

a&S

Tecnologie e soluzioni per la sicurezza professionale

ITALY

www.asitaly.com

aprile 2017
anno VIII **44**

Banche:
dove la sicurezza
fisica sposa
la sicurezza logica



Ksenia
security innovation

Vecchi cavi addio,
arriva il nuovo
regime CPR

ONVIF, profilo T e
H.265: l'evoluzione
della compressione

Controllo
perimetrale
degli accessi



SENSORI DA ESTERNO A TENDA DOPPIA TECNOLOGIA

AGATE

- anti-mascheramento attivo sull'IR
- EN 50131 Grado 3
- regolazione della sensibilità del circuito con il trimmer

AOCD-250

- fa parte del sistema wireless bidirezionale ABAX
- configurazione da remoto, tramite il DLOADX della sensibilità di rilevazione
- controllo del livello della batteria

Caratteristiche comuni

- Possono essere utilizzati sia all'interno che all'esterno
- Grado di protezione IP54
- Doppia tecnologia PIR + MW
- Resistenza alle intemperie e agli sbalzi di temperatura
- Compensazione automatica di variazioni della temperatura: funzionalità garantita per intervallo di temperatura da -40°C a +55°C

Ampia copertura

I rivelatori hanno un angolo di rilevazione di 10° orizzontale e 90° verticale e un raggio di azione di 14 m

Facile installazione mediante BRACKET dedicato



Satel®

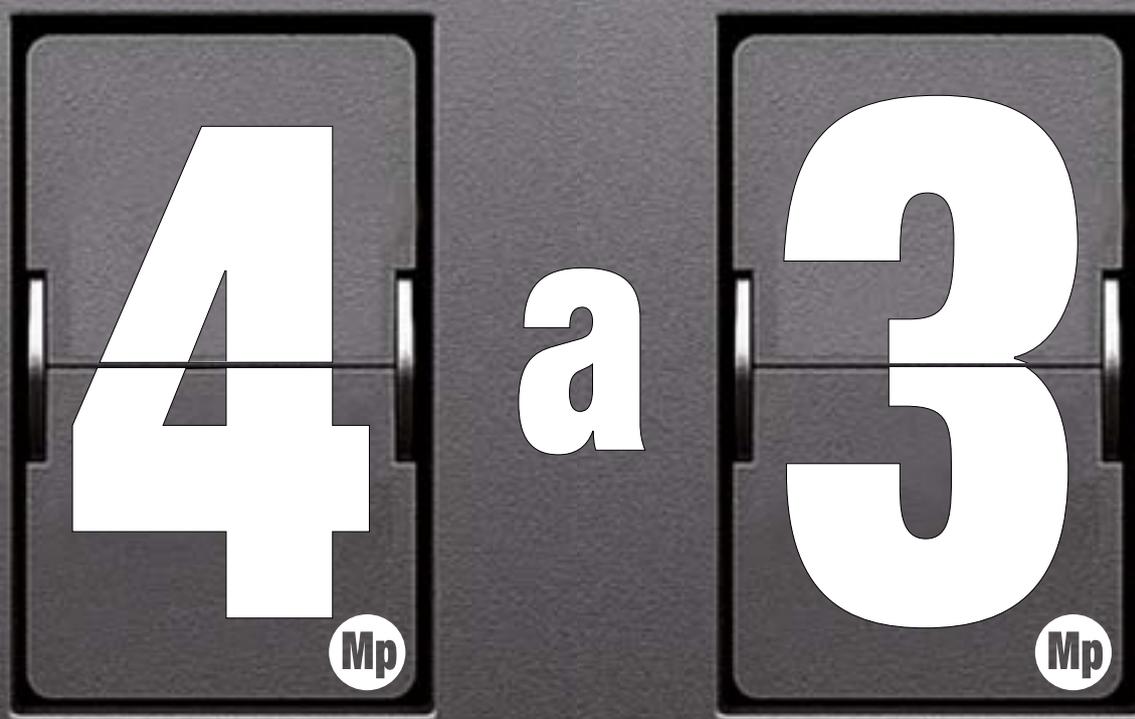
MADE TO PROTECT



AGATE

IL RILEVATORE DA ESTERNO
EVOLUTO

4MP HDCVI **REAL TIME** SU CAVO COASSIALE



**Numeri 1 al mondo nei
sistemi megapixel analogici**

Palla al centro... La sfida continua





ELKRON EGON

IL NUOVO SISTEMA ANTINTRUSIONE WIRELESS CON NOTIFICA VIDEO

Antintrusione, verifica in caso di allarme, controllo con app dedicate. Prestazioni elevate, linee eleganti e grande attenzione ai dettagli.

Il nuovo **sistema di allarme wireless Egon** è progettato per proteggere al meglio abitazioni, uffici, negozi e soddisfare le necessità di professionisti e utenti finali.



APP per l'utente

L'utente può gestire il suo sistema da smartphone o tablet, utilizzando l'app Elkron Egon, che è disponibile senza costi su tutti gli store.

APP per il professionista

Elkron Egon Professional è l'App che permette agli Installatori di svolgere da remoto, tramite smartphone e tablet, tutte le operazioni di diagnosi e di programmazione.



elkron.it

ELKRON

Elkron è un marchio commerciale di Urmet S.p.A.

LE INDAGINI

38 TVCC: tra conferme e sorprese, spunta l'ipotesi di un comparto regolamentato

Ilaria Garaffoni

TECH CORNER

48 ONVIF, Profilo T e H.265: l'evoluzione nella compressione

Fredrik Svensson

CHIEDI AL LEGALE

90 Come e dove installare telecamere nei condomini?

Barbara Pandolfino

VERTICAL MARKET SOLUTIONS GALLERY

- 16** La videosorveglianza IP nella sicurezza e nel controllo accessi
La Redazione
- 18** Infrastrutture critiche: dalla protezione del perimetro all'area
La Redazione
- 20** L'Unione dei Comuni Lombarda "BBO" risparmia con la lettura targhe
La Redazione
- 22** Argentina: un sistema rivoluzionario di controllo semaforico
La Redazione

RIFLESSIONI

- 26** Vecchi cavi addio, arriva il nuovo regime CPR
La Redazione
- 30** Manutentori Fire: certificare la professionalità
La Redazione
- 96** La sicurezza pubblica secondo la standardizzazione
Marc Chevenoy
- 116** Bonus sicurezza: al via il canale telematico per la dichiarazione precompilata
La Redazione
- 136** Smart City e sicurezza: innovazione, condivisione, competenze
La Redazione

LE INDAGINI

- 34** Tecnologia, terrorismo, reati contro la proprietà: i driver del mercato globale della security
La Redazione

TECH CORNER

- 72** Storage, networking, chipset, camere: cosa è bene sapere
La Redazione
- 80** Il computer estrae a sorte i dipendenti da perquisire
La Redazione
- 86** Integrazione di sistemi e tecnologia IP: due driver in costante evoluzione
La Redazione
- 102** La Videoverifica degli eventi, un aiuto concreto
La Redazione
- 106** Il problema delle riprese notturne: soluzioni tecnologiche
La Redazione

MERCATI VERTICALI

- 52** Banche: dove la sicurezza fisica sposa la sicurezza logica
Elvy Pianca
- 56** Sicurezza negli istituti bancari: il parere del progettista
Pierdavide Scambi

PARLIAMO DI BUSINESS

- 60** L'approccio olistico alla security secondo ASIS International
ne parliamo con Thomas J. Langer, CPP - ASIS International President

VOCI DAL MERCATO

- 64** Compressione e cybersecurity: nuove sfide per la videosorveglianza
Antonella Sciortino

CHIEDI ALL'ESPERTO

- 68** Public Safety e ICT Organizzazioni ed Enti, pubblici e privati, tra nuove tecnologie e soluzioni
Filippo Novario
- 76** Controllo perimetrale degli accessi: sicurezza *trasversale*
Giovanni Villarosa
- 94** Controllo a distanza e Videosorveglianza nel lavoro domestico
Marco Soffientini

ACADEMY

- 110** Qual è l'ambito di applicazione del DM 37/2008?
Roberta Rapicavoli

COMPONENT CASE

- 112** La centralità del cavo in un sistema di videosorveglianza

FOCUS PRODUCT

- 120** Nuovo sistema wireless: integrazione bidirezionale supervisionata
- 122** Piccoli e medi impianti: software per controllo accessi



secsolution.com



/ethosmediagroup



/SecSolution



/SecSolution.it



- 124** Centrali per la sicurezza industriale e residenziale
- 126** Più di un sistema d'allarme: sicurezza e comfort
- 128** Tutti i vantaggi della videocitofonia ibrida bifilare
- 130** Personal Tracker/APP per la sicurezza personale
- 132** Centrali di evacuazione vocale compatte e certificate

EVENTI

- 134** Verona goes vertical con IP Security Forum
La Redazione

VISTI PER VOI

- 138** L'Innovazione senza sicurezza è una falsa innovazione
- 138** OMC: sicurezza e innovazione nell'industria Oil&Gas
- 138** Richmond Forum: il successo 2017, le novità 2018

DA NON PERDERE

- 139** Elettromondo 2017: oltre le aspettative
- 139** IFSEC 2017: sicurezza di persone, proprietà e asset
- 139** Euralarm Symposium: security e fire

TOPNEWS

12

PRODOTTI

140

Chi ha i numeri non dà i numeri

L'espressione "dare i numeri" presenta una radice curiosa. Si riferisce infatti ai numeri che gli indovini asseriscono di ricevere dai sogni, rivendendoli come puntate infallibili per il lotto. Una premessa non del tutto fuori luogo in un'Italia dove si tende, dalla politica al giornalismo, a "dare numeri" senza disporre di un ancoraggio statistico affidabile ed indipendente. Purtroppo anche le punte industriali più tecnologiche, come il comparto sicurezza, talvolta operano senza ancoraggi, in parte perché è difficile scovare analisti realmente indipendenti, ma in parte per una tendenza tutta nostrana ad agire fidandosi dell'intuito e delle capacità personali. Eccellenti qualità che ogni imprenditore deve naturalmente possedere, ma che in un mercato globale e ad altissimo tasso di competitività possono mostrare più di una carenza. Per fare fronte a queste esigenze, a&s Italy – assieme all'analista KF Finance - elabora ogni anno un'analisi finanziaria indipendente sul mercato italiano, che fornisce anche importanti suggerimenti sugli indicatori che ogni imprenditore dovrebbe conoscere di se stesso, oltre che dei suoi competitor. a&s Italy elabora inoltre sondaggi e pubblica contributi di analisti (disponibili anche alla vendita su <http://media.secsolution.com/libri-pubblicazioni.asp>) per rendere accessibile i numeri veri del mercato. Un knowhow che può portare interessanti sorprese, come il fatto che la domanda c'è e i capitali pure e che esistono precise tendenze tecnologiche e preferenze dell'utenza, che consentono di guidare l'attività con un vantaggio competitivo, e quindi crescere.

Starlight



Professional-level network camera,
with rich functions and superior image
quality, meets various applications.

Speed Dome 2/3 Megapixel Starlight H.265



Network cameras provide pan, tilt and zoom functions,
enabling wide area coverage and all-round monitoring.



Bullet PTZ 2/4 Megapixel Starlight H.265



Milesight

Official distributor

Professional security system business unit of Melchioni S.p.A.

Scienze & Technology Make Life Better

IPC



12MP
4K
H.265
WDR
Starlight
Smart
Analysis

NVR



H.264/H.265
4K
POE

AHC



AHD - TVI
CVI - CVBS
Switable
UTC control
OSD

ADVR

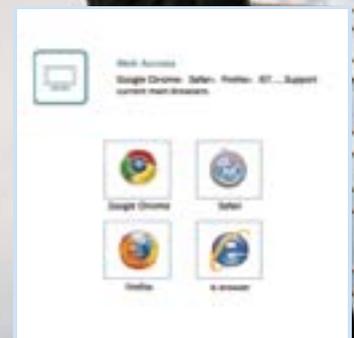
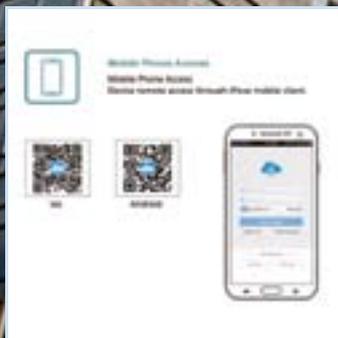


AHD - TVI
CVI - CVBS - IP
self-adaptive
4MP encoding
realtime

ACCESSORIES



Videowall
Monitor
Switch
Balun



JF TECH

Multifocal sensor technology **PANOMERA®**



La soluzione definitiva per la sicurezza negli stadi



Monitoraggio video illimitato - una risoluzione senza precedenti, anche nei minimi dettagli

Dallmeier è azienda leader nella progettazione, sviluppo e produzione di soluzioni e prodotti per la videosorveglianza. Il sistema di sensori multifocali Panomera è stato studiato ed ingegnerizzato per coprire vaste aree, come gli stadi, le piazze, parcheggi o gli aeroporti. Con questa tecnologia completamente nuova e rivoluzionaria, una grande area può essere controllata da un singolo punto di osservazione.

- Zoom fino ai più piccoli dettagli anche da grande distanza
- Registrazione continua di tutta la scena inquadrata
- Real time fino a 30 fps
- Risoluzione fino a 64 MP
- Playback frame by frame
- Riduzione dei costi dell'infrastruttura e di manutenzione





www.kseniasecurity.com

Nuovo design, qualità di sempre.

Look rinnovato
per Simplya,
la prima tastiera
touch screen
italiana.

combivox.it



Simplya

NUOVO DESIGN, QUALITÀ DI SEMPRE.

Simplya si rinnova nel design: grazie alla sua linea semplice e alle dimensioni contenute (**spessore di soli 15 mm**) è in grado di adattarsi a qualsiasi situazione ambientale. **Display touch screen 5"** e interfaccia grafica per icone, completamente rinnovata, per una gestione rapida e intuitiva delle funzioni Antifurto e Domotica. Dotata di microfono e altoparlante per l'assistenza utente tramite menu vocale, integra anche un lettore per chiave di prossimità. Collegamento su BUS RS-485, **compatibile con tutte le centrali Combivox.**

Scopri di più su www.combivox.it



MADE IN ITALY

COMBIVOX
ENJOY LIFE, SAFELY.



DS- 2TD2136
THERMAL BULLET CAMERA

INDUSTRIAL

TELECAMERE TERMICHE SENSIBILITÀ E VIDEOANALISI

Le telecamere termiche restituiscono in un'immagine le differenze di temperatura tra gli oggetti e l'ambiente anche quando condizioni estreme rendono lo scenario invisibile all'occhio umano e alle tradizionali telecamere. Analitica video a bordo con funzioni Smart ed attivazione automatica di allarme contribuiscono, con la visione termica, a rendere questo prodotto particolarmente adatto ad impieghi di alta Sicurezza come monitoraggio di aree estese, perimetri, impianti industriali e siti sensibili.

Hikvision Italy
Via Abruzzo 12, Z.I. S. Giacomo
31029 Vittorio Veneto
T +39 0438 6902
F +39 0438 690299
info.it@hikvision.com

Vittorio Veneto | Roma | Milano | Bologna

www.hikvision.com



IL MERCATO DELLA VIDEO ANALISI: LE PREVISIONI DEGLI ESPERTI



STOCOLMA (S) - Con una crescita sostenuta, sebbene meno rapida del previsto, la video analisi si è affermata come uno dei principali trend della videosorveglianza. Ma nei prossimi mesi assisteremo a un ulteriore step: gli analisti di IHS prevedono infatti che, archiviata la delusione per le aspettative non del tutto soddisfatte, il mercato sia pronto per rinnovare la propria fiducia all'analisi video, grazie alla nuova generazione di sistemi potenziati dalle tecnologie di deep learning e di analisi dei big data e da strutture informatiche ad alta prestazione.

<http://www.secsolution.com/notizia.asp?id=7670>

CONVERTITO IN LEGGE IL DL 14 SICUREZZA URBANA



ROMA - Il Senato ha convertito in legge il DL n. 14 in materia di sicurezza delle città: sono stati introdotti incentivi per installare sistemi di videosorveglianza pubblica (37 milioni di euro in tre anni) ed è previsto che i privati possano attivarsi in modo organizzato per lo stesso fine, con la possibilità di ottenere benefici fiscali. L'amministratore di condominio o uno qualsiasi dei soggetti interessati potrà predisporre un progetto finalizzato alla sicurezza di una zona più o meno ampia, dal singolo condominio all'isolato, al quartiere, per mezzo di sistemi intelligenti collegati alle centrali delle forze dell'ordine.

<http://www.secsolution.com/notizia.asp?id=7672>

TELECAMERE NEI LUOGHI DI LAVORO: AGGIORNATI I MODELLI PER L'AUTORIZZAZIONE



ROMA - A poche settimane dalla prima pubblicazione (10 marzo 2017), l'Ispettorato nazionale del lavoro ha aggiornato i modelli di istanza di autorizzazione all'installazione di sistemi di sicurezza, organizzazione e protezione del patrimonio che consentono anche il controllo a distanza dell'attività degli addetti (comma 1 del nuovo art. 4 dello Statuto dei lavoratori). I modelli rimangono tre, ma sono diversamente denominati. Il primo riguarda gli impianti audiovisivi, il secondo le apparecchiature di localizzazione satellitare, il terzo gli altri strumenti di controllo.

<http://www.secsolution.com/notizia.asp?id=7668>

FONDAZIONE ENZO HRUBY PER LA FONDAZIONE SCIENZA E TECNICA DI FIRENZE



MILANO - La Fondazione Scienza e Tecnica di Firenze, nata nel 1987, si impegna a conservare, valorizzare e incrementare un patrimonio storico, scientifico e librario proveniente da tutta Europa e custodito in oltre un secolo di storia, un patrimonio che la Fondazione Enzo Hruby intende proteggere sostenendo la realizzazione di un progetto di adeguamento dei sistemi di sicurezza tramite l'impiego delle più avanzate tecnologie di sicurezza e di videosorveglianza.

<http://www.secsolution.com/notizia.asp?id=7648>

SIGLATO UN ACCORDO TRA ACCREDIA E CEI



MILANO - Grazie all'accordo sottoscritto lo scorso 30 marzo, Accredia, Ente Italiano di Accreditamento, oltre a partecipare con i propri esperti agli Organi Tecnici CEI, potrà segnalare temi di interesse in relazione a esigenze o problemi di propria competenza per indirizzare eventuali lavori tecnici nell'elaborazione di documenti normativi. CEI si impegna a raccogliere le istanze espresse all'interno degli Organi Tecnici più opportuni, anche in sede europea e internazionale.

<http://www.secsolution.com/notizia.asp?id=7630&c=1>

A BARI LA VIDEOSORVEGLIANZA È SEMPRE PIÙ SMART



BARI - Una sicurezza intelligente quella che il nuovo sistema di videosorveglianza intende garantire alla città di Bari. Il programma integrato denominato "Musica" (Monitoraggio urbano attraverso soluzioni innovative per città agili) prevede infatti l'installazione di 86 telecamere di ultima generazione, dotate di videoanalisi e collegate al cruscotto di controllo urbano e alla centrale operativa della Polizia municipale. Le telecamere, attraverso una trasmissione dati continua, comunicheranno con i corpi di polizia municipale in centrale e con le unità mobili.

<http://www.secsolution.com/notizia.asp?id=7671>



LA PRIVACY INFORMATICA È PIÙ IMPORTANTE DELLA LOTTA AL TERRORISMO?



ROMA - La piattaforma di dibattito Prover-si.it ha di recente pubblicato un testo di approfondimento su un argomento di grande attualità: il rapporto tra lotta al terrorismo e privacy informatica. I fatti riconducibili al fenomeno del terrorismo di matrice jihadista, verificatisi in Europa a partire dal 2014, hanno portato il governo italiano a reagire e a dotarsi di strumenti e di tecniche che dovrebbero aiutare a prevenire qualunque tipo di minaccia sul suo territorio.

<http://www.secsolution.com/notizia.asp?id=7590>

VIDEOSORVEGLIANZA: ENTRO IL 2022 IL FATTURATO RADDOPPIERÀ



HADAPSAR (IND) - Secondo Marketsand-markets il mercato della videosorveglianza nel 2016 valeva \$30.37 miliardi e di qui al 2022 raggiungerà quota \$75.64 miliardi. L'implementazione dell'analitica video, l'aumento dell'installazione di sistemi di videosorveglianza, l'utilizzo di servizi cloud-based per i dati centralizzati e l'uso di telecamere ad alta definizione, oltre alla crescente esigenza di sicurezza, sono i fattori principali che faranno da volano al mercato della videosorveglianza.

<http://www.secsolution.com/notizia.asp?id=7644>

ANIE SICUREZZA: "UN MERCATO DA 2,2 MLD"



MILANO - Rosario Romano, presidente di Anie Sicurezza, ha commentato l'andamento del settore sicurezza, anche alla luce degli ultimi episodi che hanno rinnovato nel nostro paese il senso di timore e impotenza dinanzi a eventi criminosi come furti e rapine. "E' un settore - ha spiegato Romano - che va molto bene: dal 2012 a oggi è l'unico che, nel suo complesso, tra quelli di ambito Anie, è cresciuto in media del 5% all'anno. Ed è un settore che per quanto riguarda le nostre imprese vale un mercato da 2,2 miliardi".

<http://www.secsolution.com/notizia.asp?id=7622>

ANTINTRUSIONE E SMART HOME: COME CRESCE IL RESIDENZIALE SECONDO IHS



LONDRA (UK) - Si preannuncia aspra la competizione nel mercato professionale della smart home, con l'affermazione di nuovi operatori provenienti dal mondo delle telecomunicazioni, secondo l'analisi di IHS Markit, alla luce delle recenti acquisizioni che hanno movimentato il primo trimestre del 2017. Come quella di ObjectVideo da parte di Alarm.com e di Icontrol da parte di Comcast (cresciuto tanto rapidamente da rappresentare già il 2% del mercato USA del monitoraggio a distanza nel residenziale).

<http://www.secsolution.com/notizia.asp?id=7591>

SCUOLE IN VENETO: 1,5 MLN PER LA SICUREZZA



MILANO - Con la delibera pubblicata il 24\03\2017 nel Bollettino ufficiale della Regione Veneto, la Giunta mette a disposizione un milione e mezzo di euro per interventi di adeguamento e manutenzione nelle scuole materne, elementari e medie del territorio veneto (i bandi destinano 1.125.000 agli istituti pubblici e 428.725 alle scuole private). In tema di sicurezza risultano finanziabili, tra i vari interventi, anche gli impianti di videosorveglianza e antintrusione.

<http://www.secsolution.com/notizia.asp?id=7580>

SECURITY ANALYTICS: BIG DATA E MACHINE LEARNING



MILANO - Nell'era dell'informazione, il dato è uno degli asset più importanti per qualsiasi organizzazione, dalla più piccola alla grande realtà Enterprise, perché da esso può essere estratta la "conoscenza". E' sulla base di questo principio che prodotti come i PSIM si stanno facendo strada nel mondo della sicurezza fisica, soprattutto in ambito Enterprise e Corporate. In realtà, anche se in forma diversa, il concetto era già presente nei più tradizionali sistemi di supervisione e building automation: si trattava infatti sempre di raccogliere le informazioni dai sistemi periferici e di riportarli verso il centro.

<http://www.secsolution.com/notizia.asp?id=7483>

Integrazione WIRELESS

**Nuovo sistema wireless:
integrazione bidirezionale supervisionata
a doppia banda di frequenza**



**Semplicità di installazione
ed elevati standard di sicurezza**



**1977 - 2017
40 anni di ricerca e innovazione**

SYNC@BWL



**Doppia banda
bidirezionale
supervisionata**



**16 canali per banda
con sintonia
automatica**



**Sincronismo
modulare
anticollisione**



**Protocollo
con doppia chiave
di crittografia**



**Autoregolazione
dinamica
potenza RF**



**Gestione
intelligente
degli assorbimenti**



I dispositivi possono essere controllati da remoto grazie all'esclusiva tecnologia RSC® (Remote Sensitivity Control) che permette la comunicazione tra l'impianto e il centro di controllo tecnico dell'installatore.

La videosorveglianza IP nella sicurezza e nel controllo accessi



LA PROBLEMATICA

Nel settore dell'impiantistica tecnologica, gli ultimi anni sono stati caratterizzati dall'integrazione dei diversi impianti destinati a sicurezza, controllo accessi e videocontrollo. Le soluzioni sono state spesso soddisfacenti ma altrettanto spesso complesse e costose, e non sempre alla portata dell'utente. E' il caso, per esempio, di un punto vendita di una nota catena italiana di supermercati. Qui le esigenze erano molteplici: partendo dalla videosorveglianza interna ed esterna, per arrivare al controllo porte/uscite di sicurezza, passando dal controllo di corridoi di accesso per depositi o celle frigorifere, fino alla verifica dell'apposito accesso dei dipendenti, oltre ad un conteggio delle presenze, giornaliere, settimanali e mensili nelle diverse fasce orarie. La prima soluzione proposta all'utente prevedeva software di centralizzazione, PC che

ne potessero supportare l'applicazione, istruzione al personale ed impiantistica complessa, con un preventivo di costo estremamente elevato e non giustificato per la dimensione della struttura. Ma l'esigenza dell'utente era, comunque, forte ed evidente. Il system integrator interessato al progetto ha quindi contattato Eurotek prospettando il problema. Dopo un'attenta analisi, Eurotek ha proposto la soluzione partendo dalle tecnologie presenti nelle telecamere IP H.265, con relative Smart Function di UNV, nella versione Mini Bullet, Mini Dome, Bullet, Dome, e Speed Dome da 4 e 8 Megapixel.

