

break-in, the perpetrators would likely take the recording device with them. Marcus Spira, head of the engineering department at Trollmühle water supply association added: "If necessary, I want to be able to immediately see the video in the office without having to first drive into the forest to the tank in question to view or collect footage."

SLK GmbH, a Genetec Value-Added Distributor in Germany, was contracted to assist in deploying a more advanced security solution. Thus the central control office with the main pump station in Windesheim and the seven largest high-level tanks were first equipped with IP cameras and connected back to the central office via the existing telephone lines. However, in time, the Trollmühle water supply association began to realize the limits of their existing and very basic video management software and consulted SLK for a new security platform.

Not only was the water supply association looking for a reliable, user-friendly and scalable system that would allow them to gradually grow their camera count; but they also wanted a software solution that would permit them to unify other systems like access control and other water treatment systems under one platform. SLK thought Genetec's Security Center unified security platform would be the right solution for the job.



The Solution

Genetec's Security Center is a leading unified security platform that blends IP video surveillance, access control, number plate recognition and other third-party business systems within one simple solution. Security Center consolidates live monitoring, video playback, alarm management, configuration and reporting across all systems in a simple and easy-to-use interface. In this case, Security Center gave the water supply association the ability to initially install the IP video surveillance component, Omnicast, with the flexibility to add other components, such as the Synergis access control system, in the future.

Specifically, Sony's RZ50 motorized camera with motion detection and zoom, was installed in the central control office and various vandalism-proof fixed IP cameras from Sony such as SNCDF80P, SNCRZ50P and SNCCH140, were installed at the other locations and connected back to the central control office's system. Since Omnicast comes with highly-advanced redundant and failover features, the new video management system guarantees that all current and archived data will be available at any time, even in the event of a failed component.

To ensure added reliability and privacy of data, Trollmühle water supply association only saves recorded video and data for two weeks. After that, all data will automatically be overwritten. Spira explained "The server on which the video is saved uses redundant array of independent disks (RAID) storage technology. In case of a failure of a hard disk, it can be replaced without any risk of data loss." However, in order to optimize bandwidth and keep the quantity of archived data as low as possible, the water association is using Omnicast's sophisticated multi-streaming feature to configure different video settings for live viewing or recording. For instance, depending on the

setting, a server will record all video from high-priority cameras and then only event-driven video from lower priority cameras.

Similarly, another tool used to reduce network load and save storage space is Omnicast's built-in motion detection algorithm. Certain cameras installed in the water tanks will only start recording when motion has been detected in the system. This feature is also combined with Omnicast's event-action mechanism which dictates the system to trigger specific actions such as start/stop recording, point a camera to a specific pre-set, send email notifications, or trigger an alarm when an event is detected in the system.

The combination of these features provides the water supply association with a highly intelligent tool that helps them immediately respond to only the situations they deem critical. For example, when entering the tank or facility for maintenance and water samples, authorized personnel must swipe their access card to enter which tells the system this is not an important event and does not require recording.

However, in instances where there is no card swipe and motion is detected, the camera will immediately start recording and an alarm will be sent to operators to address the situation. Other key system features of Omnicast that have helped secure the water supply, include the system's open architecture which allowed Trollmühle to preserve their existing hardware; configurable user-access privileges and authenticated user logins that prevent manipulation and falsification of video through an unauthorised access to the system; and easy upgrade paths which enable Trollmühle to increase camera counts and benefit from even more advanced feature sets when they are ready.

The Benefits

According to Marcus Spira, the handling of the Genetec solution is comfortable and convenient. During investigations for example, retrieving information is very simple and the quality of the images is excellent. Likewise, Security Center helps Trollmühle water supply association build consistent workflows across their system and set standardized procedures to address critical situations. All in all, this unified platform simplifies operations and helps streamline the operator's daily tasks in ensuring the safety of Trollmühle's water supply.

To date, not one single break-in has occurred since video surveillance system and cameras have been installed in the central control office. Combined, the Sony cameras and the Omnicast system act as a deterrent to any vandalism, theft or sabotage. In the event of any such intrusion in the future, Trollmühle water supply association can now quickly identify to the reason for break-in and apprehend suspects faster than ever before. Further plans to offer remote access to local authorities are also being discussed to enhance situation awareness for first responders and speed up investigations. The plant manager, Willy Orben, added: "Genetec's solution makes it possible for us to quickly make sound decisions." SST