LA SOLUZIONE

Si è provveduto dunque allo sviluppo di un progetto che tenesse conto delle esigenze di videosorveglianza nelle aree interne ed esterne della struttura - quindi una copertura totale ed accurata. Laddove era necessario

definire le aree inviolabili al pubblico si sono utilizzate le Smart Function nelle loro diverse tipologie: "Line Cross" per delimitare e segnalare l'eventuale violazione sulle uscite di sicurezza, sui passaggi o tunnel verso le aree di servizio; "riconoscimento facciale" per controllare le aree di pericolo per i minori; funzione "conta persone" per avere un report delle presenze nei diversi giorni della settimana e nelle diverse fasce orarie. Ad ogni funzione corrispondeva una segnalazione analogica od un invio di notifica su mobile o PC, centralizzando il tutto sul software EZStation di UNV totalmente gratuito, pertanto completo, semplice ed intuitivo nel suo utilizzo. Infine nelle aree esterne (destinate sia a parcheggi che ad aree di transito antistanti gli ingressi alla struttura e le uscite di sicurezza) si è potuto facilmente monitorare l'eventuale impropria occupazione o presenza di ostacoli che impedissero il normale deflusso degli utenti, assi-

curando un transito regolare e in sicurezza. Anche questo è stato possibile grazie alle Smart Function presenti sulle telecamere destinate a monitorare l'area, utilizzando la funzione "area protetta" che consente la segnalazione immediata delle violazioni.

I BENEFICI

La centralizzazione attraverso la EZStation ha consentito al centro di sorveglianza di ottenere informazioni costanti e continue, ma soprattutto di avere sotto mano le registrazioni di ogni possibile evento, in totale libertà e movimento, viste le notifiche push in real time su apparati *mobile*. La risposta snella, pratica e accessibile alle esigenze dell'utente ha trovato piena soddisfazione del committente e del system integrator, rispondendo appieno alle esigenze di sicurezza, controllo accessi e video controllo con un'infrastruttura di rete efficace e potente, permettendogli così di lanciare l'utilizzo di molteplici applicazioni spesso realizzabili per costi e complessità. L'H.265, le Smart Function, il 4K e il software di centralizzazione EZStation in UNV riscrivono infatti le soluzioni degli impianti speciali, aprendo a nuove opportunità di mercato per le molteplici e semplici applicazioni, e concretizzando in opportunità di lavoro progetti altrimenti difficili da realizzare. Possiamo, quindi, affermare che l'evoluzione delle tecnologie di videosorveglianza IP, denominate da Eurotek 3.0, aprono il mercato a soluzioni che già oggi rappresentano il futuro. Sarà questo oggetto, oggi definita telecamera IP, l'elemento che incorporerà sempre di più le tecnologie che soddisferanno le esigenze di sicurezza e comfort nel nostro mondo?

EUROTEK www.eurotek-srl.it



■ La funzione di riconoscimento facciale viene utilizzata per controllare le aree a rischio per minori e discriminazione persone o cose.



■ La funzione "Line Cross" delimita e segnala ogni possibile violazione sulle uscite di sicurezza, sui passaggi o tunnel verso le aree di servizio



■ Il software di centralizzazione EZStation e l'app per per smartphone EZView permettono la gestione remota e completa del sistema

Infrastrutture critiche: dalla protezione del perimetro all'area



LA PROBLEMATICAZIONE

La protezione delle infrastrutture critiche occupa un posto di particolare rilievo nello scenario attuale. Tali infrastrutture critiche (Aeroporti, Porti, stazioni elettriche o idriche, dighe, raffinerie ed alcuni siti industriali strategici) hanno caratteristiche comuni: perimetri particolarmente estesi (decine di Km); assenza di energia elettrica e rete dati lungo il perimetro; localizzazione in aree isolate facilmente attaccabili. La protezione di aree così ampie rappresenta una sfida per i Security Manager, che si trovano a fronteggiare intrusioni ripetute nel tempo con tecniche di attacco sempre più evolute. L'approccio normalmente adottato prevede la realizzazione di una linea di protezione lungo il perimetro con tecnologie tradizionali, quali telecamere termiche e visibili con aggiunta di video analisi esterna, sensori sulle recinzioni, cavi interrati, ecc. Tale metodica presenta

tuttavia numerose limitazioni:

- a) elevati costi di manutenzione dovuti all'alto numero di sensori installati in campo;
- b) rapida diminuzione dell'efficacia nel tempo del sistema di sicurezza a causa delle difficoltà di manutenzione;
- c) alto tasso di falsi allarmi (meteo, vegetazione, animali);
- d) possibilità per gli intrusi di simulare falsi allarmi per distrarre il personale di sicurezza;
- e) protezione solo di una piccola area lungo il perimetro;
- f) assenza di informazioni sulla posizione degli intrusi nel sito;
- g) assenza di informazioni sul numero di intrusi presenti al momento dell'attacco;
- h) alto rischio di perdere gli allarmi reali (spesso confusi insieme a numerosi falsi allarmi).

Per realizzare un sistema di sicurezza efficace ed affidabile nel tempo occor-

re quindi cambiare l'approccio: dalla protezione della sola linea di perimetro alla protezione dell'intera area del sito.

LA SOLUZIONE

La soluzione Crisma Security per le infrastrutture critiche prevede l'utilizzo di tecnologie di protezione di area, quali Radar Navtech, Thermal Radar e telecamere termiche intelligenti Sight-Logix, integrate in una console di gestione unica. Caratteristica comune di tali tecnologie è quella di poter rilevare la posizione ed il numero degli intrusi sull'intera superficie del sito. Gli elevati range di copertura consentono una drastica riduzione del numero di sensori da installare in campo, con conseguente riduzione dei costi di installazione e di manutenzione. Radar Navtech rileva una persona fino a 1000m di raggio; Thermal Radar (innovativa telecamera termica che consente una visione a 360°) rileva una persona fino a 200 m di raggio; le Telecamere Termiche Intelligenti SightLogix rilevano una per-

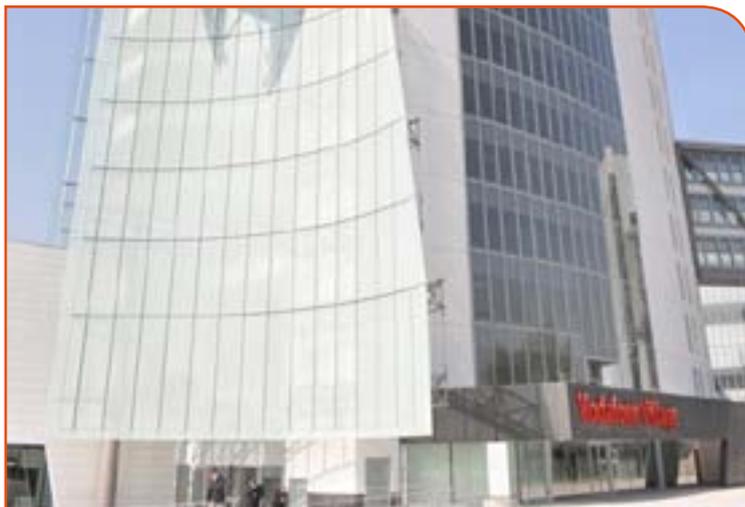
sona fino a 600m di distanza. L'area di detection si può definire liberamente in fase di configurazione, in modo da rilevare i tentativi di intrusione con elevata precisione solo dove effettivamente è necessario. E' possibile definire anche policy di allarme per fasce orarie e giorni della settimana per garantire il presidio automatico quando non vi è la presenza di operatori in loco.

I BENEFICI

Questa soluzione si adatta a varie esigenze, grazie alla modularità dei suoi componenti, che consentono la scelta del range di rilevamento e della capacità di visione delle telecamere. Tra i principali vantaggi si annoverano:

- a) numero ridotto di sensori per proteggere aree molto ampie;
- b) costi di manutenzione contenuti;
- c) elevato livello di efficacia nel tempo;
- d) numero di falsi allarmi estremamente ridotto;
- e) protezione dell'intera area del sito, con aumento significativo del livello di sicurezza;
- f) informazioni precise sul posizionamento ed il numero degli intrusi (coordinate GPS) sia all'interno che all'esterno della recinzione;
- h) utilizzo di sistemi radar in grado di rilevare target in condizioni ambientali avverse senza degrado di performance anche in presenza di nebbia e pioggia;
- g) capacità di valutare in pochi secondi l'entità dell'attacco grazie alle funzionalità di auto-tracking con telecamere PTZ;
- h) visione ottimale sia di giorno che di notte grazie all'utilizzo di sensori termici altamente performanti;
- i) possibilità di ricevere allarmi e visualizzare immagini in tempo reale direttamente da Smartphone e Tablet;
- l) semplicità di utilizzo per gli addetti alla sicurezza.

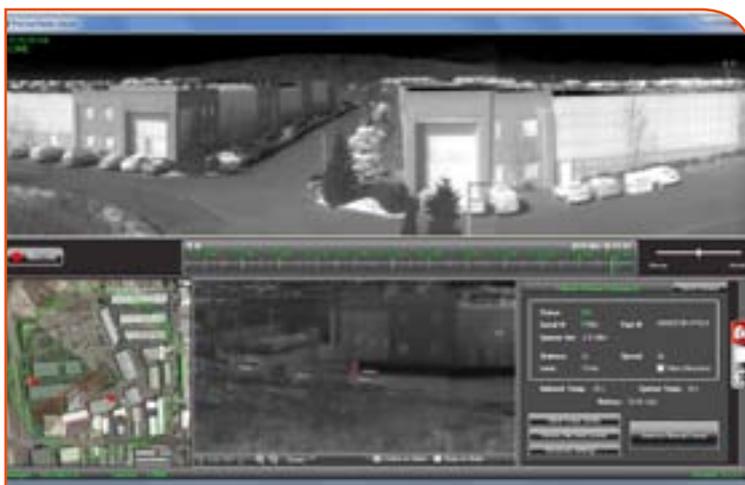
CRISMA SECURITY www.crimasecurity.it



■ Vodafone Italia ha adottato la soluzione Crisma Security per la protezione di aree ampie con Thermal Radar e telecamere Sightlogix



■ Oltre 20 Aeroporti europei utilizzano Radar Navtech e telecamere termiche intelligenti SightLogix integrate in una console di gestione unica



■ Tra i vantaggi: meno sensori per aree molto ampie, meno falsi allarmi, protezione dell'intera area (non solo perimetro), informazioni su posizione e numero intrusi

L'Unione dei Comuni Lombarda "BBO" risparmia con la lettura targhe



LA PROBLEMATICATA

Il territorio dell'Unione dei Comuni Lombarda "Bassa Bresciana Occidentale" coincide con quello dei Comuni di Lograto, Longhena, Maclodio, Orzinuovi, Orzivecchi e Villachiera. L'Unione nasce per migliorare la qualità dei servizi erogati e ottimizzare le risorse economico-finanziarie, umane e strumentali. Gli obiettivi? Semplificazione, efficienza ed economicità dell'azione amministrativa, nonché complementarità, integrazione e valorizzazione delle potenzialità dei singoli Comuni. La sicurezza è sempre stata tra i principali obiettivi dell'Unione, ma la vera intuizione è stata quella di sfruttare le informazioni reperite dalla lettura del dato per ulteriori e più approfondite analisi.

LA SOLUZIONE

La scelta tecnologica è ricaduta su

un centinaio di telecamere di lettura targhe (*Vigilate* A1C, ANPR con OCR e contesto integrato ad 1,3 MPX) per 14 varchi in ingresso/uscita nel territorio, tutte integrate nella piattaforma software Xscanner. Grazie ai dati rilevati, l'Unione ha potuto censire il traffico in ingresso ed in uscita, condividere il dato real time tra le forze dell'ordine presenti, individuare in tempo reale veicoli rubati (la criminalità spesso effettua nuovi crimini con auto rubate), identificare veicoli sprovvisti di assicurazione e/o non in regola, effettuare statistiche per migliorare la viabilità ed altro ancora. La condivisione dell'impianto e dei dati con altre forze dell'ordine, che ha portato anche alla risoluzione di indagini, ha portato la Questura a richiedere l'abilitazione di un accesso dedicato alla piattaforma (dislocata presso la centrale operativa del comune di Orzinuovi, dove risiede anche un VMS per gestire la videosorveglianza urbana). La soluzione può

essere interrogata in qualsiasi punto del territorio previa connessione dati: le forze dell'ordine sono state infatti munite di tablet. La scelta delle telecamere *Vigilate* serie v-PLATE si deve alle funzionalità, che vanno ben oltre la lettura targhe (perfetta sincronizzazione tra immagini di lettura targhe e quella di contesto a colori; lettura targhe e contrassegni che indicano il trasporto di merci pericolose; targhe speciali e straniere; stima sulla velocità di transito; doppia classificazione dei veicoli realizzata con entrambe le ottiche; ricerca per colore; generazione di allarmi in caso di contromano). Tutte queste funzioni sono utilizzate dal software xScanner, grazie al quale è possibile generare allarmi al transito di veicoli non assicurati, non revisionati, rubati o segnalati; monitorare i transiti di merci pericolose e generare allarmi al passaggio di determinate merci; generare una serie di statistiche (conteggio, nazionalità dei veicoli, tipologia, anno di immatri-

colazione, classe EURO, velocità di transito in prossimità dei varchi, tempi di percorrenza tra varco e varco, distribuzione del traffico mediante analisi per origine e destinazione tra varchi). Il collegamento tra i vari apparati è stato effettuato tramite tecnologia wireless con antenne Cambium. La gestione di flussi video tramite ponti radio consente di coprire lunghe distanze (anche di km), difficilmente raggiungibili con la fibra. La tecnologia Cambium garantisce sincronizzazione degli intervalli di trasmissione e ricezione dei moduli radio; efficienza spettrale; Time Division Multiple Access (TDMA) e modulazione adattativa.

I BENEFICI

Surveye – FGS Brescia ha affiancato l'amministrazione consigliandola sulle soluzioni tecniche migliori, e dopo l'aggiudicazione della commessa ha formato gli incaricati sulla parte tecnica e giuridico – amministrativa (in particolar modo privacy). Come dichiarato dal Comandante Vittorio Paloschi, i portali di lettura targhe rappresentano un "muro virtuale" di difesa, dove chi entra e chi esce è rilevato, il tutto nel rispetto della privacy e con obiettivi di condivisione dati atti anche ad evitare sprechi. Ad esempio, se un Comune mette in opera un controllo del varco in ingresso ed uscita al confine con un altro Comune, le due amministrazioni possono scegliere di rendere comune l'accesso dei dati per il varco in questione. In questo modo il Comune confinante non solo risparmierebbe, ma potrebbe anche ottimizzare le risorse, dirottabili magari su altri varchi di accesso al paese, in modo da aumentare sicurezza ed efficacia del sistema.

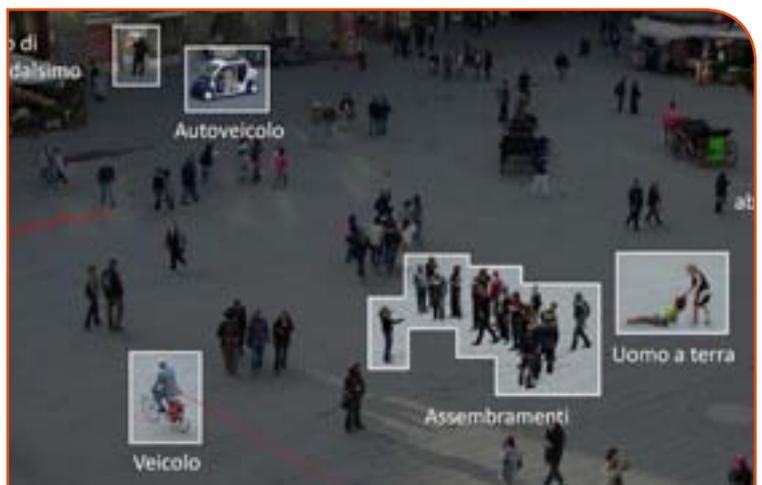
SURVEYE www.surveye.it



■ Centro stella ponte radio Orzinuovi; consente di gestire i punti da monitorare a distanze lunghe, difficilmente raggiungibili con la rete a fibra



■ Telecamere *Vigilate A1C*, telecamera ANPR con OCR e contesto integrato ad 1,3 MPX, il tutto integrato con piattaforma Xscanner



■ La gestione del dato tramite piattaforma Xscanner può fornire una serie di informazioni ad integrazione della sicurezza

Argentina: un sistema rivoluzionario di controllo semaforico



LA PROBLEMATICAZIONE

Prima che fosse sviluppato il nuovo sistema da parte di Vialseg, il controllo ai semafori in Argentina dipendeva da dispositivi basati su circuiti induttivi fisici installati sotto la strada e una connessione fisica al controller del semaforo. Ciò causava costantemente tempi morti, risultanti nell'impossibilità di verificare le infrazioni, ad esempio a causa di manutenzioni stradali o quando mancava la connessione con il semaforo stesso.

LA SOLUZIONE

Vialseg, fornitore leader nei sistemi di controllo della velocità veicolare per i settori pubblici e privati in Argentina, ha avuto l'idea innovativa di combinare due telecamere con una soluzione affidabile di License Plate

Recognition (LPR), unendo le forze con il distributore locale di VIVOTEK, Selnet, e il partner per software LPR, Neural Labs. Vialseg poi ha sviluppato il sistema e il software basato sulla tecnologia fornita da VIVOTEK, leader mondiale nelle soluzioni complete di sorveglianza, e la sua rivoluzionaria telecamera di rete H.265 da 3 megapixel tipo box IP9171-HP.

Lavorando fianco a fianco con gli esperti di License Plate Recognition (LPR), Neural Labs, Vialseg e i suoi partner hanno sviluppato una soluzione in cui il sistema di controllo semaforico di Vialseg utilizza immagini ad alta risoluzione prese dalle telecamere IP9171-HP, e per mezzo del software sviluppato appositamente da Vialseg applica tali immagini al software LPR di Neural Labs per analizzare lo stato del traffico semaforico (rosso/giallo/verde) e la posizione del veicolo all'incrocio, rilevando se uno di essi passa con il rosso.

I BENEFICI

I funzionari competenti riceveranno automaticamente tutte le immagini da utilizzare come prove nel perseguire tali infrazioni. Tale sistema di controllo semaforico è già stato adottato nelle città di Escobar, Moreno, Necochea e Coronel Pringles, tutte nella provincia di Buenos Aires, la più grande in Argentina sia in termini di dimensioni che di popolazione, e il sistema è in continua espansione. Si prevedono ulteriori installazioni nella città di Buenos Aires e in altre metropoli importanti, con un totale stimato di oltre 100 sistemi da allestire nel corso del 2017.

Con i suoi occhi elettronici essenziali per sistema, il modello IP9171-HP di VIVOTEK è una nuovissima telecamera H.265 tipo box da 3 megapixel, che offre fino a 30 fps a 3 megapixel con una straordinaria qualità di immagine e fornisce un'accurata iden-

tificazione delle targhe in qualsiasi condizione. Eccone alcune caratteristiche:

1. *Vista corridoio* - questa funzione esclusiva permette di catturare immagini panoramiche del semaforo e dell'incrocio in modo molto efficiente.
2. *Vero giorno-e-notte* - nel caso della "Zoom Camera", è puntata verso un'area più piccola dell'incrocio per identificare il veicolo utilizzando l'LPR e dispone di illuminazione a infrarossi per migliorare la lettura della targa in condizioni di scarsa luminosità e di notte.
3. *Messa a fuoco da remoto* - aiuta gli installatori a regolare la messa a fuoco con più precisione senza bisogno di scale o altri mezzi di sollevamento.
4. Combinando le tecnologie WDR Pro e Supreme Night Visibility (SNV), la telecamera può registrare e catturare immagini ad alta risoluzione sia nelle condizioni di illuminazione ad alto contrasto tipiche del giorno, sia nelle condizioni di scarsa luminosità esistenti di notte. Insieme, queste caratteristiche permettono all'apparecchio di fornire una qualità video sorprendentemente vicina alle capacità dell'occhio umano e forniscono la tecnologia ottica di base necessaria per garantire un'applicazione rigorosa dei segnali semaforici in tutto il paese. A rendere possibile un tale sistema è stata la capacità della IP9171-HP di integrarsi perfettamente con il software LPR di Neural Labs e di fornire una qualità video eccezionale.



■ **Telecamere + LPR = controllo semaforico senza connessione fisica ai segnali stradali e semaforici. E' realtà in Argentina**



■ **Telecamera di rete H.265 da 3 megapixel tipo box di VIVOTEK. Obiettivo precisione.**



■ **Analizzando stato semaforico (rosso/giallo/verde) e posizione del veicolo all'incrocio, si individua chi passa col rosso**

VIVOTEK www.vivotek.com



IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK

THE ONLY LARGE SCALE SECURITY EVENT IN EUROPE THIS YEAR



Over 10,000 security products to test & trial

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

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

Supported by:



Your badge also gives you entry to:





**SICURTEC
BRESCIA.
SICURI
DI DARE
IL MEGLIO.**



SICURTEC BRESCIA SRL

Sede: Via Bernini, 14 - 25010 San Zeno Naviglio (BS) - Tel. 030 35.32.006
Filiale: Via Venier, 7 (ang. via Pialoi, 20) - 30020 Marcon (VE) - Tel. 041 59.70.344
info@sicurtecbrescia.it - marcon@sicurtecbrescia.it - www.sicurtecbrescia.it



La Redazione

Vecchi cavi addio, arriva il nuovo regime CPR

Dal primo luglio 2017 diventerà definitivamente cogente il Regolamento CPR (Construction Products Regulation o Regolamento prodotti da Costruzione UE 305/2011), che segna l'inizio di una rivoluzione nel settore cavi. Concluso l'anno previsto per l'adeguamento, la nuova norma, entrata in vigore il 1° giugno 2016 in tutta Europa, rimarrà l'unico punto di riferimento per i prodotti, cavi compresi, destinati ad essere installati o utilizzati in modo permanente negli edifici e nelle altre opere d'ingegneria civile. Ma quali sono i nuovi obblighi per i produttori di cavi elettrici, per il trasporto di energia o per la comunicazione? Quale la sorte dei cavi già prodotti? E quella degli impianti progettati prima del prossimo luglio?



Per scoprire le carte di un gioco che si preannuncia più complesso del previsto, ospitiamo due contributi eccellenti che ci aiuteranno a comprendere le conseguenze del nuovo regime CPR sull'attività dei produttori di cavi e su quella di professionisti, imprese elettriche e installatori: le riflessioni di **Marco Moretti**, presidente UNAE, Istituto di qualificazione delle imprese d'installazione elettrica, che rivolge anche una proposta al Ministero dello Sviluppo Economico, ed il commento di **Stefano Bulletti**, presidente di AICE, Associazione che all'interno di ANIE rappresenta una trentina di aziende attive nel comparto dei cavi, con un fatturato di circa 2,4 miliardi di euro nel 2015. Un'ultima nota riguarda i cavi non incorporati in modo permanente nelle opere da costruzione: per questi nulla cambia, perché rimane in vigore la Direttiva 2006/95/CE.

UNA PROPOSTA PER REGOLARE LA TRANSIZIONE

Marco Moretti, Presidente UNAE

Le differenze tra i cavi rispondenti al CPR e quelli rispondenti alla direttiva BT 2006/95 sono poche e non sostanziali, in particolare nei confronti della reazione al fuoco. La novità più importante introdotta dal CPR UE 305/2011 è la sostituzione della "dichiarazione di conformità", prevista dalla Direttiva 95/2006, con la DoP ("Dichiarazione di prestazione"), dove sono elencate in modo puntuale tutte le caratteristiche che devono essere indicate per poter apporre il marchio CE ad un prodotto. Fatte queste considerazioni, dal primo luglio 2017 i cavi marcati CE secondo la Direttiva 95/2006 potranno essere ancora incorporati in modo permanente nelle opere da costruzione, e cioè edifici e opere di ingegneria civile? Non è facile rispondere, perché ci sono altri aspetti da chiarire. Ad esempio: i cavi che le imprese hanno acquistato e hanno in magazzino al 30 giugno 2017 possono essere installati fino al loro esaurimento? È quanto sembra di potersi dedurre dal CPR - Capo I - Disposizioni Generali - "Art. 1- Oggetto: Il

presente regolamento fissa le condizioni per l'immissione o la messa a disposizione sul mercato di prodotti da costruzione, stabilendo disposizioni armonizzate per la descrizione della prestazione di tali prodotti in relazione alle loro caratteristiche essenziali e per l'uso della marcatura CE sui prodotti in questione." Ed ancora: dopo il 1° luglio non sarà possibile realizzare impianti con solo cavi rispondenti al CPR, visto che di tutti quelli che servono – energia, telecomunicazione (telefonia, dati), impianti speciali, come per esempio quelli resistenti al fuoco – solo alcuni saranno in regime di CPR. La conseguenza è che anche negli impianti con inizio lavori successivo al 1° luglio dovranno in ogni caso coesistere cavi rispondenti al CPR e alla direttiva BT 2006/95; per questo motivo, apparirebbe logico che negli impianti in fase di realizzazione si possa continuare ad installare cavi rispondenti alla Direttiva 95/2006.

Le risposte possono comunque venire solo dal MiSE, Ministero dello Sviluppo Economico, che dovrebbe emanare interpretazioni in merito al CPR, sia per gli impianti in corso di realizzazione al 30 giugno 2017 che per quelli che saranno iniziati dopo quella data. Una proposta potrebbe essere la seguente: a) gli edifici e le opere di ingegneria civile, con data di inizio lavori antecedente al primo luglio 2017, possono essere completati con "prodotti da costruzioni aventi caratteristiche rispondenti alla precedente Direttiva bassa tensione 95/2006 e relative leggi e norme"; b) fino a quando non saranno disponibili tutte le tipologie di cavo rispondenti al CPR UE 305/2011 necessarie e sufficienti per realizzare un impianto elettrico, in edifici e in opere di ingegneria civile "i prodotti da costruzione (esempio cavi) possono avere caratteristiche rispondenti sia alla CPR UE 305/2011 che alla Direttiva bassa tensione 95/2006". Si evidenzia che, relativamente al punto "a", il Ministero degli Interni adotta questa soluzione in situazioni simili. La speranza è che il MiSE prenda quanto prima in esame questi temi ed assuma decisioni in merito.

Se ciò non dovesse accadere, le imprese elettriche dopo il primo luglio 2017 non avranno riferimenti certi per redigere le Dichiarazioni di Conformità e i professionisti potrebbero avere difficoltà ad “asseverare” gli impianti per richiedere il CPI (Certificati Prevenzione Incendio).

NUOVI CAVI CPR: A CHE PUNTO SIAMO?

Stefano Bulletti, Presidente AICE

Partiamo da una constatazione: il mercato è partito. Ai produttori di cavi è stato richiesto un grande impegno, ma abbiamo accettato la sfida di questo cambiamento epocale. I produttori di cavi hanno iniziato a produrre le nuove tipologie di cavo rispondenti al Regolamento CPR per poter rispettare l'obbligo di legge che vieta ai costruttori di cavo, dal 1 luglio 2017, l'immissione sul mercato di cavi non rispondenti alle prescrizioni previste dal Regolamento. Il CEI ha predisposto norme di prodotto e tabelle di codifica delle sigle e dei materiali. Le aziende hanno confermato il listino prezzi e le consegne dei nuovi cavi già dal mese di maggio.

La nostra associazione AICE ha dato vita ad una campagna di comunicazione molto strutturata: abbiamo realizzato un documento informativo (I cavi e il Regolamento prodotti da costruzione – CPR UE 305/11), abbiamo dato vita al road show “Revolution Tour: la nuova era dei cavi” che sta toccando diverse città d'Italia, insieme a CEI, TUTTONORMEL, Collegi professionali e diversi altri attori della filiera elettrica. IMQ ha sviluppato un nuovo marchio EURO FIRE PERFORMANCE che, oltre a garantire le caratteristiche obbligatorie di prestazione al fuoco

con la marcatura CE – come stabilito dal Regolamento CPR – garantisce anche tutte le altre caratteristiche del cavo meccaniche, chimiche ed elettriche. Anche altri attori della filiera, a partire dalla Federazione dei grossisti, sono impegnati nel percorso di informazione diretta, a livello nazionale, a tutti i distributori di materiale elettrico e ai loro clienti diretti, ovvero gli installatori. Il percorso impostato dal punto normativo prevede ora che, assieme all'entrata in vigore del Regolamento CPR, sia pubblicata anche la Norma di buona tecnica emessa dal CEI a supporto dell'utilizzo dei cavi. Dal punto di vista normativo, a livello di prodotto, sono state recentemente pubblicate le norme CEI, mentre a livello installativo è ancora in attesa di pubblicazione la variante alla Norma CEI 64-8, che indica destinazione d'uso e tipologia di cavi CPR da utilizzare. Il mercato sta attendendo l'uscita di questa norma, prevista entro maggio, per capire fino in fondo i cambiamenti imposti dal Regolamento CPR. Eventuali e non accettabili ritardi sarebbero a discapito della transizione tra vecchia e nuova tipologia di cavi, con conseguenti disagi per gli operatori. Tale tema sta sicuramente a cuore agli installatori, progettisti e ordini professionali i quali comunque stanno reagendo, per esempio modificando già nelle specifiche dei progetti le tipologie di cavo per consegne oltre il primo di luglio. Sempre sul tema vorrei far notare che l'aumento di prezzo dei cavi a norma CPR è assolutamente marginale rispetto alla variabilità del prezzo del rame, considerando che il prezzo del metallo ha una incidenza in molti casi ben superiore all'80% sul valore complessivo del cavo. Perciò oggi possiamo affermare che oramai il processo di sostituzione della tipologia di cavi sul mercato è in corso e non vediamo motivi di rallentamento o di slittamento: dal 1 luglio commercializzeremo solo cavo CPR.

La gamma EEA si arricchisce con i nuovi

Syrio PET FRIENDLY



**PET
FRIENDLY**



La Redazione

Manutentori Fire: certificare la professionalità



Cosa significa oggi, per aziende e tecnici manutentori di impianti antincendio ed evacuazione, certificare la propria professionalità? Significa prima di tutto assicurare che le persone addette a determinati processi possiedano, mantengano e migliorino nel tempo la necessaria competenza, intesa come l'insieme delle conoscenze, esperienze, abilità e doti richieste per espletare le proprie mansioni. Ma significa anche disporre di un'arma in più – e ben affilata – per distinguersi in un settore dove pesa l'assenza di una norma e di un albo professionale specifico. Da queste premesse è nata l'iniziativa che abbina formazione e certificazione, coniugando l'esperienza di Anie Sicurezza con quella di IMQ.

Il corso per tecnici manutentori di componenti di impianti di rivelazione automatica e manuale antincendio (Fire) e di evacuazione audio (Evac) – propeudeutico alla certificazione IMQ della figura professionale del Tecnico Manutentore – nasce dalla seguente constatazione: per le aziende e i professionisti che si occupano di manutenzione è di primaria importanza, ma spesso difficile, dimostrare la propria competenza e professionalità. Ecco allora intervenire, a conclusione di un percorso di formazione specializzata, la Certificazione delle figure professionali, quale valido strumento – indipendente, imparziale e trasparente – per attestare il possesso dei requisiti necessari per operare in un determinato settore di attività. “In assenza di una norma o di un albo professionale specifico – spiega l’ing. **Dario Noll**, coordinatore Commissione Didattica ANIE SICUREZZA – lo schema di certificazione IMQ-ANIE T.I.R.A.E., rivolto ai Tecnici Manutentori Fire ed Evac, si pone quale percorso qualitativo in grado di attestare tali competenze e fornire un’oggettiva garanzia all’utente finale.” “Si tratta del primo e unico schema certificativo in tale ambito – precisa **Paolo Giussani**, responsabile certificazione figure professionali di IMQ – ANIE e IMQ hanno congiunto le loro esperienze per redigere un capitolato di qualificazione in grado di tutelare il settore e preservarlo dai rischi derivanti da competenze insufficienti o improvvisate”. Una garanzia per l’intero comparto: produttori, distributori e committenti. Altro aspetto innovativo per il settore, la formazione costante. Lo schema di certificazione è infatti fondato sull’idea dell’aggiornamento continuo del Tecnico manutentore, in relazione all’evoluzione normativa e tecnologica degli impianti di rivelazione antincendio e di evacuazione audio. La certificazione ha una durata di tre anni; il suo rinnovo prevede la verifica della continuità operativa nel settore e il superamento di un nuovo esame, nel caso in cui siano stati pubblicati aggiornamenti nell’ambito della normativa di riferimento.

IL CORSO

Il progetto formativo, che ha preso il via alla fine di marzo con il debutto del primo corso per Tecnico Manutentore Fire ed Evac, intende offrire a tutti gli operatori del settore una preparazione puntuale attraverso un programma didattico sia tecnico sia pratico. Durante le

quattro giornate di aula, i docenti si sono concentrati da un lato sulle competenze necessarie per l’attività di manutenzione dei presidi e degli impianti antincendio, dall’altro sulla corretta informazione, per tutte le figure che operano nel settore, relativa alle norme e alla legislazione vigente.

Nell’attuale contesto, la formazione specializzata abbinata alla certificazione da parte di un ente terzo rappresenta “un chiaro elemento distintivo e di valore per le aziende, in un mercato che sempre più richiede soluzioni rapide, performanti e di qualità – osserva Noll – In questa iniziativa, ANIE Sicurezza ha messo a fattor comune con IMQ le proprie conoscenze, per preparare un percorso certificativo rivolto innanzitutto ai tecnici professionali che abbiano già maturato esperienza sul campo.” Al primo corso di formazione, che ha registrato un buon riscontro di presenze e di partecipazione, seguiranno le sessioni di esame per accedere alla certificazione. Proprio in considerazione dell’interesse suscitato, ANIE Sicurezza ha già messo in calendario una nuova edizione del corso, che si svolgerà sempre a Milano, presso la sede di ANIE, dal 2 al 5 ottobre prossimi.



La sicurezza **absoluta** di una
centrale ancora più **Smart!**

ABSOLUT smart

Absoluta Smart è la nuova centrale di Bentel Security pensata per garantire una programmazione ancora **più veloce, semplice e intuitiva**, ma con la stessa sicurezza e affidabilità che da anni contraddistingue il marchio Absoluta.

Grazie, infatti, alla nuovissima **App Smart**, è possibile configurare il sistema direttamente dallo smartphone e tablet, senza la necessità del PC!

Absoluta Smart è disponibile in due Kit, versione filare e wireless, per venire incontro a tutte le esigenze e richieste di un mercato sempre più innovativo.

Sii **Smart**, Scegli **Absoluta!**



VIDEO SORVEGLIANZA FLESSIBILE

concerto

partita
di calcio

manifestazione
politica

mostra
d'arte

fiera
cittadina

QUANDO SERVE DOVE SERVE IN UN ATTIMO

INTELLIGENTE

Un sistema di videosorveglianza ha bisogno di sempre maggiore flessibilità.

UNICA, il nuovo dispositivo di Spark, riesce a soddisfare le vostre esigenze di sicurezza in modo semplice e veloce.

Potete migliorare la videosorveglianza delle diverse aree durante ogni evento, con un livello di attenzione dedicato. In un attimo potete spostare le telecamere dove necessario, grazie ad un sistema di configurazione innovativo e intelligente.

UNICA è il prodotto perfetto per ottimizzare i costi e migliorare l'efficienza e la sicurezza del vostro impianto.

VERSATILE

SEMPLICE



scopri di più su spark-security.com/unica

spark

La Redazione

Tecnologia, terrorismo, reati contro la proprietà: i driver del mercato globale della security

Una crescita media del 10,9% dal 2015 fino al 2020, quando il mercato dovrebbe raggiungere un valore di 109,3 miliardi di dollari. Questo il trend del mercato globale della sicurezza fisica secondo Frost & Sullivan, interpellato dalla fiera Intersec. Per definire il perimetro di indagine ed addentrarsi poi nei numeri e nelle considerazioni di andamento, è meglio partire dalle definizioni.

Per Frost & Sullivan il mercato della sicurezza fisica assomma tutto l'hardware relativo ai diversi segmenti della security (controllo degli accessi, videosorveglianza, antintrusione, protezione perimetrale, allarmistica), come pure i software di gestione ed integrazione - inclusi consulenza e progettazione degli stessi. Stante questa definizione, se nel 2014 il valore stimato dell'intero mercato raggiungeva i 58,6 miliardi di dollari, le previsioni di Frost & Sullivan parlano di una crescita media del 10,9% dal 2015 fino al 2020, quando il mercato dovrebbe giungere a quota 109,3 miliardi di dollari.

VALORE DEL MERCATO

Il valore globale della produzione, basandosi sul prezzo di fabbrica, si attestava nel 2013 su 23,4 miliardi di dollari per il segmento video, su 5,11 per il controllo accessi e su 6 miliardi di dollari per i sistemi d'allarme antintrusione. Se attualmente l'hardware conta per oltre il 70% del reddito complessivo del mercato (con software e servizi che si contendono il valore residuo), nel futuro sarà invece la parte software a farla da padrona, grazie al crescente bisogno di intelligenza tecnologica ed integrazione che arriva dalla stessa domanda. La TVCC passerà quindi da una monetizzazione concentrata sulla vendita di hardware alla generazione di nuovi profitti, e di più lunga durata, dovuti alla somministrazione di servizi (VSaaS). Perché il futuro, secondo l'indagine di Frost & Sullivan, sta proprio nei servizi: il mercato della VSaaS (Videosorveglianza come servizio) dovrebbe infatti chiudere il 2017 con quasi 2,4 milioni di euro e un tasso di crescita medio del 31,5% sul piano globale.

GEOGRAFIA

Secondo questa ricerca di Frost & Sullivan, se gli USA dominano ancora l'industria globale della security con un 35% di market share, saranno però Asia, Europa dell'Est, Africa e Medio Oriente a guidare la domanda nei prossimi anni. In particolare Cina e India - cresciute a ritmi superiori al 10% negli ultimi tempi - sembrano essere i paesi più promettenti in termini di generazione della domanda. La sola Cina (il cui mercato video occupa il 17% del totale) avrebbe chiuso il 2015 con un mercato del valore complessivo di 8,5 miliardi di dollari.

I DRIVER DELLA CRESCITA

Terrorismo, microcriminalità, tecnologie sempre più evolute ed aderenti alle richieste del mercato. Questi tre fattori, uniti ad una nuova ondata di urbanizzazione, quindi ad una rinascita del settore delle costruzioni e delle infrastrutture soprattutto in area asiatica, e ad un rafforzamento delle classi sociali medio-basse, stanno generando nuovi bacini di utenza per il mercato della sicurezza. E il mercato sembra destinato a crescere ancora.

PREVISIONI

A far crescere il mercato non saranno solo il costante incremento della minaccia terroristica e la moltiplicazione e recrudescenza degli atti criminosi verso il privato e le proprietà, ma anche - soprattutto in termini di redditività - l'evoluzione tecnologica del comparto. Oltre al trend ormai consolidato che sposta il focus da analogico a IP in area video e alla ricerca di una qualità ottimale dell'immagine in qualunque condizione ambientale, oggi si punta sempre più su tecnologie evolute come Object Recognition, Videoanalisi, intelligenza, cloud. L'insieme di queste soluzioni dovrebbe crescere ad un CAGR del 13,6% tra il 2015 e il 2020, grazie ad una domanda anch'essa più evoluta e soggetta a minacce sempre più complesse. La convergenza tra tecnologie IT, Telecom e Video aggiungerà sempre maggiore intelligenza ai dispositivi e minori costi di archiviazione per i sistemi.

LA SCACCHIERA COMPETITIVA

Nonostante il mercato sia ad oggi ancora frammentato (generando quindi notevole competitività), e benché si cominci solo adesso ad assistere ad una polarizzazione quanto meno del fatturato su certe aree del mondo, la sicurezza è e resta un comparto sul quale vale la pena di investire perché offre grandi opportunità, sia del breve sia del lungo periodo.



LA SECURITY NEI PROSSIMI 3 ANNI SECONDO FROST & SULLIVAN

ne parliamo con **Robert Haddon**, Security Industry Analyst Aerospace, Defence & Security di Frost & Sullivan

Il mercato della security nei prossimi tre anni: cosa prevede Frost&Sullivan?

La tecnologia più promettente a nostro avviso sarà la biometria, che continuerà a vedere sviluppi interessanti rispetto ai nuovi parametri umani che potranno essere utilizzati, o tra loro abbinati, a scopo di autenticazione. L'impronta digitale quale strumento di autenticazione per gli smartphone sta facendo conoscere al grande pubblico – e accettare maggiormente – la tecnologia biometrica: ulteriori sviluppi riguarderanno i sistemi biometrici multifattore, che possono ottenere diverse modalità di autenticazione senza utilizzare sistemi diversi (es. un sistema video che può abbinare ed analizzare molteplici dati relativi a volto, movimenti e impronte digitali da un'unica immagine). Sul fronte cyber, riteniamo che la block chain (sistema sicuro per registrare ed archiviare le transazioni all'interno della rete, senza garante di terza parte) abbia un futuro molto promettente, specialmente a causa delle continue data breach dovute alla crescente centralizzazione delle informazioni. L'industria sta mostrando molto interesse e investimenti per rendere tecnologie come questi affidabili e diffuse. Menzionerei infine l'Artificial Intelligence (AI), un'interessante area di applicazione futura per la sicurezza. Senza dubbio gli attuali livelli di affidabilità di questi sistemi non bastano a gestire un sistema di sicurezza in assenza dell'elemento umano, tuttavia l'automazione renderà più efficiente e sicuro il lavoro del personale addetto alla security.

Sistemi 5G wireless e sicurezza: quale futuro e quali prospettive ravvisate?

Il 5G diventerà sempre più importante man mano che i dispositivi saranno connessi wireless: lì si condideranno grandi quantità di dati attraverso una rete utente distribuita ed il principale beneficio del 5G sarà quello di permettere livelli di consumo dati più elevati all'interno di una rete wireless. La chiave è gestire la sicurezza dei dati in transito e il loro storage. Creare un'architettura 5G più aperta e connettere un maggior numero di dispositivi assieme potenzialmente apre la rete ad attacchi cyber e al furto di dati. Oltre alla sicurezza dello storage, sarà importante porre in essere sistemi scalabili, cosicché le organizzazioni possano gestire meglio il volume dei dati che useranno, specialmente con normative sempre più stringenti sulle tempistiche di conservazione dei dati (pensiamo in particolar modo alla videosorveglianza). Tuttavia i potenziali problemi del 5G si riflettono principalmente nei sistemi di rete attuali.

Abbiamo in qualche modo introdotto il tema dell'IoT. A suo avviso ha ancora senso parlare di IP o è giusto ormai parlare di IoT?

L'IP è ancora importante, anche con l'avvento dell'IoT. Il concetto di IP semplicemente fa riferimento alla tecnologia che condivide informazioni su una connessione internet invece che su una rete dedicata. L'IoT si basa proprio su questo concetto di IP, permettendo ai dispositivi connessi ad Internet di condividere informazioni tra di loro e con gli utenti, e permettendo al contempo la potenziale automazione di certi processi. Diffondere le tecnologie IP-enabled è dunque la chiave per il successo delle piattaforme IoT ma la vera sfida è come i nodi IoT interagiranno fra di loro e come garantiremo la sicurezza dell'hardware e degli elementi nella rete.

In tema di evoluzione tecnologica, possiamo definire Industria 4.0 il comparto della sicurezza?

Direi che si tratta di un'Industria 4.0 dal momento che ci sono tante innovazioni a livello PMI, oltre a miglioramenti in aree come il controllo accessi e la videosorveglianza (sia hardware che software). Forse si ravvisa un certo stallo in certe aree dell'industria mosse dal bisogno di bilanciare innovazione, costo per l'utente finale e rispetto delle normative.

Passiamo alla scacchiera competitiva. Quali novità ipotizzate 2017 in merito a fusioni e acquisizioni?

La gran quantità di M&A negli anni dal 2014 al 2016 è la dimostrazione di un'industria security in rapido e forte movimento e del bisogno di fornitori/integratori più dimensionati di riallinearsi con le tendenze evolutive del mercato. Se guardiamo in avanti, le acquisizioni di cybersecurity rimarranno aree importanti di M&A man mano che le aziende cercheranno non solo di proteggere meglio i loro clienti ma anche di rafforzare la sicurezza logica delle proprie linee di prodotto: una necessità per le installazioni di sicurezza sempre più connesse e integrate.

Utilizza i tuoi dati in modo intelligente

Sicurezza, cost saving e qualità dei servizi.
Con applicativi evoluti di analisi
ti aiutiamo ad usare le tue informazioni per crescere.



via Leonardo da Vinci , 8
San Zeno Naviglio (BS)

T +39 030 349117
info@surveye.it

surveye.it

Ilaria Garaffoni

TVCC: tra conferme e sorprese, spunta l'ipotesi di un comparto regolamentato

An illustration of a man in a dark blue suit and white shirt running to the right. The background is a dark blue grid with a lighter blue line graph element that starts from the left and trends downwards. The man is positioned as if running along the line graph.

In questo numero di Aprile, *a&s Italy* continua la tradizione di tracciare un confine, cercare di interpretare ed ipotizzare una linea di commento sui trend di mercato interrogando direttamente i protagonisti che ogni giorno vivono – e soffrono – l'attività d'impresa. Gli intervistati sono stati 1047 su un campione comprensivo di produttori, distributori ed installatori/integratori di sistemi. Sul fronte geografico, il campione risulta distribuito sull'intero territorio nazionale con questa ripartizione: Nord 54%; Centro 34%; Sud e Isole 12%. La raccolta dati, realizzata online sul portale www.secsolution.com, è avvenuta nel primo trimestre 2017 ed è databile al mese di Marzo.

Interessante la doppia velocità alla quale si muove il mondo della produzione rispetto al mondo dell'installazione (**grafici 1 e 2**). Sebbene l'anticipazione tecnologica sia naturalmente fisiologica nell'industria produttiva, che deve prevedere ed influenzare le nuove tendenze del settore, il ritardo nella metabolizzazione di alcuni trend da parte del canale fa tuttavia insorgere due ipotesi: o l'obsolescenza tecnologica è troppo rapida rispetto ai tempi di assimilazione dell'utenza finale, oppure il canale non è sempre adeguatamente aggiornato sulle novità, quindi non le promuove con la necessaria convinzione. Un primo dato emerge dalla stessa tipologia di campione, che giustifica due velocità: i produttori si dichiarano in maggioranza dedicati ad una tipologia di produzione per fascia alta (trasporti, GDO, grande industria, PA, banche, monitoraggio urbano etc), mentre la maggioranza (48%) del canale che ha risposto al sondaggio dichiara di occuparsi di mid-end, ossia di esercizi commerciali medio/piccoli, gioiellerie, tabaccherie, farmacie etc. Un dato che non sorprende, in quanto la maggioranza dei produttori è costituita in forma di multinazionale o presenta ragione sociale estera, quindi segue logiche geograficamente "macro", mentre il canale dell'installazione è per sua natura fortemente localizzato su un territorio contraddistinto da un tessuto imprenditoriale medio o piccolo. Peraltro la grande utenza finale è spesso seguita direttamente dalla casa produttrice o comunque da grossi system integrator/centri di acquisto, quindi è naturale che la fascia media e bassa sia gestita dal canale. Più interessante è in tal senso quel 26% di installatori che dichiara di lavorare sul residenziale (segmento che fino a dieci anni fa poteva dirsi di esclusivo appannaggio della sistemistica d'allarme), a testimoniare la diffusa presenza sul mercato di un TVCC ormai entry-level e alla portata di tutte le tasche.

COM'È ANDATO IL 2016

La differenza tra gli alti margini dell'high end e quelli più accessibili – ma forse meno accattivanti - del mid e low end si ravvisa anche nel sentiment di andamento sul 2016 (**grafici 3 e 4**): associando quanti hanno risposto *molto bene* e quanti *abbastanza bene*, si raggiunge infatti ben il 90% dei produttori. Il restante 10% ha dichiarato comunque di aver tenuto nel 2016, quindi il mercato c'è (come peraltro risulta anche all'ultima indagine finanziaria Ethos Media Group - Gruppo K Finance, che

Su quale fascia si posizionano i vostri prodotti per tipologia di clientela?

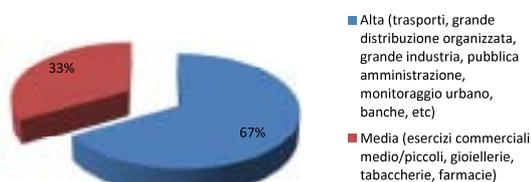


Grafico 1 - Risposta dai PRODUTTORI

Su quale fascia si posizionano i vostri prodotti per tipologia di clientela?

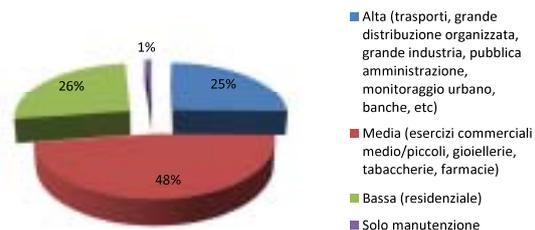


Grafico 2 - Risposta dagli INSTALLATORI

Come è andato il 2016?

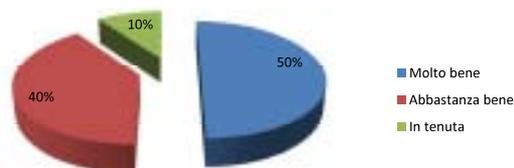


Grafico 3 - Risposta dai PRODUTTORI

Come è andato il 2016?

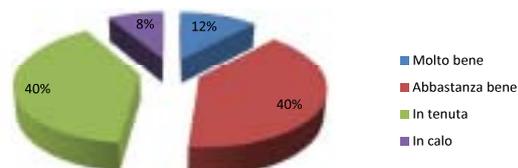


Grafico 4 - Risposta dagli INSTALLATORI

Quale tecnologia va per la maggiore nel segmento della videosorveglianza?

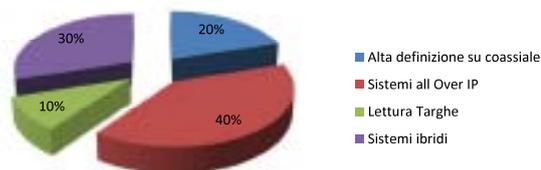


Grafico 5 - Risposta dai PRODUTTORI

Quale tecnologia va per la maggiore nel segmento della videosorveglianza?

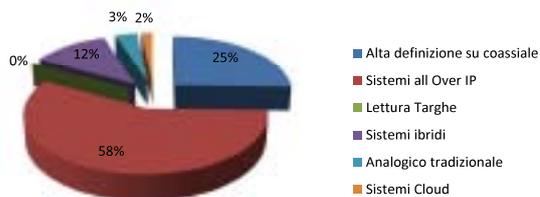


Grafico 6 - Risposta dagli INSTALLATORI

mostrava fatturato e redditività in crescita). E non molto diversamente, nella sostanza, risulta essere il dato rilevabile sul canale: il complessivo 80% di risponditori del campione installatori ha infatti registrato un 2016 *abbastanza buono o in tenuta*; sono però decisamente meno gli operatori che si dichiarano *molto soddisfatti* (12%) e un 8% dichiara anche un calo di fatturato, seppur non

deciso. E questo nonostante, sul fronte tecnologico, la convergenza – con il suo carico di redditività - sembri essere ormai un fatto assodato.

COSA SI VENDE

Il dato rilevabile dalle risposte del canale sul venduto di soluzioni integralmente digitali (all over IP - **grafico 6**) assomma infatti il 58% del paniere: una vera cartina di tornasole sulla migrazione digitale, al suo evidente culmine, visto anche il misero 3% di analogico tradizionale rilevato. Interessante indicatore è anche l'importante venduto di alta definizione su coassiale, che essenzialmente rispecchia lo stesso dato riferito alla produzione (**grafico 5**) e che legittima ad ipotizzare una obsolescenza forse meno rapida del previsto per una tecnologia sicuramente di transizione, ma al contempo altrettanto utile al mercato - e soprattutto ad un utente finale ormai abituato da TV e smartphone a vedere in alta definizione. La quasi assenza di lettura targhe o cloud nel grafico degli installatori, tecnologie invece ben rappresentate nel paniere dei produttori, può essere giustificata dalla tipologia di clientela prevalente riferita dal canale, ossia un mid-low end che in genere non si avvale di tecnologie tanto sofisticate, essenzialmente perché sproporzionate rispetto alle esigenze, oltre che eccessivamente costose.

COSA SI COMPRA

Si compra un prezzo o si compra un prodotto? La domanda è lecita in quasi tutti i comparti, ma – a quanto risulta - non in questo. E' infatti il rapporto qualità/prezzo (e non il prezzo più basso *tout court*) l'elemento numero

Quale caratteristica va per la maggiore nell'acquisto dei sistemi?

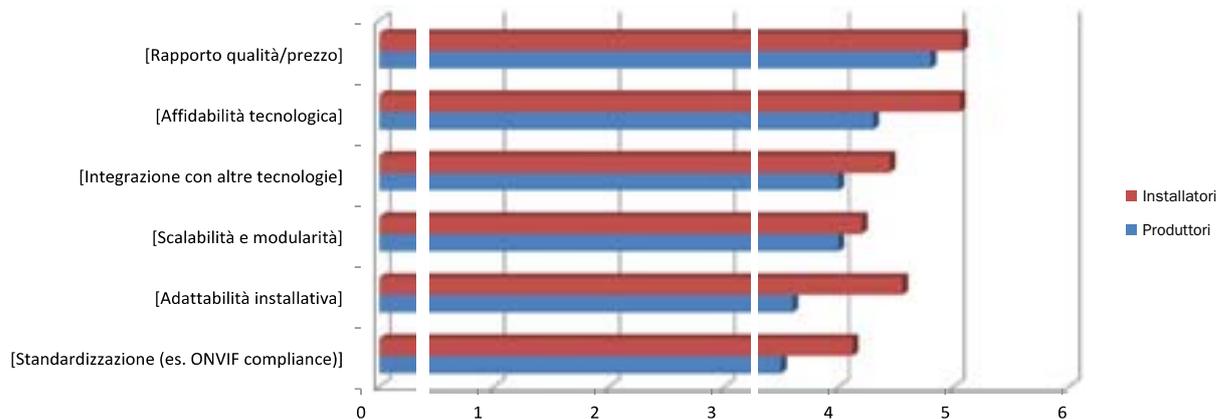


Grafico 7 - Comparazione risposte tra PRODUTTORI e INSTALLATORI

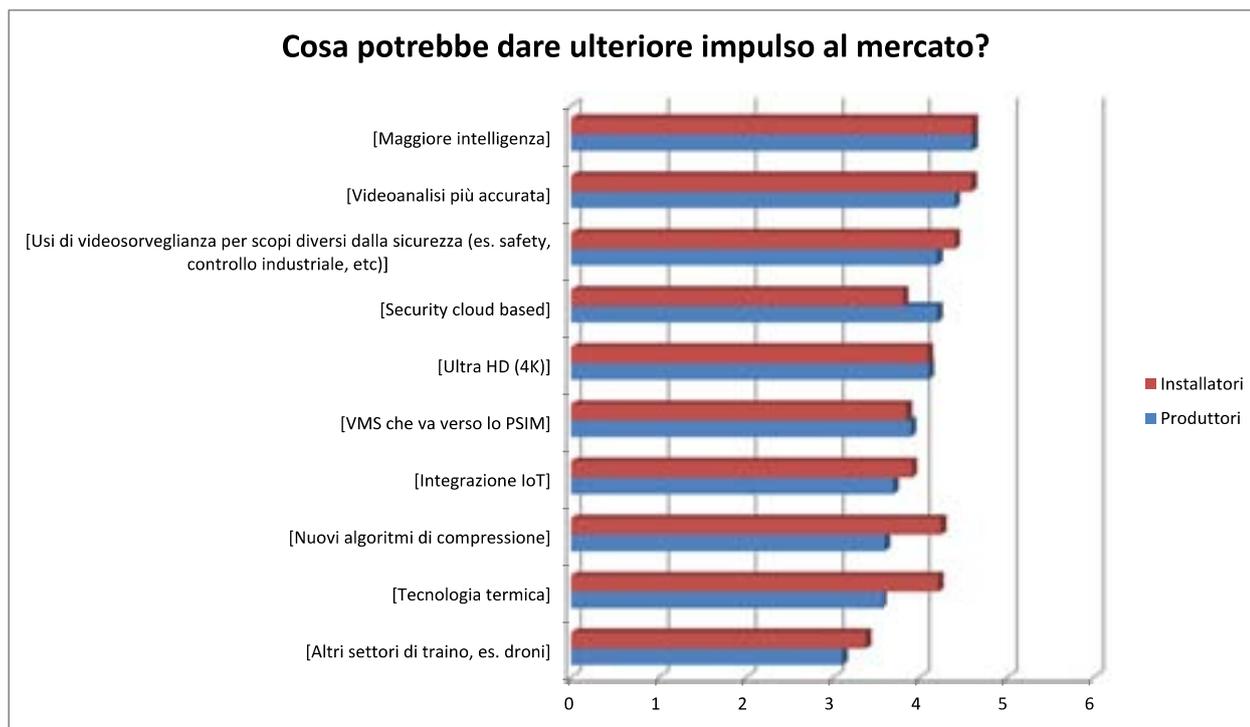


Grafico 8 - Comparazione risposte tra PRODUTTORI e INSTALLATORI

uno a determinare la scelta di una soluzione piuttosto che un'altra (**grafico 7**), e su questo punto canale e produttori sono sulla stessa lunghezza d'onda. Il secondo elemento di determinazione all'acquisto, anche qui coerente nei due livelli distributivi, è l'affidabilità tecnologica. Seguono adattabilità installativa (tema ovviamente più sentito nel grafico relativo al canale, per il quale flessibilità significa anche compressione del tempo-lavoro), integrazione tecnologica, scalabilità e modularità e standardizzazione, intesa come compliance a standard industriali, in particolare ONVIF.

COSA MANCA

E se il mercato cresce o quanto meno tiene, la domanda successiva è cosa potrebbe dargli ulteriore impulso (**grafico 8**). La risposta, dal produttore all'installatore, punta sulla sofisticazione tecnologica: più intelligenza,

più accuratezza in tecnologie d'avanguardia come videoanalisi, cloud, IoT e Ultra HD. Ma ovviamente per supportare queste sofisticazioni occorrono anche strumenti di compressione più performanti (e l'H265 si sta già standardizzando), ma soprattutto si ipotizzano applicazioni più creative della videosorveglianza atte anche ad aprire nuovi mercati: dalla safety al controllo industriale, dalla lotta all'incendio alla sicurezza perimetrale con la tecnologia termica.

Insomma, la scelta vincente pare essere un portafoglio integrato di offerta, soprattutto se tra i mercati verti-



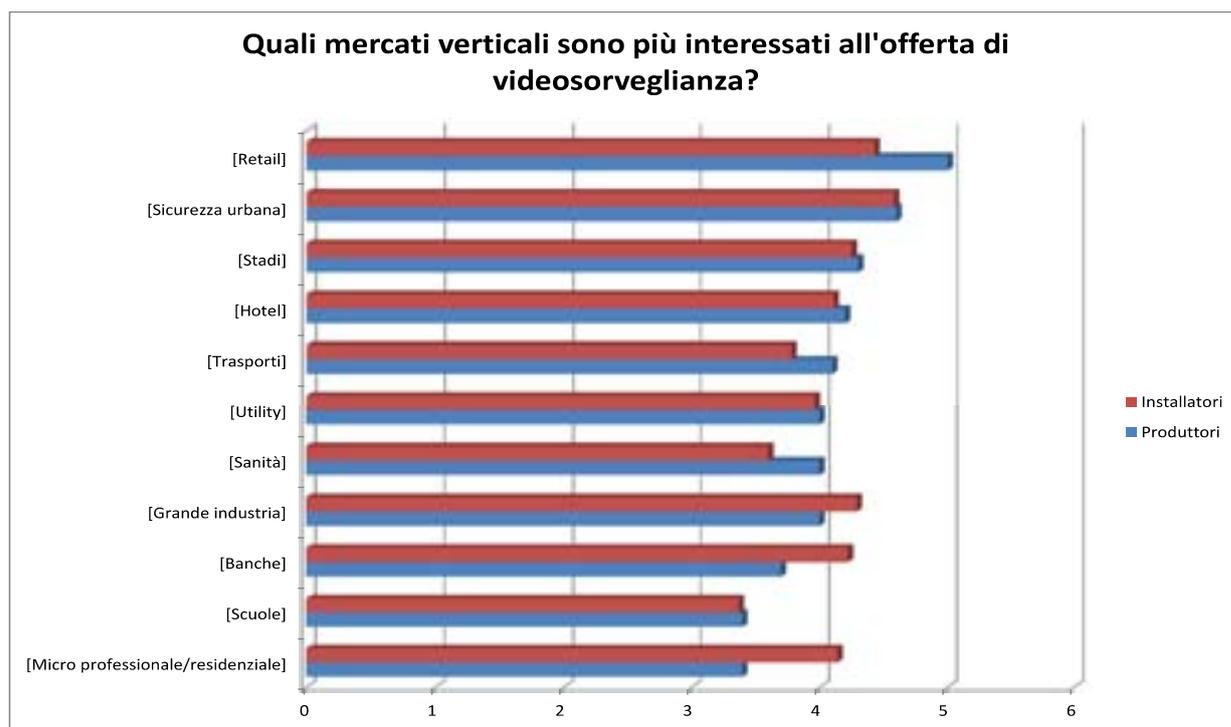


Grafico 9 - Comparazione risposte tra PRODUTTORI e INSTALLATORI

cali più interessati all'offerta di security (**grafico 9**) si annoverano grandi utenti caratterizzati da complessità strutturali e funzionali e che quindi presentano richieste articolate (retail, pubbliche amministrazioni, banche, industria, hotel, stadi, trasporti, aziende sanitarie o utility di diverse tipologie). Le scuole ancora paiono di interesse minore, ma si ipotizza nei prossimi anni un forte (ri) lancio del relativo mercato, se – come dovrebbe acca-

dere - anche al Senato passerà la proposta di legge di videosorvegliare asili nido, scuole d'infanzia e strutture socio-assistenziali per disabili e anziani. Un discorso a parte va fatto per il segmento residenziale e micro professionale (SOHO, small office soft office), dove il canale vede un forte interesse purché si tratti di soluzioni ad hoc - entry level, plug&play e cost-effective - e che sta prendendo piede soprattutto da quando i produttori tra-

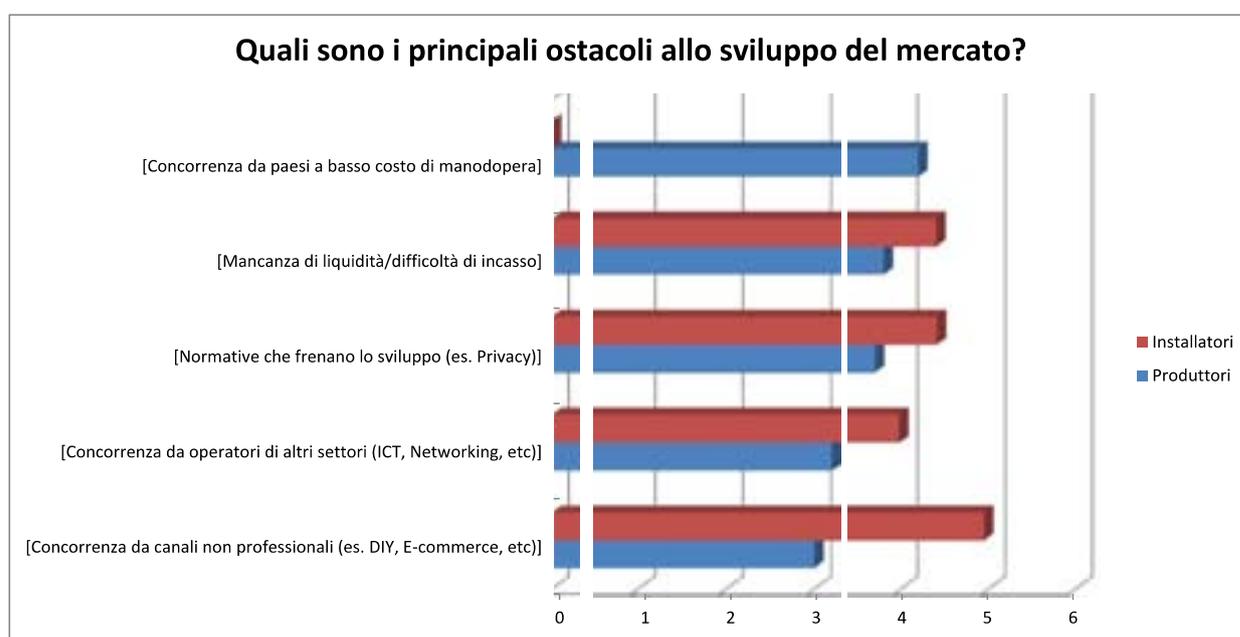


Grafico 10 - Comparazione risposte tra PRODUTTORI e INSTALLATORI

dizionali di soluzioni professionali hanno esteso la propria offerta anche ad utenze meno sofisticate (curioso notare che invece i produttori che inizialmente si sono dedicati al low end si stiano elevando, in termini tecnologici e commerciali, verso mid e high end, in un processo inverso di apertura mercati ...il cui risultato finale è che *tutti fanno tutto*).

COSA NON VA

E veniamo alle brutte notizie. Quali sono i principali ostacoli allo sviluppo di mercato?

L'abbiamo chiesto sia ai produttori, sia agli operatori del canale (**grafico 10**). Inutile dire che per i produttori l'elemento di maggiore allarme è la concorrenza da produttori di paesi a basso costo di manodopera (problema che ovviamente non colpisce il canale, il quale al contrario premia la produzione asiatica, come dimostra l'assoluta concentrazione della ricchezza nelle mani di brand di tale provenienza geografica). Altro forte elemento di allarme per i produttori è la concorrenza di operatori ben più finanziariamente robusti e abituati a climi ad altissima competizione e ridotta redditività come le realtà di area ICT, consumer o networking. Per gli installatori è invece la concorrenza da canali non professionali (DIY, e-commerce) - ma anche da produttori che vendono in forma diretta - a generare la massima

preoccupazione: saltando di netto la catena del valore, si azzerano infatti ruolo (e redditività) dell'installatore. Ed il fenomeno delle vendite online cresce di continuo: secondo una recentissima analisi del comparatore di prezzi online *idealo*, nel primo trimestre 2017 l'interesse degli italiani verso i prodotti di videosorveglianza fai-da-te è cresciuto del 34% rispetto ai soli tre mesi precedenti. Il tema non preoccupa però nella stessa misura l'industria produttiva, che può vedere nel do it yourself una possibilità di diversificazione dell'offerta e dei mercati. Ma la lista dei guai non finisce qui: per gli operatori del canale seguono nella graduatoria due problemi tutti italiani (e che quindi colpiscono soprattutto chi ha che fare con clientela diretta del Belpaese, ossia chi installa). Il primo problema è la mancanza di liquidità e soprattutto la difficoltà ad incassare, tema talmente ampio che meriterebbe trattazioni infinite, ed il secondo è la presenza di normative non di rado pervasive, come la Privacy, che frenano la determinazione all'investimento da parte dell'utente - e lato produttore (soprattutto per chi produce su scala globale) impongono costose personalizzazioni per il solo mercato italiano.

PROBLEMI CON I DISTRIBUTORI

Con il **grafico 11** si potrebbe scrivere il manuale del perfetto distributore, o meglio ciò che mai deve fare un

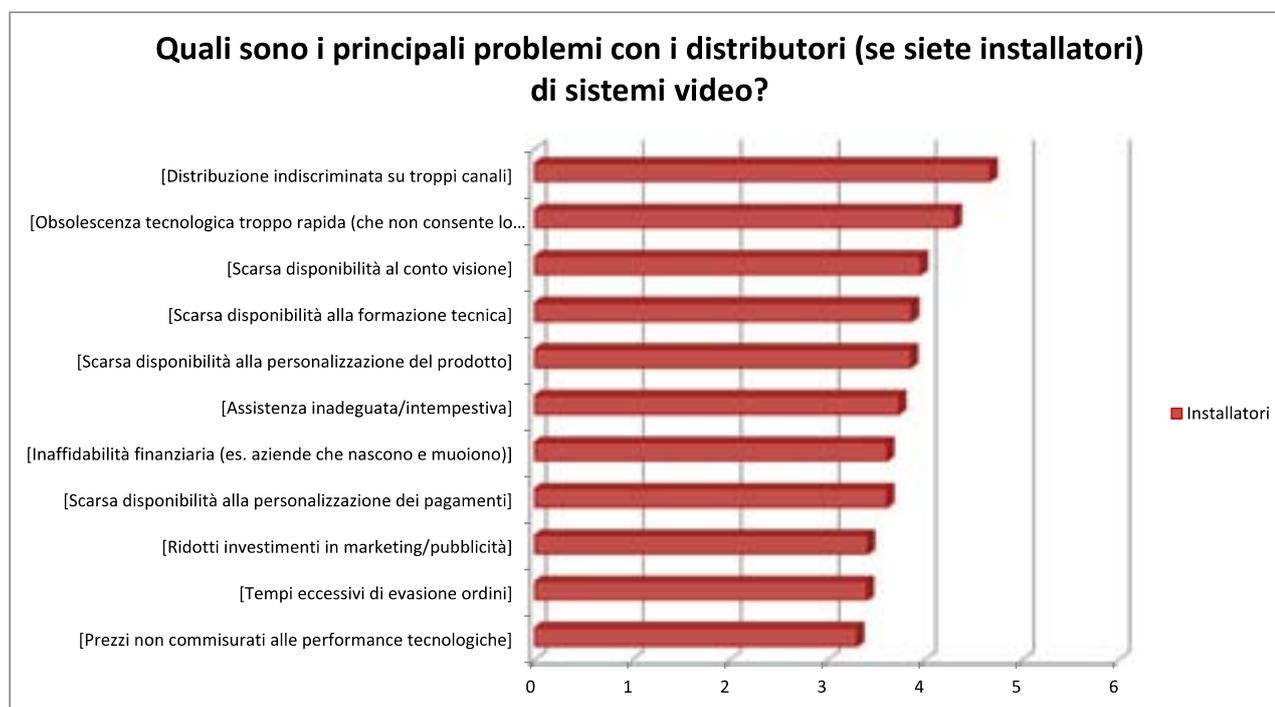


Grafico 11 - Risposte dai soli INSTALLATORI

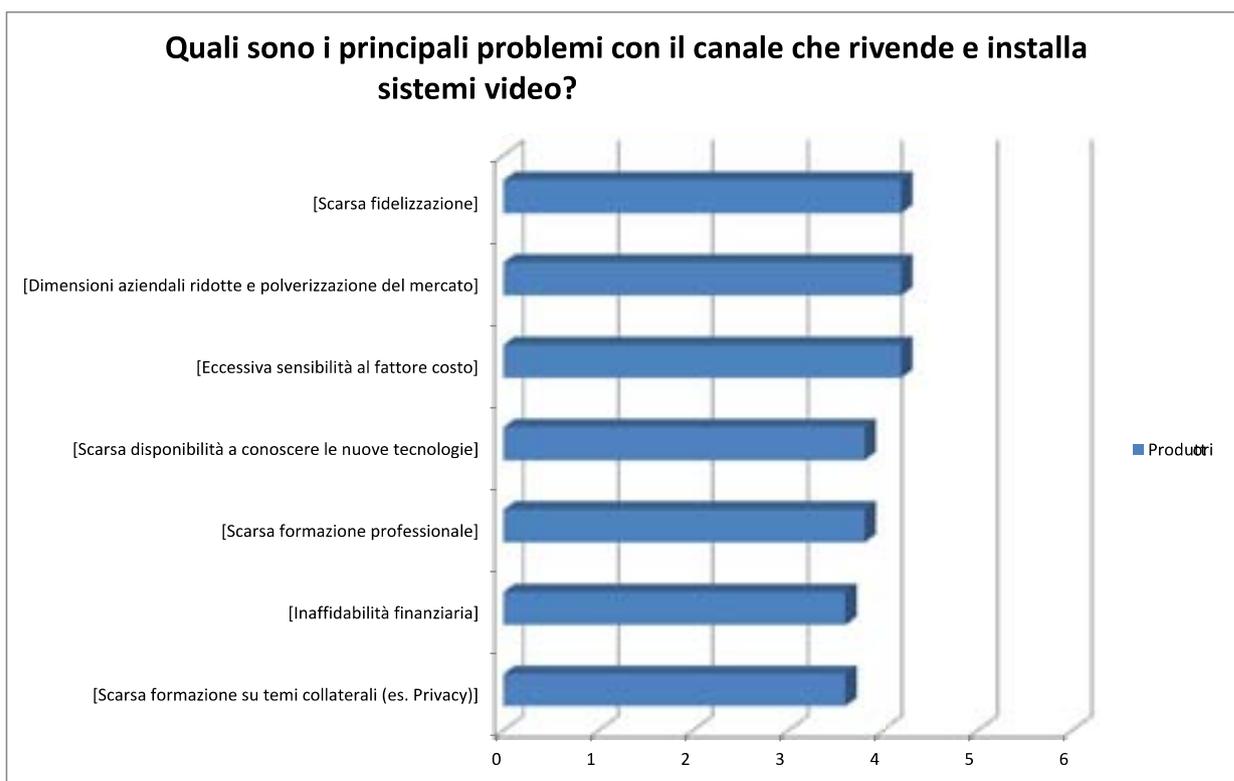


Grafico 12 - Risposte dai soli PRODUTTORI

distributore se non vuole inimicarsi a vita il proprio cliente. La prima strategia commerciale non premiante è la distribuzione indiscriminata su troppi canali, che mette gli operatori in concorrenza sul solo fattore prezzo, generando inutili conflittualità e banalizzando il livello produttivo generale del comparto. Il secondo tema è la vendita di prodotti caratterizzati da un'obsolescenza tecnologica talmente rapida da non consentirne lo smaltimento lato utenza (tema che – lato produzione - si sposa con la strategia, anch'essa poco premiante, del riempire i magazzini dei distributori con nuove linee produttive pur di alleggerire il proprio magazzino industriale). Altre fonti di lamentela verso i distributori: scarsa disponibilità al conto visione, alla formazione tecnica, alla personalizzazione del prodotto o all'investimento in marketing/pubblicità. Due temi sono poi di natura finanziaria e dipendono, se vogliamo, da una scarsa tenuta dell'intero sistema commerciale d'impresa italiano, con aziende che nascono e muoiono impunite, zero tutela del credito e quindi "scarsa disponibilità dei distributori alla personalizzazione dei pagamenti". Un buon segnale è invece che l'inadeguatezza o intempestività dell'intervento tecnico risulta essere solo in sesta posizione e i tempi eccessivi di evasione ordini addirittura a fine classifica: se ne può dedurre che i distributori italiani forniscano in

linea generale un buon livello di servizio e di assistenza tecnica. Ancor più interessante è l'ultima voce indicata, ossia prezzi non commisurati alle performance tecnologiche. Stando a queste rilevazioni, per chi installa la tecnologia, prezzo e valore viaggiano dunque di pari passo: sta quindi al distributore aggiungere ulteriore valore con servizi e cura della propria clientela.

PROBLEMI CON GLI INSTALLATORI

E ora ascoltiamo il rovescio della medaglia: nel **grafico 12**, dedicato agli elementi di criticità rilevati dai produttori verso distributori ed installatori, per certi aspetti sembra potersi ribattere punto per punto. Si parte con la maggiore rimostranza, ossia la scarsa fidelizzazione del canale verso il produttore (dolore lamentato ormai anche dai *più fortunati*, quanto meno lato fidelizzazione, produttori di sistemi d'allarme e antintrusione). La seconda problematica è la polverizzazione del mercato, ossia le dimensioni aziendali ridotte che comportano, a cascata, il terzo problema (eccessiva sensibilità al fattore costo), il quarto (scarsa disponibilità a conoscere le nuove tecnologie), il quinto e il settimo (scarsa formazione professionale e a maggior ragione su temi collaterali come la privacy), oltre ovviamente al sesto

Pensa che la formazione tecnica di settore (tecnologia e normative di riferimento), ma anche extra-settore (es. in tema di privacy) possa essere un valore aggiunto spendibile in termini di offerta commerciale?

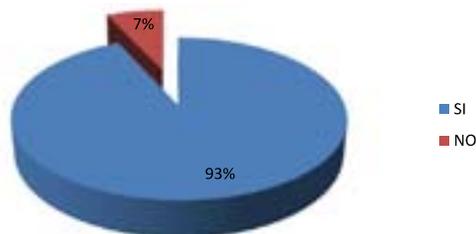


Grafico 13 - Risposta dagli INSTALLATORI

e assai drammatico problema (inaffidabilità finanziaria). Tutto sembra connesso in questo paese dove fare impresa è la più arduosa delle imprese. Certamente la polverizzazione delle imprese del canale, spesso composte anche solo da una o due figure professionali, si contrappone ad una sempre più forte concentrazione dell'industria produttiva, che si avvia verso una stretta polarizzazione dei brand. Più piccole sono le imprese, meno capitali ci sono per fare formazione e scegliere tecnologie sulla base del rapporto prezzo/prestazioni.

Sarebbe favorevole alla creazione di un registro di professionisti dell'installazione di sicurezza?

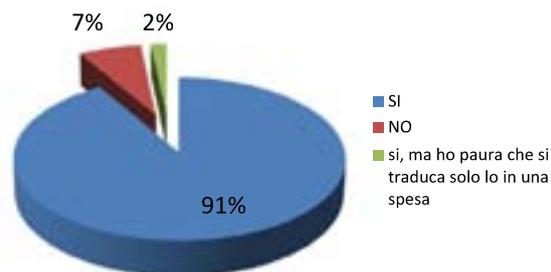


Grafico 14 - Risposta dagli INSTALLATORI

Anche se, sul fronte formazione, il 93% dei rispondenti lato canale ha dichiarato di ritenere il training tecnico di settore (tecnologia e normative di riferimento), ma anche la formazione extra-settore (ad es. in tema di privacy) un valore aggiunto spendibile in termini di offerta commerciale, quindi di redditività (**grafico 13**). E la maggioranza sarebbe anche favorevole alla creazione di un registro di professionisti dell'installazione di sicurezza (**grafico 14**).



Ipotizzereste un mercato "Security" regolamentato da una normativa armonizzata, sottostante ad un Regolamento Europeo (come nell'ambito della prevenzione incendi)

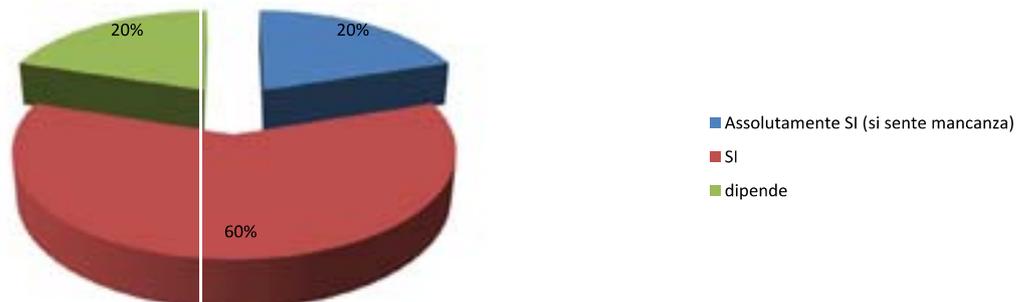


Grafico 15 - Risposta dai PRODUTTORI

UN MERCATO REGOLAMENTATO?

Dal canto suo, la maggioranza dei produttori dichiara che sarebbe favorevole ad un mercato della security regolamentato da una normativa armonizzata, a sua volta sottostante ad un Regolamento Europeo, come succede – per intenderci - nell'ambito della prevenzione incendi (**grafico 15**). La somma di queste ultime rilevazioni lato produzione e lato canale, peraltro in netta controtendenza rispetto a quanto emerso da un nostro precedente sondaggio datato 2007, ci racconta molto delle difficoltà che stanno attraversando le aziende oggi rispetto alla congiuntura precrisi. Nel felice 2007 nessuno (salvo pochissimi) voleva registri, ordini o altre restrizioni di mer-

cato, soprattutto sul fronte della produzione, che al contrario chiedeva la più assoluta libertà costruttiva. Oggi invece si immagina un mondo più selettivo, regolato da norme che premiano sicurezza, aggiornamento, rispetto delle regole, fair play competitivo. C'è da scommettere che la crisi strutturale che ha attraversato il periodo tra un sondaggio e l'altro abbia giocato un ruolo determinante. Sarà interessante vedere cosa risponderanno i player di mercato tra altri 5 e poi 10 anni. *a&s Italy* sarà ancora lì a raccogliere testimonianze, a documentarle e commentarle.



H.265 & 4K design PoE NVR



Serie NVR301-L-P

4/8/16 canali H.265

Supporto telecamere 4K

Uscita video 4K

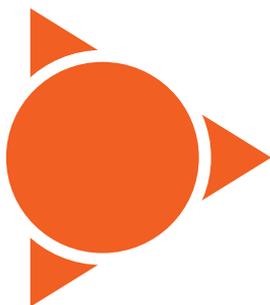
4/8 porte PoE extended 300m

Aggiornamento via Cloud

App Android e iOS



Distributore ufficiale per l'Italia



advanced innovations

www.adin.it - info@ad-in.net

Fredrik Svensson^(*)

ONVIF, Profilo T e H.265: l'evoluzione nella compressione

L'uso efficiente di banda e storage rappresenta oggi un aspetto fondamentale della manutenzione di qualunque sistema di videosorveglianza evoluto. La capacità di un sistema di gestione video di analizzare, notificare un evento in tempo reale ed offrire un eccellente dettaglio dell'immagine sono fattori di tutta importanza, ma possono essere garantiti solo se la rete presenti velocità e larghezza di banda adeguate allo scopo.

^(*)ONVIF Profile T Working Group Chair www.onvif.org

Nell'industria della sicurezza fisica, l'H.264 è oggi il formato di video compressione utilizzato dalla maggior parte delle aziende. Alcune aziende utilizzano anche versioni potenziate dell'H.264 per comprimere aree dell'immagine che non sono rilevanti per l'utente ad un rapporto più alto di stream video e dedicare una maggiore qualità dell'immagine solo ai dettagli più importanti (volti, targhe, edifici). L'anno prossimo è probabile che sarà l'H.265, successore naturale dell'algoritmo H.264, ad essere usato sempre più frequentemente. Alcune aziende hanno già adottato il protocollo H.265 nelle proprie telecamere e nei sistemi di gestione video, mentre molti produttori si stanno preparando per adottare su ampia scala l'H.265 negli anni a venire.

BENEFICI DI BANDA E STORAGE

Storage e larghezza di banda ridotti sono i principali benefici che possono apportare le tecnologie di compressione video. In alcuni casi l'H.265 può duplicare il rapporto di compressione dati dell'H.264, mantenendo la stessa qualità. Tassi di compressione maggiori significano minori requisiti di storage sugli hard drive, minore utilizzo di banda e meno switch – tutti elementi che, assieme, incidono sul costo totale di proprietà di un sistema. La compressione H.265 offre un bitrate minore dell'H.264, il che è importante per gli utenti finali e gli integratori perché un bitrate minore riduce il lavoro dell'hardware e può risolvere alcuni problemi legati al playback.

È molto importante che l'algoritmo di compressione sia però supportato da tutti i componenti del sistema: telecamere, computer su cui gira il VMS e sistema di video gestione stesso. Utenti finali e integratori devono anche essere messi nelle condizioni di comprendere le nozioni base della compressione video, in modo da poter modificare il settaggio e ridurre ulteriormente l'impiego di banda (molte telecamere vengono ad esempio fornite con un settaggio di default che può essere ridotto per comprimere i costi).

ONVIF E H.265

Nell'industria della sicurezza fisica, ONVIF lavora per accorpare alle proprie specifiche l'uso di nuovi formati come l'H.265, ma non è direttamente coinvolta nello svi-

luppo degli standard di compressione. Con il Profilo T, che ONVIF sta attualmente sviluppando, verrà utilizzato un nuovo servizio chiamato "agnostica di compressione" *compression agnostic*. Questo nuovo servizio consentirà di supportare nuovi formati di compressione video, compreso l'H.265, e nuovi formati di compressione audio, includendo nuovi codec audio e video senza dover riprogettare il servizio.

Fra le organizzazioni di standardizzazione che stanno occupandosi direttamente dei nuovi standard di compressione citiamo la International Telecommunication Union (ITU), il Moving Picture Experts Group (MPEG) e la commissione congiunta International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), che sta lavorando sulla codificazione di audio, immagini, informazione multimediale ed ipermedia. Altri formati di compressione al pari di H.264 e H.265 vengono sviluppati da aziende come Google.

H.265 E PROFILO T

Utilizzare prodotti dotati di compressione H.265 permetterà di comprimere i costi riducendo la larghezza di banda e regolando i settaggi di default sulle telecamere.

Nuovi miglioramenti all'H.265 verranno poi probabilmente sviluppati dagli stessi produttori di telecamere per ridurre ulteriormente la larghezza della banda, come già è successo con l'H.264. Quando l'H.265 sarà pronto, il suo valore come strumento dei sistemi di sorveglianza IP dipenderà poi dalla presenza di codec adeguati in ogni elemento del sistema: VMS, server hardware, schede grafiche, telecamere.

Nonostante sia prevista una grande diffusione dell'H.265, la tecnologia sta uscendo con tempistiche diverse in base ai diversi sviluppatori. Nel frattempo l'ONVIF sta comunque includendo nel suo nuovo profilo video (T) anche l'H.265, anticipando questa migrazione, nella convinzione che l'H.265 diventerà il formato di compressione più utilizzato. Il nuovo servizio, che verrà implementato assieme al Profilo T, sarà pronto per adeguarsi a qualsiasi sviluppo futuro poiché quando verranno rilasciati nuovi formati di compressione, l'ONVIF sarà in grado di adottarli in velocità – una flessibilità che aiuterà certamente gli integratori. L'idea è di rilasciare la prima bozza di specifiche per il Profilo T per una revisione pubblica come 'Release Candidate' nel 2017: seguiranno sviluppi.

Siamo **VINCENTI** sul mercato grazie
alla qualità delle **nostre aziende**

Professionalità, eccellenza nel servizio e dei prodotti sono i nostri tre punti di forza

DiMAR
ELECTRONIC Srl



www.dimarelectronic.eu

ASN



www.asntransformer.com

JIANFU



www.jian-fu.com

FC



www.forward-relays.com

WISeNET
SAMSUNG



WISeNET X series
eXtreme performance

- eXtra potenza di analisi video & audio on-board
- eXtra compressione per una migliore efficienza, fino al 99%
- eXtra video processing per prestazioni eccezionali
- eXtra storage on-board, fino a 512MB
- eXtra WDR fino a 150db, per immagini perfette in ogni condizione

eXperience it now www.WisenetX.com

 **Hanwha**
Techwin

Elvy Pianca

Banche: dove la sicurezza fisica sposa la sicurezza logica

Mercato bancario, dove la tradizionale sicurezza fisica deve essere abbinata con la difesa più all'avanguardia contro i cyberattacchi. Restano dunque le guardie giurate e le videocamere a tecnologia potenziata, come il 4K e la compressione H265, per garantire immagini di elevata qualità, utili per l'analitica forense, e, nello stesso tempo, che hanno una minore necessità di archiviazione. Ma sono indispensabili sistemi sempre più integrati, con VMS e software di ultima generazione, che interagiscono con il controllo accessi e con le banche dati. Anche se l'ultima frontiera, per garantire la sicurezza, è la biometria... e i dispositivi di autenticazione sempre più dinamici ed evoluti.



Si sa che le banche dovrebbero essere il “luogo sicuro” per eccellenza, perché è lì che, da secoli, tutti deponiamo i nostri risparmi, sia per farli maturare sia per conservarli in un posto che offra quelle garanzie che i nascondigli domestici non possono dare. E anche se, oggi, i soldi hanno sempre più un aspetto virtuale, e perfino nelle casseforti degli istituti bancari ce ne sono pochi, quando noi pensiamo alla sicurezza e ai sistemi di sorveglianza il primo edificio che ci viene in mente è certamente una banca. Sappiamo anche, purtroppo, che non sempre le strategie difensive funzionano, perché, a dispetto dei numerosi investimenti che gli istituti di credito fanno nel settore della sicurezza, il crimine è sempre in agguato, anche se, negli ultimi anni, sembra avere preso un'altra direzione. Anche nel corso dell'ultimo convegno “Banche e Sicurezza” del 2016, organizzato dall'Associazione Bancaria Italiana, è emerso che i malviventi non sono più i classici rapinatori con pistole in pugno e passamontagna in testa, ma si sono *evoluti* verso il cybercrimine. In ogni modo, le banche continuano a investire moltissimo sui sistemi di sicurezza fisica più tradizionali. Ed è da qui che partiamo nella nostra disamina sul mercato verticale rappresentato dagli istituti di credito.

SICUREZZA FISICA

Di solito, le banche devono bilanciare dei sistemi discreti e poco intrusivi, come i pulsanti di emergenza e le videocamere nascoste (ad esempio, nelle vicinanze degli sportelli ATM) con misure molto più visibili, come i grandi dispositivi per la videosorveglianza e le guardie giurate. Questo per scoraggiare i criminali, ma anche per dare ai clienti quella sicurezza che è imprescindibile dallo stesso concetto di istituto di credito. Facciamo l'esempio più classico della videosorveglianza: di solito, al di fuori dell'edificio sono installate delle telecamere a infrarosso, per assicurare un monitoraggio costante, giorno e notte, mentre all'interno le dome e le bullet sono indispensabili per avere immagini chiare e nette, che possano essere anche utilizzate per l'eventuale analitica forense.

Oggi la tecnologia di videosorveglianza IP, full HD e 4K, assieme alla compressione H.265, consentono di mantenere elevata quella qualità delle immagini che è indispensabile per riconoscere tutti i dettagli, ma anche di ottimizzare la lunghezza di banda e di ridurre notevol-



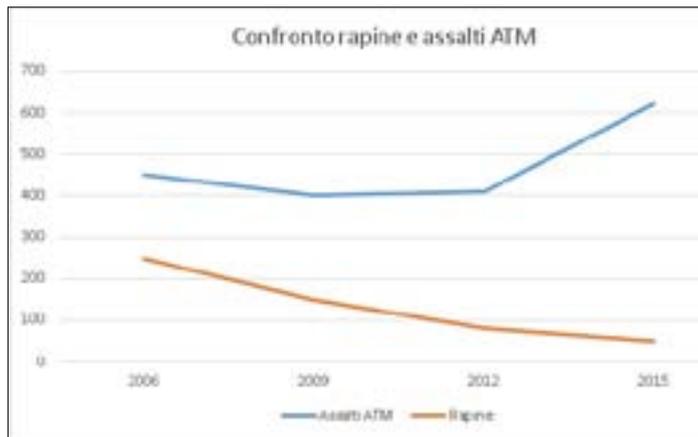
mente lo spazio di archiviazione dei dati, spesso molto pesanti.

Alle videocamere, ovviamente, va abbinato un potente software VMS, che possa integrare il monitoraggio dei video, il controllo degli accessi, il sistema di allarme e quello di comunicazione, in modo da poter interagire in tempo reale con il personale e le forze dell'ordine. Inoltre i sensori come quelli per il rilevamento fumi e la temperature, oggi, sono inseriti nelle videocamere e quindi lanciano un allarme diretto al Sistema DVR. In questa maniera, non solo si ottiene un ambiente sicuro e confortevole in cui lavorare, ma si riducono notevolmente i costi per gli altri sistemi di automazione come, per limitarsi a un solo esempio, l'HVAC.

Oggi uno dei problemi maggiori che incontrano gli istituti di credito è quello della loro *decentralizzazione*: ad esempio, sempre più spesso si trovano delle filiali abbastanza piccole all'interno di palazzi uffici o di centri commerciali. Per giunta, anche la struttura stessa delle banche è cambiata, sia dal punto di vista architettonico, con edifici sempre più aperti, sia da quello gestionale, con sempre meno personale che ha, per contro, maggiori mansioni da svolgere.

NUOVI CRIMINI

Ma la vera svolta è avvenuta proprio nella tipologia dei fenomeni criminosi. Abbiamo già accennato al calo delle rapine, però, d'altra parte, sono aumentati in maniera notevole i furti e gli assalti agli sportelli ATM. I grafici alla pagina successiva, desunti dalla disamina svolta dall'OSSIF (Centro di Ricerca dell'ABI sulla Sicurezza



Fonte: OSSIF

Anticrimine) proprio in occasione del già citato convegno, mostra immediatamente questo andamento e le metodologie d'assalto più diffuse. Secondo le analisi del fenomeno, gli assalti agli ATM hanno subito una sorta di evoluzione nel corso degli anni, passando dallo scasso più tradizionale con martelli e quant'altro all'utilizzo, sempre più diffuso, di gas ed esplosivi di ultima generazione, come la gelignite e il PETN, motivo per cui i produttori di ATM si sono a loro volta dovuti evolvere, garantendo la protezione da questi tipi di attacchi proprio a livello di sicurezza fisica del dispositivo. Ma non basta... Perché, e qui entriamo già nel campo delle frodi e del cybercrimine, gli attacchi agli sportelli ATM prevedono anche il furto delle carte o la loro clonazione, con conseguente acquisizione dei dati del malcapitato. E' per



Fonte: OSSIF

questo motivo che la videosorveglianza è utilizzata in maniera esaustiva negli ingressi o nelle vicinanze degli sportelli ATM. E non è ancora sufficiente.

Per il mercato verticale bancario, infatti, è indispensabile l'integrazione di video e di dati, tramite una piattaforma evoluta di VMS, in modo non solo da avere tutto sotto mano e consultabile in tempo reale, ma di poter prevenire, ove possibile, eventuali attacchi tramite il raffronto con le banche dati, ad esempio, delle forze dell'ordine, o, nel caso peggiore, di far partire un allarme immediato, anche video, in caso di sabotaggi o attacchi.

Ma la vera svolta, per il controllo accessi in generale, così come per la difesa degli sportelli ATM da attacchi fraudolenti, cyber o meno, è rappresentata dalla biometria. I lettori di impronte digitali o quelli dell'iride, infatti, si sostituiranno gradatamente alle tradizionali card, perché garantiscono una sicurezza maggiore rispetto a codici e numeri.

CYBER

Concludiamo con il problema, sempre crescente, dei cyberattacchi, svolti da criminali che, di solito, non si prendono nemmeno il disturbo di muoversi dalla loro postazione PC. Tutti, ormai, utilizziamo l'home banking oppure le APP su smartphone per far girare i nostri soldi e, di conseguenza, siamo maggiormente esposti ai rischi dei "cyberladri". Per riportare solo un dato, nel 2015 Kaspersky Lab, che gestisce soluzioni per la sicurezza e la protezione, fra l'altro, da attacchi on line, ha comunicato che un team di criminali multinazionali è riuscito a rubare circa un miliardo di dollari nell'arco di 2 anni in più di 100 banche in 300 Paesi diversi, tra cui Russia, Giappone e USA. Una risposta tecnologica ai servizi bancari on line è l'autenticazione cosiddetta "dinamica", in cui il livello di protezione passa sia per il firewall sia per il cloud. Ma lo stesso cellulare, che utilizziamo spesso per le operazioni finanziarie, può diventare una sorta di token, che genera una OTP (one time password), basata su una combinazione unica mediante algoritmi che garantiscono la massima sicurezza. E' per questo motivo che, oggi, le banche, senza trascurare, ovviamente, la difesa fisica, devono essere in grado di garantire quella IT, in modo che i clienti siano sicuri non solo i loro soldi reali, ma anche quelli virtuali risultino sempre protetti. E solo una soluzione *olistica* può affrontare al meglio entrambe le minacce.



Scopri la soluzione Axis per la protezione perimetrale.



Telecamere termiche di rete Axis



AXIS C3003-E Network Horn Speaker



Telecamere di rete Axis PTZ



AXIS Perimeter Defender

Consulta il calendario completo del nuovo corso ufficiale Axis Perimeter Protection, le registrazioni sono aperte



Non importa quale sia la tipologia di perimetro che vuoi proteggere, puoi contare su una soluzione affidabile 24 su 24. La soluzione di protezione perimetrale Axis consente di agire quando accade realmente qualcosa.

Visita www.axis.com/it/perimeter-protection

Pierdavide Scambi^(*)

Sicurezza negli istituti bancari: il parere del progettista

Il settore bancario, e specificatamente le banche, è stato storicamente il principale integratore e utilizzatore di sistemi di sicurezza fisica, elettronica e informatica. E' infatti di fondamentale importanza, in ambienti di natura finanziaria, poter eliminare ogni possibile rischio per le strutture, che non a caso richiedono un livello di sicurezza e protezione di massima efficienza.

^(*) Titolare dello studio di progettazione e consulenza e formazione Scambi in Vicenza www.studioscambi.com

sistemi di sicurezza continuano a rivestire un ruolo fondamentale per la gestione dei rischi all'interno delle banche e devono rispondere a criteri severissimi in ambito di sicurezza, protezione e comunicazione. Tra i problemi da gestire, occorre menzionare: rischio rapina; rischio sequestro; rischio estorsione; rischio rapimento; rischio aggressione da clienti o terzi in genere; rischio vandalismo e frode agli sportelli automatici; integrazione dei concetti di sicurezza e protezione nelle operazioni bancarie; gestione di un'ampia varietà di autorizzazioni di accesso; sistemi antintrusione e allarme, videosorveglianza, rilevamento incendio e monitoraggio costante.

La piena consapevolezza che il fenomeno delle rapine tocca aspetti molto delicati dell'operatività quotidiana ha condotto il sistema bancario, da un lato, a perseguire lo sviluppo e il rafforzamento di nuove forme di collaborazione con le istituzioni preposte all'ordine pubblico e, dall'altro, a dirigere gli sforzi verso una più efficace prevenzione interna, soprattutto attraverso iniziative rivolte alla progressiva diffusione di sistemi di sicurezza ad alta innovazione tecnologica e di strumenti informativi e formativi per i dipendenti.

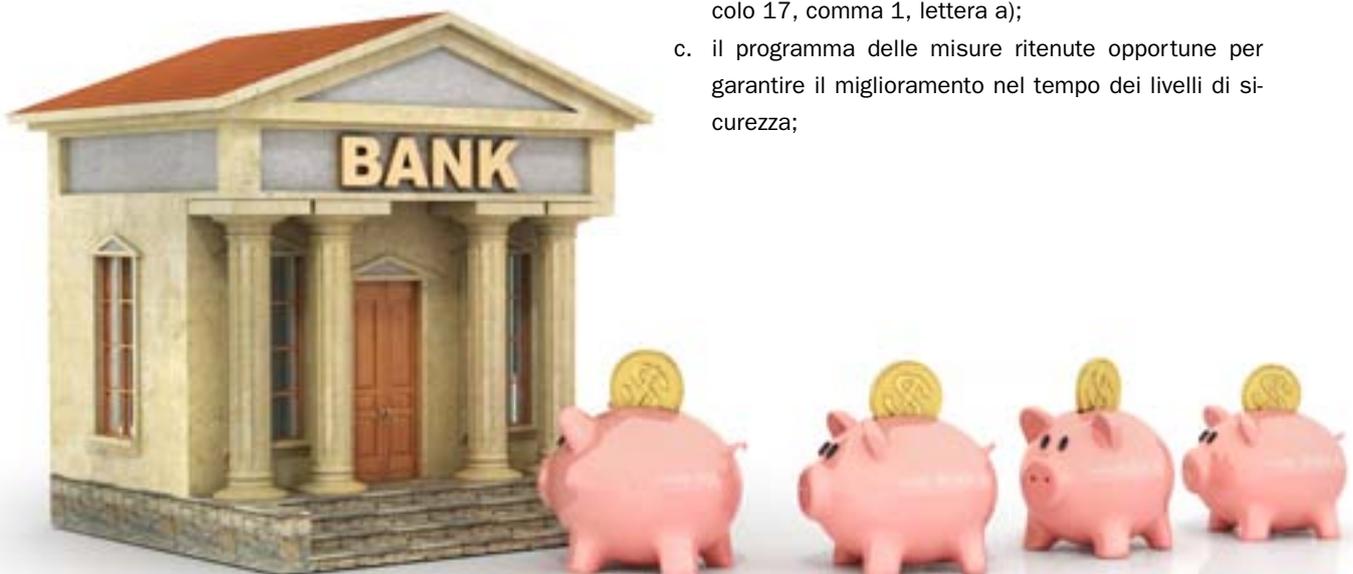
NORME, GIURISPRUDENZA, PROTOCOLLI

L'evoluzione è stata anche sottolineata da numerose pronunzie giurisprudenziali. Difatti l'articolo 2087 del

Codice Civile recita: "l'imprenditore è tenuto ad adottare, nell'esercizio dell'impresa, le misure che secondo la particolarità del lavoro, l'esperienza e la tecnica sono necessarie a tutelare l'integrità fisica e la personalità morale dei lavoratori". La norma impone un obbligo di protezione: il datore di lavoro deve dunque adottare tutte le misure idonee a proteggere il lavoratore nell'ambiente di lavoro, non solo in relazione ad attività collegate direttamente allo svolgimento della prestazione lavorativa, ma anche ad attività ad essa estranee, quali ad esempio quelle criminose messe in opera da terzi (Cassazione Civile Sez. Lav. 22 marzo 2002 n.4129). Le "misure" da adottare non si riferiscono solo a regole di esperienza collaudate e preesistenti, ma a tutte quelle idonee a preservare l'integrità psicofisica, tenuto conto della concreta realtà aziendale e della possibilità di venire a conoscenza e di indagare sull'esistenza di fattori di rischio in un determinato momento storico (Cassazione Civile Sez. Lav. 14 gennaio 2005 n.644).

La valutazione del rischio secondo il D.L. n.81 del 9 aprile 2008 testualmente recita all'articolo 28, comma 2: Il documento di cui all'articolo 17, comma 1, lettera a), redatto a conclusione della valutazione, deve avere data certa e contenere:

- a. una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa, nella quale siano specificati i criteri adottati per la valutazione stessa;
- b. l'indicazione delle misure di prevenzione e di protezione attuate e dei dispositivi di protezione individuali adottati, a seguito della valutazione di cui all'articolo 17, comma 1, lettera a);
- c. il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;



- d. l'individuazione delle procedure per l'attuazione delle misure da realizzare, nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, a cui devono essere assegnati unicamente soggetti in possesso di adeguate competenze e poteri;
- e. l'indicazione del nominativo del responsabile del servizio di prevenzione e protezione, del rappresentante dei lavoratori per la sicurezza o di quello territoriale e del medico competente che ha partecipato alla valutazione del rischio;
- f. l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione e addestramento.

A dimostrazione dell'impegno e dell'attenzione con cui il settore bancario segue il fenomeno criminoso, si pongono i numerosi protocolli d'intesa finalizzati a prevenire e contrastare la criminalità in banca sottoscritti dall'ABI e dalle banche con le Prefetture e con le Forze dell'Ordine (Polizia, Carabinieri e Guardia di Finanza).

MISURE TECNOLOGICHE

Per tutelare sia i dipendenti bancari che i clienti della filiale, gli istituti bancari si sono dotati di vari tipi di misure di protezione contro i fenomeni di furti, aggressioni e rapine. Ma spesso dotarsi solamente di bussole per l'accesso controllato, di tornelli, porte accessibili solo con consenso elettronico, metal detector e impianto di videosorveglianza, non basta. L'orientamento generale (che comunque trova riscontro anche nel mercato privato, pubblico e industriale) è la progettazione e realizzazione di una serie di prodotti altamente tecnologici, basati su tecnologia IP, che integrati anche su sistemi di sicurezza già esistenti, permettono di gestire in modo automatico

tutta la sicurezza e la videosorveglianza bancaria.

Per quanto riguarda il controllo accessi, attraverso l'utilizzo di sistemi software di riconoscimento biometrico, le telecamere installate all'interno e/o all'esterno delle bussole di accesso sono in grado di rilevare i volti delle persone che si presentano coperti o mascherati, associando quindi in determinate aree identità e diritti di accesso. Ad integrazione delle funzioni sopra descritte, l'analisi video permette inoltre, in automatico, di rilevare spostamenti di persone nell'area monitorata e di identificare il superamento di barriere fisiche (finestre, balconi, terrazze, griglie, porte ecc.), compreso l'abbandono di borse e oggetti sospetti. Inoltre, tramite moduli aggiuntivi costituiti da schede di campo o protocolli di supervisione di centrali antintrusione, controllo accessi e rilevazione fuoco o fumo di terze parti, si aggiungono tutti i dispositivi di filiale (quali sensori volumetrici, sismici, contatti, rilevatori di fumo, badge, transponder ecc.) visualizzandone la gestione all'interno della piattaforma software. I presenti moduli, dotati di interfaccia web, di alimentazione PoE e predisposizione su barra DIN, consentono di controllare da remoto qualsiasi dispositivo, integrando in una unica soluzione sistemi di sicurezza, domotica e building automation con una estrema semplicità. E' anche disponibile per sistemi in ambito enterprise e corporate una gestione di parametri ambientali, funzioni di storage failover, backup a caldo, connessioni contemporanee, centralizzazione multi sito, virtual machine, watermarking (certificazione sulla non manipolabilità delle immagini registrate) per un numero illimitato di utenti. Il concetto di piattaforma aperta consente, attraverso il software, di personalizzare ogni aspetto dell'interfaccia, adattandola ad ogni ambito installativo, ponendo in primo piano le esigenze di sicurezza della filiale bancaria.





Costruire nebbiogeni è un'arte

scopri la nuova Serie Eos



**Il più sottile
al mondo**



**Tecnologia
brevettata Vortex®**



**Distribuzione
specialistica**



**Gestione via web
integrata**



Numero verde

800944848

approfondisci su

aes.aurasicurezza.com

ne parliamo con Thomas J. Langer, CPP – ASIS International President

L'approccio olistico alla security secondo ASIS International

Three gingerbread men are standing on a computer keyboard. They are positioned in a row, with their arms slightly out to the sides. The keyboard keys are visible in the foreground and background, creating a sense of depth. The gingerbread men are a reddish-brown color with white icing details on their heads and bodies.

A fine marzo si è tenuta a Milano l'annuale ASIS Conference. Tante le tematiche sul piatto, ma in particolare una, lanciata dal Presidente di ASIS International Thomas J. Langer: pensare in modo diverso, uscire dalla propria comfort zone, abbracciare nuove prospettive, avere un approccio olistico. In due parole: think different.

D all'osservatorio ASIS, a quali aspetti dovrebbe fare più attenzione l'industria?

È fondamentale che la disciplina della sicurezza si faccia parte integrante del lavoro di progettazione e dell'innovazione del prodotto già a partire dal front end; diversamente diventa molto costoso trovare soluzioni ai problemi della committenza e recuperare poi la fiducia dell'utente aggiungendo tecnologie che sappiamo essere state corrotte.

In termini di protezione degli asset, delle persone e delle informazioni, quali trend ravvisa?

Innanzitutto che sono tutti e tre egualmente importanti. Certo abbiamo degli obblighi in termini di protezione fisica dei nostri impiegati ma, poiché ormai le aziende non hanno più veri confini fisici, le informazioni si estendono oggi a tutti gli addetti, ovunque essi si trovino. Dobbiamo quindi progettare piattaforme che permettano loro di lavorare in tutta sicurezza anziché progettare la sicurezza in modo artificioso, finendo poi di fatto per indurli ad aggirarla. I professionisti della sicurezza non devono progettare soluzioni che siano per loro rassicuranti se poi il business non ne beneficia.

Cosa si dovrebbe imparare dagli attacchi di cybersecurity e quali altre minacce ci attendono?

Il tema cyber è onnipresente: ovunque siano le nostre informazioni, lì ci saranno beni da proteggere. Ed il primo pericolo risiede nelle nostre reti. Occorre ad esempio scegliere con attenzione il cloud: consegnare i propri dati ad un provider cloud sbagliato può mettere a serio repentaglio le informazioni e, visti i progressi nella portabilità dei dati e nella loro disponibilità, non possiamo avere idea di dove finiranno in futuro. Una secondo fonte di preoccupazione è la necessità di mettere in campo adeguati programmi formativi man mano che si introducono nuovi dipendenti: tutti devono capire cosa devono tenere al sicuro e come.

Quale sarà la locomotiva alle aziende sicurezza? IoT e big data?

Occorre primariamente capire come le aziende utilizzeranno i big data, e per farlo occorre sedersi al tavolo decisionale e condividere con i vertici le decisioni su



Thomas J. Langer, Presidente di ASIS International

come mettere al sicuro la piattaforma, anticipandone per quanto possibile le vulnerabilità. E' essenziale che l'industria guardi un dispositivo chiedendosi anche come verrà usato, perché innovare senza mettere al sicuro la propria innovazione è un errore che può rivelarsi fatale, dato che prima o poi l'utente finale farà scelte basate sulla sicurezza, di questo sono convinto. Attraverso l'Enterprise Security Risk Management (ESRM), come ASIS cerchiamo di diffondere il pensiero che la gestione del rischio aziendale richiede una visione olistica per comprendere le vulnerabilità di un'organizzazione nel suo complesso, nelle linee funzionali e di business. Molti di noi già lo fanno, ma credo sarebbe utile dare un nome a questo approccio e creare una disciplina che stimoli la community a pensare in modo olistico. Il CSO, chief security officer, con la giusta rete di rapporti, può infatti aumentare la consapevolezza generale sul rischio, far sì che tutti i manager comprendano minacce e conseguenze e possano scegliere di assumersi il rischio come team manageriale.

Se la risposta dev'essere olistica, anche il rischio può ormai considerarsi olistico?

La convergenza tra rischio fisico e cyber sta cambiando le aspettative della funzione corporate della security e le

MANTA

50-80m

BARRIERA A MICROONDA DIGITALE
ANCHE IP & PoE



IP
READY
& PoE

FUZZY
LOGIC
INSIDE

6 YEAR
warranty

WAVE-TEST2
SOFTWARE PER
CONFIGURAZIONE
E MANUTENZIONE
DA REMOTO



- ANTENNA PLANARE 10Ghz
- 100% DIGITALE **FUZZY LOGIC**
- **IP & PoE READY**
- SETTAGGIO MASCHERAMENTO
- SETTAGGIO SENSIBILITÀ
- GESTIONE DA REMOTO
- **16 CANALI**
- PASSAGGIO CAVI PROTETTO
- **6 ANNI** DI GARANZIA
- ALIMENTAZIONE 13,8Vcc

SINCE 1974



CIAS ELETTRONICA S.R.L.
VIA DURANDO, 38 | 20158 MILANO | ITALY
T +39 02 3767161 | F +39 02 39311225
WWW.CIAS.IT | EXTREME@CIAS.IT

competenze dei professionisti della security stanno evolvendo di conseguenza, come pure le carriere. Mentre la gestione della sicurezza un tempo era una “seconda professione” che attingeva da persone con un passato in ambito militare o nelle forze dell’ordine, i nuovi arrivati cominciano la professione direttamente dall’università o giungono alla sicurezza da altre funzioni aziendali. ASIS International si sta adattando alle necessità in cambiamento dei soci, dai nuovi arrivati ai senior executive, e dei loro dipendenti.

Cos’ha ASIS da offrire?

Una community, innanzitutto. Ci sono tanti liberi professionisti in questo ambito che non sanno a chi rivolgersi: noi offriamo un gruppo di pari che li possano aiutare ad affrontare i problemi facendo crowd-sourcing di soluzioni e vogliamo dar vita ad una comunità sempre più grande. Il Chapter è piccolo, ma l’organizzazione si espande nelle varie regioni di tutto il mondo: al momento esistono 241 Chapter a livello globale e 34 Council. Possiamo dire di rappresentare il settore.

Due parole sul Chapter italiano?

E’ estremamente attivo e svolge un lavoro formidabile: bastava vedere le 700 persone richiamate a Milano per toccare con mano il loro impegno. L’importante presenza del CEO di Microsoft Italia ha dimostrato la trasformazione di questa Associazione, che vuole portare grandi leader del pensiero davanti a professionisti della security e non vuole solo far dialogare soggetti del settore con altri soggetti del settore. L’obiettivo è far uscire i nostri operatori fuori dalla comfort zone ed aiutarli a pensare in modo diverso.

Quali sono le opportunità mancate o le soluzioni necessarie secondo i membri di ASIS?

Un’opportunità mancata avviene ogni volta che lasciamo i soci soli mentre cercano di risolvere un problema. Vogliamo creare reti locali o regionali a cui un membro si possa rivolgere per ricevere assistenza. Dal momento che la tecnologia cambia rapidamente e ci espone a vulnerabilità prima inimmaginabili, vogliamo che ASIS sia una risorsa a cui gli associati possono rivolgersi sempre.

SPEED DOME IP

H.265/HEVC 2 megapixel 30X con IR 150 m

Speed Dome IP **2MP** (1920x1080)

Sensore CMOS Sony EXMOR R da 1/2.8"

Obiettivo 4.5-135mm

Filtro IR meccanico, **zoom ottico 30x**, zoom digitale 16x

H.265/HEVC e **H.264** Multistream

Alimentazione **PoE++**

4 ingressi di allarme e 1 uscita, RS485

Ultra WDR 120dB, funzione Defog, IR 150m

IP66, **IK10**, **sensore giroscopico**, slot microsd max 64GB

Funzioni analisi video intelligente

Speciale verniciatura antigoccia (Huawei coating glass)

Temperatura -40°C / +60°C



DEATRONIC

Cell. +39 335 1306127- cartasegna@deatronic.com

www.deatronic.com

Antonella Sciortino^(*)

Compressione e cybersecurity: nuove sfide per la videosorveglianza



Il settore delle telecamere di sorveglianza vede un'evoluzione tecnologica praticamente quotidiana in particolare a livello di lenti, sensori ed elaborazione dell'immagine signal. La ricerca ha l'obiettivo di consentire una registrazione nitida e accurata delle immagini di sorveglianza di persone e auto. Parlando di risoluzione, ad esempio, si è partiti un decennio fa con l'analogica (720 x 480), per poi passare negli ultimi anni all'HD (1280 x 720), al FHD (1920 x 1080) e poi al 4K (3840 x 2160) e si prevede che l'evoluzione futura verso l'ultra definizione sarà ancora più veloce. L'avanzare dell'alta definizione alza in modo esponenziale il volume di dati video, a livelli non paragonabili a quelli dell'epoca analogica e, di conseguenza, anche i costi di rete e storage sono diventati un punto critico.

^(*) Field Marketing Manager Pro Camera Solution BU Panasonic System Communications Company Europe
<http://business.panasonic.it/soluzioni-di-sicurezza>

D' altro canto, è importante analizzare il fatto che non tutto il contenuto video registrato viene effettivamente utilizzato dal committente - che, anzi, spesso elimina gran parte del girato ancora prima di analizzarlo. Va da sé, quindi, che gli sforzi in ricerca e sviluppo da parte dei produttori devono puntare a fornire al mercato soluzioni e tecnologie che permettano di ottimizzare storage e trasmissione di dati, consentendo quindi di risparmiare concretamente sui costi della videosorveglianza, salvando e memorizzando cioè solo i filmati che si rivelano veramente necessari. Ci sono ambiti, come quello della sicurezza urbana, ad esempio, in cui oggi è più che mai indispensabile avere a disposizione immagini nitide e chiare di persone e automobili, tenendo, al contempo, sotto controllo il volume dei dati complessivo. Esistono elementi cosiddetti "di fondo", quali muri e strade, di cui non è così fondamentale raccogliere immagini al massimo della risoluzione ed accuratezza e l'evoluzione tecnologica oggi permette di ridurre i dati fino a circa il 65% rispetto al passato (col FHD) o fino a circa 80% (col 4K).

SMART CODING

Sul mercato⁽¹⁾ sono ormai disponibili sistemi estremamente avanzati e prodotti dotati di tecnologie di compressione all'avanguardia. Tra queste, ad esempio, si parla molto dello Smart Coding, che permette di raccogliere i filmati delle telecamere di videosorveglianza per un lungo periodo di tempo e di selezionare quali parti e immagini conservare in alta qualità. Lo *Smart Coding* si compone di due tecnologie principali. La prima trasforma in "dati di analisi" solo le immagini dei soggetti che si desidera monitorare, ad esempio persone o auto. La seconda agisce sulla riduzione del rumore generato durante la notte o in ambienti a bassa illuminazione, abbassando il volume di dati. La combinazione di tutte queste funzionalità, con la risoluzione 4K oggi applicabile alle telecamere in commercio, permette di raggiungere risultati davvero mai raggiunti prima nella videosorveglianza urbana.

H265

Un'altra delle tecnologie del momento, mirata a ridurre l'utilizzo di banda e i relativi costi aziendali senza dover

predisporre infrastrutture aggiuntive dedicate, è l'H265. Il nuovo standard di compressione soddisfa le esigenze di sicurezza dei contesti più complessi, quali sicurezza cittadina, incroci stradali, aeroporti, stazioni, aree portuali, grossi centri commerciali. Noto anche come High Efficiency Video Coding (HEVC), il nuovo standard supporta risoluzioni fino a 8192x4320, raddoppiando il rapporto di compressione dei dati rispetto al "vecchio" H.264 e garantendo lo stesso livello di qualità video con una maggiore efficienza del sistema, grazie ad un minor consumo di banda⁽²⁾. Grazie all'H265 non è necessario avvalersi di NVR o server di registrazione e archiviazione per sfruttare appieno le immagini riprese in alta definizione, direttamente sulla camera.

SECURE COMMUNICATION

La capacità di resistenza al pericolo di attacchi cybernetici sta diventando poi un fattore sempre più critico e prioritario nella valutazione, da parte delle aziende, delle tecnologie e dei sistemi di cui avvalersi per il proprio impianto di videosorveglianza. All'interno del cyberspazio è molto facile che i dati scambiati durante qualsiasi tipo di comunicazione vengano intercettati da terze parti per essere utilizzati a fini fraudolenti e lo stesso rischio di furto e di utilizzo scorretto di contenuti può verificarsi con le immagini. Per fronteggiare l'aumento di attacchi alla sicurezza delle infrastrutture di rete, i produttori più accorti⁽³⁾ hanno sviluppato una serie di tecnologie affidabili per la protezione dei dati nelle proprie soluzioni di videosorveglianza. La funzionalità *Secure Communication* permette di proteggere da attività illecite quali lo spoofing (i dati falsi), la manomissione e l'alterazione di video (modifica di immagini) e lo snooping (il furto di password), salvaguardando le comunicazioni di sorveglianza IP. Si tratta di una tecnologia di sicurezza di livello simile a quello dei PC che può essere integrata nelle telecamere IP per fornire varie funzionalità di protezione dei dati, tra cui la crittografia delle informazioni, la crittografia delle comunicazioni IP e la verifica, garantendo l'integrità delle evidenze video e dei dati complessivi per i flussi di streaming video IP.

⁽¹⁾ Panasonic sviluppa sistemi avanzati, mirati a soddisfare specifiche esigenze di aziende e istituzioni, ed investe per dotare i propri prodotti di tecnologie di compressione all'avanguardia come lo Smart Coding.

⁽²⁾ Che nei prodotti Panasonic migliora ulteriormente grazie alla combinazione con la funzione Smart Coding.

⁽³⁾ Panasonic ha integrato questa tecnologia di sicurezza nelle sue telecamere IP per fornire varie funzionalità di protezione dei dati.

soluzioni

tecnologie

normative

IP Security forum 2017

19^a edizione

**NUOVA
FORMULA**



BARI • 26 MAGGIO 2017

THE NICOLAUS HOTEL - VIA CARDINALE A. CIASCA, 27 - BARI

un evento di:



event.**secsolution**

Ethos Media Group s.r.l. - Via Venini, 37 - 20127 Milano (Italy) - ethos@ethosmedia.it - www.ethosmedia.it

in collaborazione con:



registrazione su: www.ipsecurityforum.it



HIKVISION



TOTAL SOLUTION PROVIDER

CCTV | Intrusion | Intercom | Access Control

www.hikvision.com

HIKVISION VIDEOSURVEILLANCE: UN'INTERA GAMMA DI OPPORTUNITÀ

Essere partner del produttore n. 1 al mondo di videosorveglianza significa essere partner di un leader da 4,67 miliardi di dollari di fatturato nel 2016, che cresce ad un ritmo del 50% (media sugli ultimi 10 anni) e che vanta una gamma di videosorveglianza assolutamente unica per completezza di soluzioni e capacità di soddisfare qualunque esigenza prestazionale e di budget. L'intera linea si caratterizza per performance, semplicità d'uso e intuitività di installazione, configurazione, manutenzione ed upgrade.



APPARATI DI RIPRESA

Le telecamere Hikvision, indoor e outdoor, spaziano su tutti i formati (bullet, dome, box, minidome, cube, turret, fisheye, panoramica, covert) e tutte le funzionalità (camere termiche, ANPR, termometriche, ad uso mobile, PTZ), coprono qualsiasi specificità (antivandalo, anticorrosione, explosion proof), risolvono ogni problematica di luce, criticità e alimentazione ed incorporano tutte le tecnologie: dall'analogico standard alle più sofisticate network camera con funzioni di analisi Smart, passando per il Turbo HD, che porta la tecnologia megapixel sull'infrastruttura coassiale.



APPARATI DI REGISTRAZIONE

Assieme a DVR e NVR tradizionali, Hikvision ha progettato dei DVR che sfruttano più protocolli (HD-TVI, analogico standard, AHD, IP megapixel) e modelli evoluti che incorporano il modulo interfaccia per l'ATM. La linea comprende infine encoder e decoder, apparati di trasmissione (switch, router) e dispositivi per lo storage (SD card, HDD), nonché custodie ed accessori, monitor, tastiere e display.



VIDEO MANAGEMENT SOFTWARE

L'estrema flessibilità tecnologica della linea Hikvision ruota attorno al software di video gestione PC e mobile iVMS: una piattaforma unica e trasversale sulla quale converge l'intera gamma di soluzioni end to end - dall'entry level al professional, fino ai più raffinati mercati verticali. Hikvision ha infatti sviluppato applicativi e soluzioni specifiche per soddisfare anche i mercati più esigenti: dai trasporti alle realtà governative, dalle banche alle infrastrutture critiche. Essere partner di un leader come Hikvision significa quindi disporre di una gamma intera di opportunità e avere tutte le carte in regola per affrontare qualunque progetto.

HIKVISION

Hikvision Italy
Via Abruzzo 12, Z.I. S. Giacomo - 31029 Vittorio Veneto
T +39 0438 6902 - F +39 0438 690299
info.it@hikvision.com

Vittorio Veneto | Roma | Milano | Bologna

www.hikvision.com

a&S ITALY

sale a quota 55.000

e da' i numeri...



55.000

le copie totali
nel 2016

70%

il market share
raggiunto anche nel
2016

9

le indagini pubblicate
nel 2016

6

numeri l'anno

9.167

le copie a numero
(sei) sottoposte
a certificazione
nel 2016

59.000

le copie previste
nel 2017

53

gli eventi a cui
abbiamo partecipato
in Italia e all'estero
nel 2016

968

pagine stampate
nel 2015

986

pagine stampate
nel 2016

132

i punti di
distribuzione
delle copie

Filippo Novario^(*)

Public Safety e ICT Organizzazioni ed Enti, pubblici e privati, tra nuove tecnologie e soluzioni

L'avanzamento tecnologico legato allo sfruttamento civile delle soluzioni informatiche non è parallelo a quello concernente il loro sfruttamento in caso di crisi ed emergenza. Know-how, sviluppo tecnico e cura delle infrastrutture ICT, da parte degli enti non coinvolti direttamente nella tutela della pubblica sicurezza, sono doveri civici che possono annullare il *gap*.

^(*) Dott. Ric. Filippo Novario, Dottore di ricerca e già Docente a contratto per università nazionali ed internazionali di Informatica Giuridica e Forense; *Senior Consultant* per enti pubblici, privati ed enti di certificazione internazionale nei campi della *Cybersecurity*, Informatica Giuridica, *Digital Forensics* e *Hacking*; Direttore scientifico della banca dati *online IGFWeb*, Giappichelli Editore; docente Ethos Academy.

La *Public Safety*, in italiano Sicurezza Pubblica, è l'insieme di organizzazioni ed enti, istituiti a livello nazionale ed internazionale, per la creazione e la gestione di un territorio in modo stabile e sicuro. Lo scopo è perseguito attraverso la protezione di persone - soggetti presenti sul territorio - e *asset* strategici - aziende di importanza vitale per il Paese - da pericoli naturali e provocati dal uomo. A titolo di esempio: attacchi terroristici, *fault* tecnologici, pericoli radiologici, accadimenti naturali, etc. Nonostante la disciplina sembri più orientata alla sicurezza fisica, l'impatto dell'*Information and Communication Technology* è sempre stato un elemento fondante. Gli addetti alla tutela della pubblica sicurezza, per un performante svolgimento dei loro compiti, hanno la necessità di acquisire, analizzare, distribuire e conservare informazioni provenienti da differenti contesti e realtà. Sotto questo aspetto, la principale applicazione dell'ICT per la *Public Safety* è nell'ambito delle comunicazioni, vocali e telematiche, al fine di consentire, e garantire, il coordinamento gerarchico di differenti organizzazioni e di aziende strategiche.

IMMOBILISMO TECNOLOGICO

Prerogativa dell'impatto ICT sulla *Public Safety*, nonostante il suo importante apporto, è il quasi totale immobilismo tecnologico delle soluzioni connettive, portato da tre fattori fondati su questioni non prive di ragionevolezza:

- la *Public Safety* è ambito d'intervento pubblico, che poggia su soli fondi pubblici non illimitati;
- le tecnologie utilizzate devono essere sicure, testate e concretamente funzionanti;
- i protocolli di sicurezza per l'utilizzo delle soluzioni tecnologiche devono essere solidi, concretamente performanti e di alto livello.

L'immobilismo tecnologico si fonda anche sull'alto grado di sicurezza, associato alle attività disposte dai soggetti coinvolti nella *Public Safety* attraverso tecnologie ICT. Questi, infatti, svolgono alcune attività sensibili, sotto il profilo della sicurezza nazionale come della *privacy* dei cittadini, tra cui: consultazione di *database* per la verifica dei dati; sorveglianza attraverso soluzioni video e sensori connessi via *wireless* o rete cablata; scansione digitale di documenti; localizzazione satellitare; trasmissione telematica di planimetrie; monitoraggio medico da remoto per utenti e membri dello staff.

Le attività digitali-telematiche disponibili dalle organizzazioni pubbliche, ma anche private di tipo strategico, a fini di sicurezza pubblica, sono dunque pervasive. Tecnicamente, la possibilità di svolgere le attività affonda le radici in quattro principi essenziali, che possono minare diritti costituzionali come essere minati dall'evoluzione tecnologica:

- Interoperabilità:** l'utilizzo di differenti sistemi con il mantenimento di un alto livello di riservatezza nell'elaborazione-trasmissione dei dati.
- Connettività:** l'utilizzo di sistemi *hardware* e *software* tali da consentire la connettività in momenti di emer-



genza e crisi, infrastrutturale ed energetica.

- **Robustezza:** l'utilizzo di sistemi *hardware* e *software* di tale solidità da poter essere difficilmente compromessi o distrutti.
- **Ciclo di vita tecnologico:** l'utilizzo di sistemi *hardware* e *software* tali da garantire un'ampia funzionalità operativa nel tempo.

INFORMATIZZAZIONE MASSIVA

I fattori, le attività e i principi prima indicati impattano, però, con la realtà socio-tecnologica digitale-telematica. Le case produttrici di *hardware* e *software*, per fini civili e commerciali, producono soluzioni tecnologiche a ritmi esponenziali. I cittadini posseggono sistemi connettivi di alto grado tecnologico - tra cui connessioni *internet*, via *wireless* e rete cablata, *smartphone* e *tablet* - sviluppati per il grande pubblico in base a *standard* internazionali per la comunicazione vocale e dati. Gli enti pubblici e privati, anche non strategici, sono al centro di un movimento per l'informatizzazione massiva delle loro attività e delle modalità di controllo. Queste ultime sotto il profilo digitale e telematico legato alla sicurezza fisica, tra cui spiccano la video sorveglianza e il controllo accessi, e alla sicurezza logica, tra cui spicca la *cyber security* degli *asset* aziendali. I dati socio-tecnologici permettono di sollevare una questione: il substrato socio-tecnologico può essere sfruttato dai soggetti addetti alla *Public Safety* sotto gli aspetti comunicativi, connettivi e di sicurezza? La risposta è affermativa. Attraverso prerogative di coordinamento, professionali, tecniche e di *know-how* che possono essere così declinate.

1. Oltre alle infrastrutture digitali e telematiche preposte alle sole operazioni di *Public Safety*, i soggetti coinvolti è utile considerino, in casi straordinari, le infrastrutture pubbliche e private, non direttamente

legate al piano di sicurezza pubblica, come elementi utili per la connettività voce-dati.

2. I soggetti coinvolti nelle procedure di *Public Safety* è utile annoverino tra il loro personale professionisti, o gruppi di lavoro, con peculiari *know-how* informatici, in particolari concernenti l'*hacking*, per lo sfruttamento, in casi straordinari, di risorse digitali e telematiche, private e pubbliche, non direttamente ricomprese nel piano per la sicurezza pubblica.
3. Gli enti privati e pubblici, non strategici e non direttamente coinvolti nel piano per la sicurezza pubblica, a fronte del possibile contributo che possono fornire con i loro sistemi digitali-telematici sviluppati a fini civili e commerciali, è utile assicurino la *business continuity* e il *disaster recovery* delle loro infrastrutture ICT anche, se possibile, in caso di grave crisi e/o emergenza.
4. Le aziende produttrici di *hardware* e *software* è utile rispettino rigidamente gli *standard* connettivi e di sicurezza del proprio comparto di riferimento, così da agevolare le attività di *Public Safety* in casi di fruizione straordinaria dei sistemi e la conseguente collaborazione socio-tecnologica nella gestione della sicurezza pubblica.

L'incessante sviluppo tecnologico digitale-telematico delle infrastrutture ICT, in campo civile e commerciale, può essere un'importante fonte di agevolazione nella gestione della sicurezza pubblica, qualora riconosciuto quale elemento tecnico ulteriore alle tradizioni dotazioni di sistemi connettivi per voce e dati. Consentendo così il perpetrare del ragionevole immobilismo tecnologico, a fini di *performance* e sicurezza, delle infrastrutture dedicate alla *Public Safety*, ma permettendo, in casi straordinari, lo sfruttamento, secondo profili di necessità e sicurezza, di tecnologie più moderne e diffuse, seppur non *ad hoc* sviluppate per la tutela della sicurezza pubblica.



D-Link®

FOR BUSINESS



Wireless



Videosorveglianza



Reti LAN

NEL CUORE DI OGNI PROGETTO

 www.dlink.com
 it-sales@dlink.com

30 YEARS
of Innovation

D-Link®
FOR BUSINESS

La Redazione

Storage, networking, chipset, camere: cosa è bene sapere

Negli ultimi vent'anni le reti e la loro complessità sono cambiate radicalmente, portando innovazioni soprattutto nel mondo della videosorveglianza. La prima tecnologia ad essersi evoluta è quella degli apparati di rete, ma ne hanno beneficiato notevolmente anche telecamere e apparati di videoregistrazione, grazie all'aumento della qualità e della fruibilità delle immagini registrate e all'impiego di hard disk ad altissima capacità: ecco quindi che videoregistratori e telecamere IP hanno cominciato a conoscere una concreta applicazione e si sono potuti mettere in risalto i loro molteplici punti di forza.

Quando si parla di videosorveglianza IP, sono quattro le macro aree sulle quali ci si deve soffermare: *Storage* ovvero archiviazione; *Networking* ovvero comunicazione; *Chipset DSP* (digital signal processor) ovvero analisi e compressione delle immagini; *Camera* cioè la vera e propria telecamera, per catturare e acquisire immagini.

TELECAMERE

Le telecamere solitamente si distinguono in due tipologie: quelle che integrano sensore di immagine CCD (Charge-Coupled Device) e quelle che invece integrano sensore di immagine CMOS (Complementary Metal-Oxide-Semiconductor). Infatti è il sensore di immagine che fa la differenza ed è una delle componenti più importanti da tenere in conto. I sensori CMOS e CCD si misurano entrambi in pollici e la misura standard oggi utilizzata maggiormente è 1/3" con risoluzione 2MP. Ma bisogna abituarsi a pen-

sare che la dimensione del sensore conta più del numero di megapixel supportati perché i megapixel non servono a nulla se il sensore è piccolo. Quasi nessuno ha realmente idea di quali siano le dimensioni effettive di un sensore, ma si è ormai fortunatamente compreso che non sempre un sensore con tanti megapixel significa qualità più elevata. Il sensore infatti è composto da milioni di pixel ed ogni pixel è composto da una microlente e da un elemento elettrico che trasforma la luce in segnale digitale: più grande è il pixel, più grande è la luce che cattura, con una resa quindi più accurata e con un rumore minore. Il primo punto di forza della più evoluta videosorveglianza IP sta nella *qualità* dei pixel: aumentare progressivamente la quantità dei pixel, ovvero la risoluzione di sensori e telecamere, non è infatti l'aspetto più importante. E' la qualità delle immagini registrate ad assumere una rilevanza sempre maggiore.

SENSORI CMOS

I sensori CMOS in particolare si suddividono in due tipologie: FSI (front side illumination) ovvero con illuminazione frontale, e BSI (back side illumination) - ovvero con illuminazione posteriore. A parità di condizioni di utilizzo, il sensore BSI risulta disporre del 50% di sensibilità in più: ciò è dovuto alla miglior tecnologia che riesce a catturare tutti i raggi luminosi circostanti. Studi dimostrano che, a parità di condizioni di bassa luminosità, il sensore BSI da 1/2.8" (messo a confronto con sensore 1/1.8") risulta molto più luminoso, nonostante sia di dimensioni inferiori - cosa che porterebbe a rilevare, in qualsiasi altra situazione, una maggiore oscurità, proprio perché le ridotte dimensioni catturano meno raggi di luce. La maggior luminosità è quindi il secondo punto di forza della tecnologia IP sempre più evoluta.

TECNOLOGIA DSP

Ultimo punto di forza che si vuole mettere in evidenza risiede nella fase di trasmissione in rete e dunque nella



Sinora abbiamo parlato poco di compressione. All'orizzonte si sta stagliando in materia un nuovo standard tecnologico: il codec H265. In che modo cambierà il mercato?

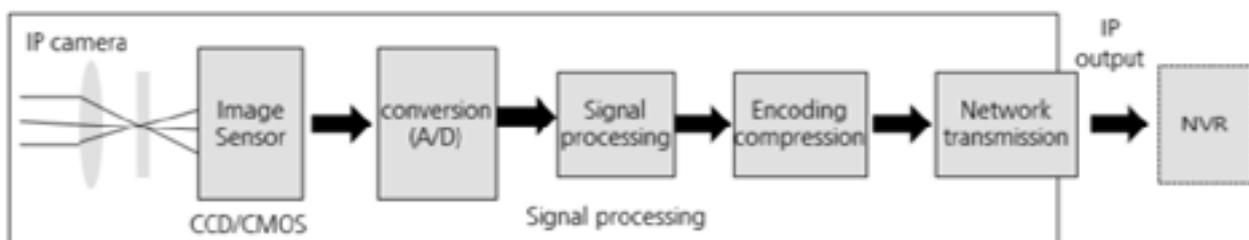
Risponde Fulvio Cartasegna, Presidente di Deatronic

Con il continuo aumentare della risoluzione video (ormai siamo prossimi all'avvento nel quotidiano del 4K) aumentano anche le necessità strutturali per supportare la sicurezza: spazio di archiviazione e soprattutto connettività adeguate. Qui entra in gioco il nuovo standard di compressione video H.265 che consente un importante risparmio di banda. Sfruttando inoltre il protocollo HEVC (high efficiency video coding), permette che le immagini siano gestite semplicemente e soprattutto oltre la risoluzione 4K. Nonostante la riduzione della quantità di banda sulle reti, gli apparati di videosorveglianza beneficiano dell'H265 poiché archiviano dati in modo più semplice e più affidabile. Potendo trasferire infatti pacchetti di dati più leggeri, si possono trasferire immagini qualitativamente superiori e diminuisce altresì la possibilità di perdere dati e quindi informazioni importanti. In conclusione, accresciamo di un nuovo step la nostra sicurezza.

www.deatronic.com

tecnologia DSP. Una volta catturata un'ottima immagine grazie alla qualità dei pixel e alla luminosità della tecnologia BSI, la nuova compressione video H265 sfoggia i suoi molteplici benefici:

1. Risparmio di spazio di archiviazione (riduzione dal 50 al 75% rispetto alla compressione video H264);
2. Risparmio di impiego di banda del networking della comunicazione;
3. migliore qualità delle immagini grazie alla sensibile riduzione (anzi, quasi eliminazione) dell'effetto mosaico. L'effetto mosaico, unitamente alla limitazione di banda, viene ulteriormente ridotto con accorgimenti software (e.g. Huawei SEC unique technology). In una situazione con circa un 20% di perdita di pacchetti, questa tecnologia annulla del tutto l'effetto mosaico.



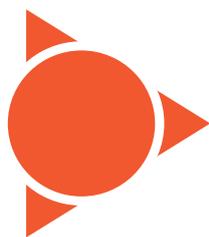
Switch industriale per videosorveglianza



UTEPO™

- Modalità TVCC tramite interruttore
- Pulsante reset PoE
- Doppio Uplink Gigabit SFP/RJ45
- Extended PoE+ fino a 250m
- Protezione sovratensioni fino a 6KV
- Doppio ingresso di alimentazione
- Range temperatura esteso da -40°C a +75°C

Distributore ufficiale per l'Italia



advanced innovations

Your perfect partner

info@ad-in.net - www.adin.it

**SORVEGLIA
E PROTEGGE**

SISTEMI SPECIALI DI SICUREZZA.



INSTALLAZIONE E ASSISTENZA H24 · GESTIONE ALLARMI · PRONTO INTERVENTO

 **SECURITYTRUST.IT**

Security Trust



Giovanni Villarosa^(*)

Controllo perimetrale degli accessi: sicurezza *trasversale*

Nello scorso numero abbiamo affrontato il tema della *security perimetrale*, intesa come protezione fisica dei perimetri. Affronteremo adesso il controllo perimetrale *degli accessi*, una tipologia di sicurezza con caratteristiche spiccatamente *trasversali* (la sicurezza ricompresa nei perimetri della *security e safety* è sempre più una componente fondamentale nella società moderna), perché volta a proteggere i perimetri e le persone da accessi indesiderati, a gestire i varchi in caso di emergenza, ad assicurare le aree di pertinenza, nonché ad archiviare e processare, anche amministrativamente, i dati personali degli utenti.

^(*) Laureato in Scienze dell'Intelligence e della Sicurezza, esperto di Sicurezza Fisica per Infrastrutture, Chief Security Officer e Data Protection Officer, Giovanni Villarosa è anche Vice Presidente di SECURTEC (Associazione culturale, composta da security manager certificati, che si occupa di tematiche legate al mondo - logica e fisica - per la protezione di infrastrutture complesse e critiche).

In un mondo sempre più a portata di mouse, dove la possibilità di operare in un sistema di sicurezza integrata globale rientra nelle attività ordinarie della nostra quotidianità, l'assicurazione circa il perfetto funzionamento degli impianti, delle tecnologie e dei vettori connettivi, ricopre un ruolo prioritario. In un mondo in cui l'apparato di sicurezza è poi spesso un dispositivo digitale collegato ad una rete, sia essa fisica o wireless, ed in stretta connessione a internet, sono essenziali nuove competenze (installatori, progettisti, operatori, know how) e nuove soluzioni (tecnologiche, hardware e software) per proteggere adeguatamente l'intera filiera del processo. Il tutto ponendo sempre una particolare attenzione all'*impatto privacy* che le tecnologie di identificazione (lettori biometrici, lettori targhe, etc) possono esercitare sui dati personali, registrati e trattati.

IOT E INTEGRAZIONE

L'integrazione tra *ICT e Security*, in campi diversi, è ormai cosa fatta: dalla registrazione dei dati di sicurezza su supporti (Hdd, Ssd) alla protezione delle reti, dai cablaggi sicuri a memorie in grado di reagire ai tentativi di furto di dati, fino a software e hardware altamente performanti per sistemi integrati in difesa dei patrimoni aziendali. Un'interessante quanto futuristica area verticale della security sarà quella dedicata allo *IoT*: l'intelligenza e la sicurezza delle *cose*, nella *cd quarta rivoluzione industriale*, diventa decisamente smart. Diversi device dialogano tra loro, interconnessi a tutto e tutti: dalle infrastrutture complesse, al mondo industriale, fino al singolo; insomma tutto è ormai inevitabilmente interfacciato, interconnesso, interagente rispetto a un dispositivo logico, ad una rete, ad un nodo web. In questo contesto il tema della sicurezza degli accessi, *in toto*, diventa prioritario: non solo la sicurezza fisica e logica, anche qui, converge nuovamente (come abbiamo già più volte sottolineato nei precedenti articoli), ma la security dedicata al controllo dei varchi diventa l'elemento cardine per garantire protezione, salvaguardia, monitoraggio costante, ma anche efficienza e miglioramento delle performance aziendali.

CONTROLLO ACCESSI

Il controllo degli accessi rappresenta oggi, e meglio di altri sistemi, la riuscita integrazione hardware e software tra i diversi sistemi perimetrali: il governo e l'applicazione sul campo di quanto esposto sinora, nel mondo della security



(logica e fisica) e della safety, risultano fondamentali per regolare gli accessi, proteggere la privacy, prevenire i rischi, salvaguardare l'incolumità personale. Tecnologia Rfid (tag attivi e passivi), lettori biometrici (impronta, iride, geometria mani e volto), badge magnetici o semplici tastiere keycode: tutte queste tecnologie, prese singolarmente o integrate tra loro, rappresentano un segmento indispensabile del processo. Ma non è tutto. Pensiamo a quali ulteriori impieghi si prestano tali tecnologie, come ad esempio in una struttura ospedaliera. Si decide già dalla fase progettuale (*security by design*) chi può avere accesso a determinate aree: UTIC, sale operatorie, TAC, RMN, centri trasfusionali, reparti sterili, reparti infettivi, farmacia ospedaliera, cavedi tecnologici, centrale gas medicali, impianti tecnologici, CUP, CED, ufficio referti e cartelle sanitarie (dati sensibili). Con queste tecnologie possiamo tracciare particolari farmaci, tenere sotto controllo clinico i pazienti (braccialetto Rfid), tracciare la sterilizzazione delle attrezzature e degli indumenti utilizzati nelle sale operatorie, e - non ultimo - tracciare i rifiuti ospedalieri classificati, poiché tali sono i residui della medicina nucleare, tanto per citare altri possibili esempi. In questo caso applicativo i perimetri della sicurezza si elevano a tre: *security, safety, emergency*.

TAV DEL SAN GOTTARDO

Altro esempio nei tre ambiti della sicurezza sopracitati: il progetto europeo per la TAV del San Gottardo, un tratto ferroviario sotterraneo nord-sud sotto le Alpi svizzere (il più lungo al mondo), suddiviso in tunnel scavati al di sotto di

quelli attuali. Per la realizzazione e la protezione integrale del cantiere (security, safety, emergency), è stato scelto un progetto (anche qui by design) di controllo accessi integrato decisamente interessante, che prevedeva tutta una serie di misure, quali il presidio dei portali d'accesso alle gallerie mediante stazioni di controllo Rfid per rilevare il transito degli operatori, ma soprattutto, la loro direzione. In questo caso il sistema accessi, ad esempio, genera un allarme safety (direttive europee 92/91/CEE e 92/104/CEE) nel caso venga superata la permanenza nelle gallerie superiore alle 8 ore, trasmettendo l'alert alla sala controllo che, *real time*, monitorizza l'elenco dei nominativi e il numero effettivo delle presenze umane all'interno del tunnel. Con lo stesso principio vengono puntualmente monitorati tutti i mezzi d'opera presenti nelle aree di cantiere, la loro operatività e direzione, la gestione degli automatismi di apertura e chiusura dei varchi d'accesso ai mezzi di lavoro (gestione semaforica), o semplicemente l'azionamento delle procedure di emergenza (attivazione della ventilazione ausiliaria). I tag propri di ogni mezzo rappresentano, peraltro, una vera rivoluzione a livello di security: infatti il software di gestione può creare profili spazio-temporali del mezzo, che – una volta violati – generano un allarme di tipo *criminogeno*.

I BENEFICI

L'uso di sistemi evoluti di controllo degli accessi nei grandi cantieri porterà senza dubbio grandi benefici sull'intera filiera produttiva: potendo infatti tracciare in modo certo oggetti, macchinari e persone, e potendo monitorare i parametri fisici ed ambientali (umidità, temperatura), si potranno prevenire infortuni e scongiurare eventi pericolosi all'interno delle gallerie. Questo nuovo approccio sta

trasformando inevitabilmente la strategia di gestione della sicurezza nel suo insieme, perché sempre di più si assottigliano le divisioni tra security e safety, tra sicurezza fisica e quella logica, tra il mondo reale e quello digitale. Quello che non cambierà - bensì si rafforzerà - sarà la centralità, a livello di continuità della gestione della sicurezza intesa come tessuto connettivo, tra le diverse aree di *business*. I presidi e le difese del patrimonio aziendale (umano, tangibile e intangibile), nonché la tutela della continuità operativa, richiedono infatti investimenti e innovazione sempre più stringenti, per rispondere a minacce a loro volta sempre più evolute.

CYBER PHYSICAL SECURITY

La *cyber physical security*, nascente dottrina di settore, rappresenta oggi la novità che unisce insieme tutti gli aspetti della sicurezza in modo resiliente e proattivo, e va ben oltre la prevenzione. Con questo nuovo approccio la sicurezza diviene un'attività ancora più *trasversale*, coinvolgendo strutture differenti a livelli differenti. E' proprio la pervasività della tecnologia che suggerisce un approccio integrato, secondo una gestione per processi che coinvolga in maniera *orizzontale* le strutture interessate, ormai saldamente vincolate alle tecnologie dei mercati *verticali*: sicurezza logica, business continuità, sicurezza fisica, business intelligence, etc. E questo significa, principalmente: progettare tutti gli asset e i servizi - a partire, per esempio, dalle applicazioni - affinché siano intrinsecamente sicure, per una sicurezza *by design* prevista non solo nelle nuove organizzazioni, ma possibilmente attuabile come approccio evolutivo per quelle esistenti.



Tiandy

5
GARANZIA
ANNI

SOSTITUZIONE
36
MESI



#CABLEFREE



Tiandy Italia

sales@tiandy.it
www.tiandy.it



TRY IT NOW!

<http://bit.ly/CABLEFREE>

LESS CABLES, MORE SIMPLICITY!

La Redazione

Il computer estrae a sorte i dipendenti da perquisire

Perquisire i dipendenti all'uscita dai luoghi di lavoro per tutelare il patrimonio aziendale si può. Lo consente lo Statuto dei lavoratori, lo confermano diverse sentenze. Ma a condizione che il controllo sia imparziale e a campione. Le persone devono essere sorteggiate in modo automatico e casuale, l'ispezione corporale deve avvenire salvaguardando la dignità e la riservatezza del lavoratore. Ad estrarre la pallina dall'urna ci pensano appositi "sorteggiatori" elettronici installati in corrispondenza delle vie di uscita. La funzione è ora anche integrata nei Controller per accessi più evoluti.

Tutte le imprese hanno il diritto di tutelare il proprio patrimonio adottando le misure più efficaci ed impiegando le soluzioni tecnologiche più appropriate. Vi sono aziende, tuttavia, che per il tipo di attività che svolgono e per le materie prime che trattano, più di altre hanno l'esigenza di prevenire e scoprire i furti da parte dei dipendenti. Si pensi, ad esempio, alle imprese che lavorano metalli preziosi (oro, argento, platino), producono gioielli o componenti elettronici di valore. Una delle soluzioni più semplici ed efficaci è l'ispezione dei lavoratori e dei "bagagli" al seguito. La perquisizione è consentita, ma a determinate condizioni indicate nello Statuto dei lavoratori (L. 300/1970) e confermate dalle numerose sentenze che nel corso dei decenni si sono succedute. In particolare, dice la legge, l'ispezione corporale deve avvenire all'uscita dai luoghi di lavoro, a campione, in modo automatico e casuale, salvaguardando la dignità e la riservatezza delle persone. Il controllo, oltre che sugli individui, è attuabile anche sui veicoli. L'ispezione sulle persone ha lo scopo di individuare la presenza di eventuali prodotti o documenti di proprietà dell'azienda, portati addosso o contenuti in borsette e borselli, valigette 24 ore, borse di plastica e di carta, scatole, contenitori e altri tipi di bagaglio a mano. Negli automezzi, invece, il controllo viene eseguito essenzialmente nell'abitacolo e nel bagagliaio, anche in questo caso alla ricerca di materiali, attrezzature e strumenti non preventivamente autorizzati ad abbandonare l'edificio.

IL SORTEGGIATORE

Da vari decenni, a selezionare in modo imparziale il dipendente o il veicolo da perquisire ci pensa il cosiddetto "sorteggiatore", un dispositivo elettronico installato in corrispondenza delle vie di uscita. L'impiegato preme



COSA DICE LA LEGGE

Le visite personali di controllo sui dipendenti sono regolate dall'articolo 6 della legge 300/70 (Statuto dei lavoratori). Tali visite, dice la legge, sono vietate "fuorché nei casi in cui siano indispensabili ai fini della tutela del patrimonio aziendale, in relazione alla qualità degli strumenti di lavoro o delle materie prime o dei prodotti". Lo stesso articolo, poi, stabilisce che le perquisizioni possono avvenire "soltanto a condizione che siano eseguite all'uscita dei luoghi di lavoro, che siano salvaguardate la dignità e la riservatezza del lavoratore". Non solo. La condizione *sine qua* non è che avvengano attraverso l'impiego di sistemi "di selezione automatica riferiti alla collettività o a gruppi di lavoratori".

Le modalità di controllo "devono essere concordate dal datore di lavoro con le rappresentanze sindacali aziendali oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro".

Dal momento in cui è entrato in vigore lo Statuto dei lavoratori, numerose sono state le sentenze, raccomandazioni e chiarimenti in merito all'articolo 6 emanate da tribunali, preture, Cassazione civile, Ministero del lavoro ecc. Come sempre, le interpretazioni dottrinarie e giurisprudenziali in Italia si sprecano. L'ultima nota è dell'8 novembre scorso. Sintetizzando: le visite corporali sono ammesse se finalizzate alla tutela del patrimonio aziendale; devono avvenire tramite sorteggio, all'uscita del luogo di lavoro e da parte di guardie giurate; le procedure devono essere concordate con le rappresentanze sindacali o, in mancanza, con l'Ispettorato del lavoro; in ogni caso deve essere salvaguardata la dignità del lavoratore. Per procedere all'ispezione occorre ottenere il consenso da parte dell'interessato. Un eventuale rifiuto del lavoratore, tuttavia, può costituire una violazione degli obblighi previsti dal contratto di lavoro ed essere passibile di sanzioni disciplinari.

un pulsante sotto lo sguardo attento della vigilanza. Se sorteggiato (accensione di una luce rossa eventualmente accompagnata da un segnale acustico), viene invitato ad accomodarsi in una saletta adiacente alla guardiana





MA IL TOP RESTA IL METAL DETECTOR

La misura di sicurezza più efficace per evitare i furti di metalli preziosi, gioielli, componenti elettronici e altri materiali di valore, è lo screening di tutti i dipendenti al momento in cui abbandonano l'azienda. La soluzione ottimale (sebbene costosa) resta l'impiego di metal detector speciali e di elevata sensibilità, in grado di identificare le persone in transito, compiere un'ispezione rapida e accurata del loro corpo, confrontare il risultato con il profilo individuale contenuto nel database (al fine di ignorare gli oggetti metallici personali e inamovibili quali protesi, fedi, piercing ecc.), richiamare l'attenzione della vigilanza in presenza di piccoli oggetti metallici.

Il dipendente, dopo essere stato "registrato" una tantum, si avvicina al metal detector, presenta il proprio badge e transita attraverso il tunnel. Il sistema "fotografa" il corpo del soggetto, intercetta gli oggetti metallici, scarta quelli personali, lascia passare senza attivare l'allarme o, al contrario, richiama l'attenzione della vigilanza indicando l'allocatione degli elementi rilevati.

o alla reception per essere sottoposto, in modo discreto, ad un'ispezione corporale. In presenza di tornelli e unità elettroniche che identificano in modo automatico i soggetti, l'azione manuale è sostituita dalla lettura del badge ovvero dal comando di apertura della barriera

fisica stessa. Analogamente avviene per gli automezzi prima che si apprestino ad attraversare il varco veicolare (sbarra, cancello ecc.) e lasciare l'area aziendale. Il sorteggiatore è ancora oggi largamente usato. Alcuni Controller per accessi particolarmente evoluti, tuttavia, integrano la funzione del controllo imparziale senza la necessità di hardware esterno, in modo conforme alla legislazione vigente e con un sensibile risparmio di denaro rispetto alla soluzione tradizionale.

IL CONTROLLO IMPARZIALE

Gli elementi da considerare nel controllo imparziale sono essenzialmente quattro: la *casualità* del sorteggio, la *frequenza* di sorteggio, la *segnalazione* da attivare e la *gestione del varco* al momento in cui un utente viene estratto a sorte. La scelta della persona da perquisire o del veicolo da controllare deve avvenire in modo automatico e casuale. L'adozione di un buon algoritmo è in grado di garantire un ottimo livello di casualità. La frequenza di sorteggio dipende dalle esigenze aziendali. Si può andare da un controllo molto blando ad uno serrato. La percentuale è un parametro programmabile; indicativamente è compresa tra l'1% e il 5%. Impostando la percentuale dell'1% significa che l'imparziale deve intervenire ogni cento persone (o veicoli) che transitano. Al momento in cui il soggetto è stato sorteggiato, il si-



L'ISPEZIONE IN TRE MOSSE

FIG. 1 - I dipendenti che si apprestano a lasciare il luogo di lavoro si portano in corrispondenza dell'uscita dove sono installati i varchi, di solito in grado di garantire il transito di una persona alla volta: tornelli, bussole ecc. © a&s Italy All rights reserved

FIG. 2 - Nella direzione di uscita, un "sorteggiatore" elettronico (o lo stesso Controller che gestisce gli accessi) estrae a sorte i lavoratori secondo una percentuale preimpostata. A sorteggio avvenuto, viene attivata una segnalazione luminosa oppure ottico/acustica per richiamare l'attenzione del personale di guardia. © a&s Italy All rights reserved

FIG. 3 - Il dipendente sorteggiato è tenuto a recarsi in un'apposita saletta per essere sottoposto a perquisizione da parte di una guardia giurata. La visita corporale, dice la legge, deve avvenire salvaguardando la dignità e la riservatezza del lavoratore. © a&s Italy All rights reserved

stema deve richiamare l'attenzione della vigilanza. Una guardia giurata (maschio o femmina, in base al sesso dell'estratto a sorte) invita il dipendente ad accomodarsi in un locale attiguo e procede all'ispezione. A segnalare l'avvenuto sorteggio è un dispositivo luminoso oppure ottico/acustico, integrato nello stesso sorteggiatore oppure separato e installato nelle vicinanze. Il sistema deve, quindi, disporre di un output (tipicamente un contatto in scambio di un relè), permettere di programmare la durata del segnale luminoso ed eventualmente gestire la tacitazione in anticipo del dispositivo ottico/acustico stesso da parte della guardia. Nella maggior parte dei casi, il controllo in uscita avviene in corrispondenza di una o più "barriere fisiche" che consentono il passaggio di una persona alla volta, come un tornello a tripode, una bussola, un varco ad ante motorizzate e simili. Il transito in uscita del dipendente attraverso il varco, inoltre, spesso è un evento che coincide con il termine del periodo di lavoro e quindi con la registrazione dell'orario di uscita, dato utile per il successivo calcolo delle ore lavorate. Nel caso in cui un lavoratore viene estratto a sorte, dunque, il sorteggiatore deve anche gestire il transito in modo appropriato. La gestione, oltre che dalle caratteristiche tecniche della barriera fisica, dipende dall'ubicazione della saletta di ispezione rispetto al tornello o alla batteria di tornelli. Se il locale si trova prima della barriera di uscita, il sorteggiatore non deve sbloccare il varco. È questa la condizione più comune. Il dipendente si reca nella saletta e, al termine dell'ispezione, ripresenta il badge per uscire. Se, invece, la



I moderni Controller per accessi sono in grado di gestire anche il "controllo imparziale" ossia di sorteggiare a campione i lavoratori da sottoporre ad ispezione corporale (o gli autoveicoli) al momento in cui abbandonano l'azienda (Foto: Courtesy Elex).

saletta è disposta a valle del tornello, a riconoscimento avvenuto e utente sorteggiato, è necessario sbloccare la via di uscita per consentire al dipendente di raggiungere il locale. In entrambe le situazioni, il sistema deve controllare il transito attraverso il varco tenendo conto delle modalità di funzionamento dello stesso e dei valori preimpostati quali la durata del comando di sblocco, il tempo massimo di attesa apertura e richiusura (avvenuta rotazione del tornello) eccetera. Nelle soluzioni più sofisticate, tutti gli eventi relativi all'intervento del controllo imparziale sono rilevati e memorizzati, utili per eventuali verifiche a posteriori.



TABELLA 1

Funzione	Descrizione	Parametri
Casualità	Algoritmo di sorteggio	
Frequenza	Percentuale di sorteggio	1-99% (tip. 1-5%)
Segnalazione	Luminosa oppure ottico/acustica	Durata Reset anticipato
Comando	Blocco/sblocco del varco a sorteggio avvenuto	Blocco/sblocco Durata Altri controlli

Un sorteggiatore d'ispezione corporale deve essere imparziale, segnalare in modo univoco alla vigilanza il soggetto sorteggiato, gestire il transito attraverso il varco in base al suo modo di funzionamento e ad altre esigenze di controllo. © a&s Italy All rights reserved

Soluzioni Audio per Diffusione Sonora

INTERFONIA E DIFFUSIONE SONORA **OVER IP**



Peer To Peer



Power over Ethernet



Voice over IP



No Server

UNV : La Videosorveglianza IP 3.0



H.265

Le telecamere Unview supportano H.265. E le telecamere H.265 supportano le funzioni smart.



4K

Le telecamere della serie 4K Unview comprendono Dome II, Bullet II, Speed Dome e Telecamere box.



U-code

U-code è una tecnologia di codifica migliorata H.265/H.265. U-code riesce a ridurre fino all'80%-95% lo spazio su disco.



Smart

Unview ha 4 funzioni smart che includono rilevamento volti, intrusione, linea cross, e conta persone.



120dB WDR

La funzione WDR produce immagini chiare e di qualità in condizioni prevenendo zone buie o troppo luminose. I prodotti Unview supportano il 120dB WDR.



Optical defog

Unview utilizza la tecnologia optical defog per visualizzare in modo perfetto tutti i dettagli dell'immagine anche in ambienti nebbiosi.



Surge protection

Il dispositivo può raggiungere la capacità di protezione da sovratensioni di 6kV senza alcuna protezione esterna. Le sovratensioni 10 metri dal cavo causano una tensione minore di 40V. Con 6kV noi riesce a soddisfare la protezione giornaliera.



IP67

IP67 indica che il prodotto è a prova di polvere e continua a funzionare anche sotto 1 metro d'acqua per 1 ora. Le telecamere Unview sono impermeabili.



Wide Temperature range

Le telecamere Unview possono funzionare in un intervallo di -43°C - 70°C, adattandosi alle più dure condizioni ambientali.



Onvif

Con la conformità Onvif sono supportate le telecamere IP di terze parti.



H.265

Le telecamere 2MP e 4MP UNV supportano H.265. E le telecamere H.265 supportano le smart function.



Plug And Play

Supporta il Plug&Play per la ricerca e autoconfigurazione automatica delle telecamere.



Long Range PoE

Con gli NVR e telecamere UNV la distanza di trasmissione PoE riesce a raggiungere i 300m con cavo Cat5E o Cat6.



EZ Cloud

Il servizio video EZCloud offre una soluzione mobile per la visualizzazione e gestione remota delle telecamere IP.



Smart Search

La ricerca normale impiega molto tempo per ottenere risultati. Con la ricerca smart è possibile specificare un'area di interesse per avere in pochi secondi il risultato atteso.



VCA

E' una funzione di analisi video intelligente che prevede: rilevamento volti e intrusioni, linea cross e conta persone.



Higher Security

Viene adottato un differente livello di sicurezza tra LAN e WAN. La LAN permette password semplici, la WAN solo password complesse.



ANR

Se viene interrotto il collegamento tra telecamera ed NVR, le telecamere memorizzano le registrazioni su scheda SD. Alla riconnessione, saranno inviate le registrazioni all'NVR.



La Redazione

Integrazione di sistemi e tecnologia IP: due driver in costante evoluzione

Da diversi anni il mercato tecnologico legato al mondo della sicurezza si sta spostando sempre di più nella direzione dell'integrazione di sistemi. Gli impianti di allarme, TVCC, controllo accessi, lettura targhe e controllo varchi e domotica non vengono più intesi come fini a se stessi, ma sempre di più si richiede la possibilità di integrare tra loro tutti gli impianti in campo. Ovviamente anche lo sviluppo dei produttori è influenzato da questa richiesta: si investe quindi sempre più, in termini di risorse, nel mondo IP perché, grazie all'esistenza di svariati standard (nel caso specifico della TVCC Onvif/RTSP/SIP/VOIP), si riesce ad integrare ad esempio un impianto di TVCC con la Videocitofonia, l'antintrusione, il controllo accessi e la domotica.

Anche per questa ragione lo sviluppo tecnologico mirato sull'HD su coassiale sarà sempre più ridotto - viste tutte le limitazioni, lato software ma anche lato hardware, che presenta questa tecnologia. Questo discorso vale nel caso di impianto verticale o dove, per esigenze strutturali, non è possibile utilizzare il classico cablaggio, ad esempio gli impianti strutturati in ambito urbano con distanze superiori allo standard. La trasmissione del segnale digitale, molto più elastica, ci permette di utilizzare diversi strumenti: Switch, ponti radio, fibra e rame. Non abbiamo dunque più la necessità di dover portare tutti i cavi al sistema di archiviazione, ma possiamo portare solo ed esclusivamente un cavo di rete, collegato poi in cascata a switch e ponti radio, tanto per fare un esempio.

COMPRESSIONE

Un altro fattore molto importante è rappresentato dalle nuove funzionalità e dai nuovi protocolli di compressione video (Analisi video, H265, Starlight, OCR, ANR). Nel caso specifico dell'H265, questo protocollo di compressione garantisce una minor occupazione di banda ed un risparmio importante in termini di archiviazione nello storage. Nel caso della video analisi, invece, si possono diminuire radicalmente i falsi allarmi oppure prevenire determinati eventi, come ad esempio la funzione di oggetto abbandonato o rimosso (molto sfruttato in ambienti sensibili quali banche, aeroporti, stazioni, stadi etc). Altre funzioni si possono invece legare ad analisi di mercato, come nel caso della funzione Heat Map o



Se integrazione è la parola chiave di un'offerta di sicurezza che aggiunge valore, e che quindi garantisce redditività in un mercato non di rado appiattito su semplici commodities, IP è il concetto chiave sul piano tecnologico. Perché?

Risponde Maurizio Renato Coates, Technical Sales Melchioni

La diffusione di standard nel mondo IP permette di integrare agevolmente impianti di diverse tipologie e la trasmissione del segnale digitale permette di utilizzare gli strumenti più adatti al caso (switch, ponti radio, fibra e rame). Per non parlare delle funzioni evolute, e sempre più richieste, che solo l'IP consente di ottenere. Le funzioni di integrazione sarebbero infatti impensabili con una tecnologia "analogica", in quanto l'integrazione di tutti i sistemi è strettamente vincolata alla tecnologia di trasmissione dati. Per questo il mercato si sta concentrando sull'individuazione di un prodotto versatile che comprenda sempre più funzioni nello stesso articolo. Di conseguenza i produttori sono alla continua ricerca di un prodotto sempre più smart che sia in grado di integrare tutte le funzioni sfruttando una sola macchina. (*)

www.melchioni.it
www.milesight.com

mapa di calore, che indica sull'immagine video le aree più movimentate e con più sosta. Un esempio pratico di quest'applicazione potrebbe essere un supermercato che riesce, tramite le analisi statistiche dell'analitica video, a stabilire quali corsie sono più visitate e i punti nei quali la clientela si sofferma maggiormente.



(*) Tutto il lineup prodotti di Milesight, che Eurotek distribuisce sul mercato italiano, supporta svariate funzioni: H.265-Starlight-WDR140db, SIP-VOIP.
www.milesight.com

LUCE

Un'altra funzione molto interessante, soprattutto nel caso del controllo cittadino/urbano, è la funzione Starlight, che sfrutta un Chipset molto più sensibile alla luce e permette di visualizzare un'immagine dettagliata, addirittura a colori, anche in condizioni ambientali quasi totalmente prive di luce artificiale. Chiaramente questa funzionalità viene utilizzata nel caso in cui si abbia la necessità di controllare aree vaste con scarsa visibilità e solitamente all'esterno.

VARCHI E TRAFFICO

Capitolo sempre più attuale ed interessante è il controllo varchi e monitoraggio del traffico. Grazie a soluzioni software che vengono integrate con i database del Ministero dei Trasporti e il Ministero degli Interni, è possibile controllare in tempo reale se il veicolo che si sta monitorando coincide con un'auto rubata o sospetta, oppure si possono ottenere dati relativi ai veicoli non assicurati o non revisionati. Grazie all'utilizzo di White e Black list è invece possibile, nel caso di controllo varchi, azionare automaticamente la sbarra o il cancello

se la targa ripresa è presente nel database delle targhe autorizzate (White list). Nel caso invece la targa sia presente nel database dei veicoli non autorizzati (Black list), il sistema può avvisare l'operatore del transito del veicolo tramite un Pop-up o un SMS. Un'altra applicazione, molto utile anche nel caso del controllo cittadino, è quella che permette di immagazzinare le informazioni su entrata ed uscita di ogni varco per capire e monitorare una zona ben precisa ed avere sempre sotto mano i dati di ogni veicolo transitato, comprensivi di giorno e orario. Oppure, in casi legati ad attività commerciali (nel caso di grossi centri commerciali, ad esempio), è possibile stabilire da quale paese si verifichi la maggiore affluenza, e questo può avere diversi influssi in termini di marketing (scelta degli articoli da vendere, cartellonistica in più lingue, accortezze legate a religione/peculiarità etniche). Infine l'innovativa funzione ANR permette di salvare i dati nella SD card interna alla telecamera in mancanza di collegamento dati verso lo storage; quando il collegamento tornerà ad essere attivo, la telecamera invierà le informazioni perse in registrazione. Un ulteriore step verso sistemi di sicurezza più efficienti ed al passo con le attuali esigenze di mercato.





Always-on



Supervisione



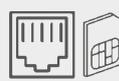
Copertura globale



Contact ID



Video verifica



Ethernet GPRS



Costi ridotti



Eventi crittografati

CENTRALE ANTINTRUSIONE



GPRS/SMS

CALLISTO

Centrale ibrida, 7 zone filari
9 zone via radio, GPRS integrato

MOBILE APP

Notifiche Push  Italiano



CONTROLLO RONDE



GPRS/SMS/VOCE

ACTIVE TRACK

Uomo a terra, Panico, RFID, GPS

PERIFERICHE



GPRS/SMS

IKLX20G3C

3 ingressi, 3 uscite, Contact ID



ETHERNET

IKEX20

4 ingressi, 2 uscite, Contact ID



ETHERNET/GPRS/SMS

IKEPX400

Multivettore, 9 ingressi, 3 uscite,
Contact ID



GPRS/SMS

IKLX2NB

4 ingressi, 1 uscita, Contact ID
Disponibile anche con ricevitore
radio integrato.

Barbara Pandolfino^(*)

Come e dove installare telecamere nei condomini?

Il costante bisogno di sicurezza e l'incessante necessità di sentirsi al sicuro dentro le proprie mura domestiche ci conduce ad approfondire un argomento già affrontato qualche mese fa. La videosorveglianza all'interno dei condomini infatti non deve – e non può- essere considerata solo dal punto di vista del mero iter procedurale di approvazione (nella scorsa trattazione ci siamo concentrati sul portato del nuovo art. 1122 c.c. introdotto dalla Riforma del Condominio Legge 220/2012), ma deve necessariamente essere valutata nelle sue accezioni più pratiche. Come installare le telecamere di videosorveglianza negli spazi comuni? Dove posizionarle?

^(*) Av. Barbara Pandolfino, Master in Criminologia e Politica Criminale Internazionale c/o ente ONU UNICRI, Spec. Scuola di Alta Qualificazione in Psicologia Interpersonale Investigativa Criminale e Forense, esperto di Privacy e Diritto delle Nuove Tecnologie; Ufficio Legale FENIVA SRL www.feniva.it - legale@feniva.it

A queste basilari domande ha risposto la più recente giurisprudenza con alcune significative sentenze. Per semplicità espositiva ci proponiamo di fornire gli aspetti più salienti degli interventi che interessano in questa nostra analisi. Con la sentenza n. 12139 del 2015, la Corte di Cassazione sezione VI ha replicato alla nostra prima domanda: come va installata una telecamera in un condominio. Per gli Ermellini la telecamera dovrà essere posizionata in modo da non riprendere (anche solo in parte) la proprietà di fronte o vicina. Se tale precetto non viene rispettato, si concretizza la violazione del diritto alla riservatezza del nostro vicino. Inoltre non rileva, nella fattispecie in esame, che la telecamera non funzioni perfettamente o non sia collegata ad uno strumento di registrazione.

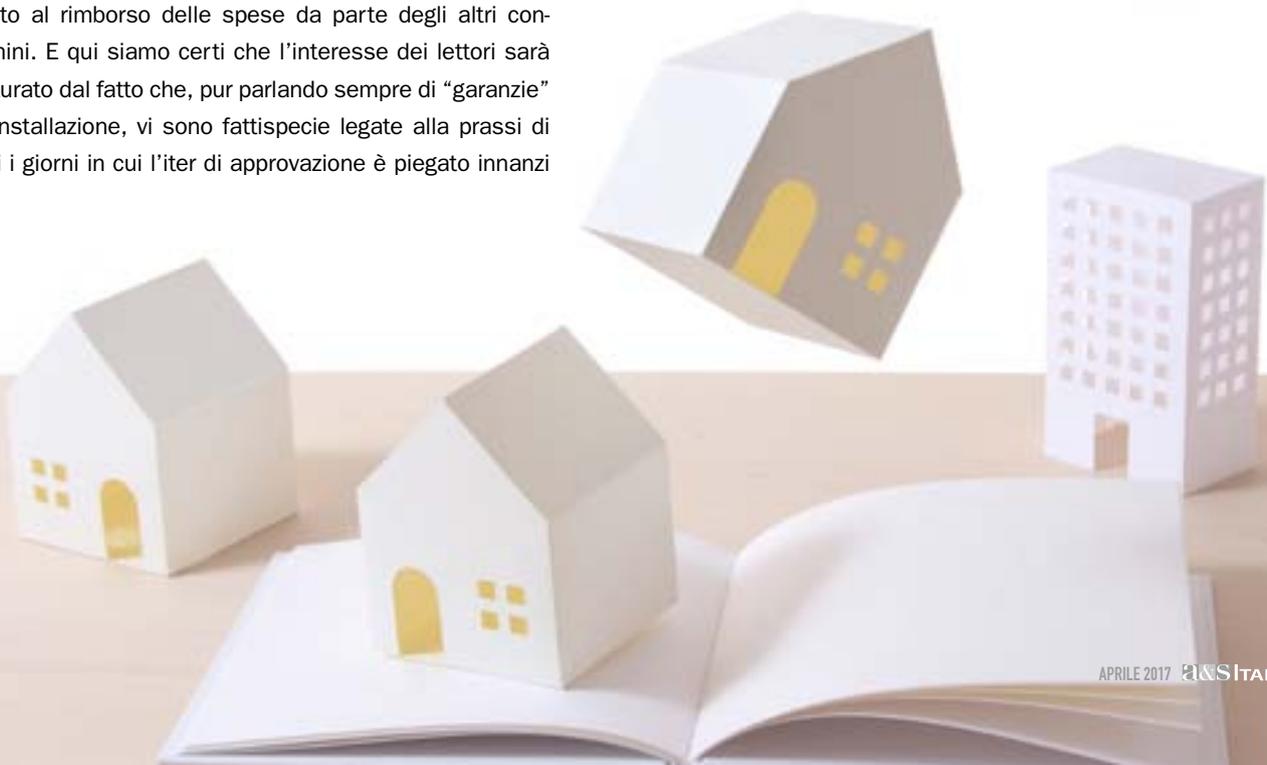
DOVE?

Proseguendo nella trattazione, volendo fornire ai lettori facili spunti di analisi, proseguiamo con la sentenza n. 71 del 2013. La Cassazione, nella fattispecie in oggetto, ha affrontato una situazione legata al “dove posizionare le telecamere” sancendo il principio di diritto secondo il quale: “il condomino può, unilateralmente, decidere di installare in via d’urgenza, senza la preventiva maggioranza assembleare, una telecamera nel parcheggio al fine di scoraggiare furti e danneggiamenti”. Ma vi è di più. Trattandosi di una decisione che pone quale principio aureo l’urgenza di garantire la sicurezza dei propri beni da danneggiamenti o dall’impossessamento doloso altrui, ecco che il condomino che ha operato l’installazione ha anche diritto al rimborso delle spese da parte degli altri condomini. E qui siamo certi che l’interesse dei lettori sarà catturato dal fatto che, pur parlando sempre di “garanzie” all’installazione, vi sono fattispecie legate alla prassi di tutti i giorni in cui l’iter di approvazione è piegato innanzi

a fini superiori. Inoltre “non sussistono gli estremi atti ad integrare il delitto di interferenze illecite nella vita privata – art. 615 bis c.p. - nel caso in cui un soggetto effettui riprese dell’area condominiale destinata a parcheggio e del relativo ingresso, trattandosi di luoghi destinati all’uso di un numero indeterminato di persone e, pertanto, esclusi dalla tutela di cui all’art. 615 bis c.p.”

Nella tecnica di posizionamento, quindi, trattandosi di un impianto comunitario ad uso di tutti i condomini, sono da mantenere saldi alcuni principi e fondamenti:

- le telecamere si possono posizionare nelle aree e spazi comuni, ponendo attenzione ai condomini dotati di servizio di portineria che non rende possibile posizionare i dispositivi senza inquadrare anche la postazione di lavoro (rif. Art.4 L.300/1970 Statuto dei Lavoratori)
- le eventuali registrazioni dovranno essere effettuate in maniera “circolare” con attività di sovrascrizione non superiore ai 7 giorni;
- l’accesso alle registrazioni non potrà essere effettuato in maniera indiscriminata, bensì motivato e con l’interessamento del Responsabile dei Dati, ovvero l’amministratore;
- dovrà essere posizionata adeguata Informativa Minima (cartellonistica) nei luoghi di accesso alle aree sottoposte alla videosorveglianza;
- l’impianto potrà essere posto in sola maniera di visualizzazione presso la postazione di portierato, qualora fosse presente.





ADRIA

Šibenik – Croatia
13–15. 09. 2017.

SECURITY SUMMIT

CONFERENCE & EXHIBITION

800+
PARTICIPANTS

70+
EXHIBITORS

300+
COMPANIES

20+
SPEAKERS

11
PARTNER
ASSOCIATIONS

Adria Security Summit is a unique annual corporate conference and exhibition event dedicated to the regional security industry. It is distinguished by its top quality level of organization, selection of renowned speakers, presentation of the leading global companies and the largest recorded number of visitors for the events of this type. Its truly regional character is confirmed by the support it receives from each of regional professional associations, diversity of visitors and rotating venues. These are the reasons why the Adria Security Summit is recognized as a central event for the exchange of information and skills which are needed for improvement of the security sector in the Adriatic region.

Telephone: +387 33 788 985
E-mail: summit@asadria.com
www.adriasecuritysummit.com



SWITCH PoE PLUG&PLAY DEDICATI ALLA VIDEOSORVEGLIANZA

Una gamma completa e specializzata di switch di rete studiata appositamente per la videosorveglianza. Unità da 8 a 24 porte PoE 10/100Mbps, Plug&Play a riconoscimento automatico di tutti i dispositivi compatibili con IEEE 802.3af/at, con alimentazione su cavo di rete.

Da oggi è possibile progettare architetture di rete complesse in modo semplice ed efficiente, installare device IP quali telecamere, telefoni anche in assenza di una fonte di alimentazione diretta fino a 250 m.

Hikvision Italy
Via Abruzzo 12, Z.I. S. Giacomo
31029 Vittorio Veneto
T +39 0438 6902
F +39 0438 690299
info.it@hikvision.com

Vittorio Veneto | Roma | Milano | Bologna

www.hikvision.com

Marco Soffientini^(*)

Controllo a distanza e Videosorveglianza nel lavoro domestico

Recentemente l'Ispettorato Nazionale del Lavoro, con nota prot. n. 1004 dell'8 febbraio 2017, ha fornito chiarimenti in merito all'installazione di impianti di videosorveglianza nell'ambito del lavoro domestico. Quest'ultima tipologia lavorativa, disciplinata principalmente dalla legge 2 aprile 1958, n. 339 ed integrata dal disposto degli artt. 2240-2246 cod. civ., consiste nella prestazione di servizi di carattere domestico diretti al funzionamento della vita familiare.

^(*) Avv. Marco Soffientini, Docente Università degli Studi di Roma UnielmaSapienza; esperto di Privacy e Diritto delle Nuove Tecnologie; Privacy Officer certificati ed in accordo a ISO/IEC 17024:2003; Coordinatore Nazionale Comitato Scientifici co Federprivacy; membro dell'Istituto Italiano per la Privacy; membro Comitato di Delibera TUV Italia per lo schema CDP e docente Ethos Academy www.academy.ethosmedia.it

Il collaboratore domestico - osserva l'ispettorato - svolge l'attività lavorativa nella casa abitata esclusivamente dal datore di lavoro e dalla sua famiglia, in quanto il rapporto di lavoro non si svolge all'interno di un'impresa organizzata e strutturata, ma nell'ambito di un nucleo ristretto ed omogeneo, di natura per lo più familiare, e risponde alle esigenze tipiche e comuni di ogni famiglia.

Pertanto, in virtù delle sue caratteristiche peculiari, il rapporto di lavoro domestico gode di una regolamentazione particolare, così come ha avuto modo di affermare la Corte Costituzionale nella sentenza 11-23 dicembre 1987 n. 585, nella quale ha statuito che "non v'è dubbio che il rapporto di lavoro domestico, per la sua particolare natura, si differenzi, sia in relazione all'oggetto, sia in relazione ai soggetti coinvolti, da ogni altro rapporto di lavoro: esso, infatti, non è prestato a favore di un'impresa avente, nella prevalenza dei casi, un sistema di lavoro organizzato in forma plurima e differenziata con possibilità di ricambio o di sostituzione di soggetti, sibbene di un nucleo familiare ristretto ed omogeneo, ed è destinato, quindi, a svolgersi nell'ambito della vita privata quotidiana di una limitata convivenza. In ragione di tali caratteristiche, la Corte ha ritenuto, in via di principio, la legittimità di una disciplina speciale anche derogatoria di alcuni aspetti di quella generale (sentenza n. 27 del 1974)". Il quadro normativo delineato - osserva l'ispettorato - è idoneo a sottrarre il lavoro domestico alla tutela dello Statuto dei lavoratori (legge n. 300/1970), poiché in questo caso, il datore di lavoro è un soggetto privato non organizzato in forma di impresa. Di conseguenza è esclusa l'applicabilità dei limiti e dei divieti di cui all'art.4 della legge n. 300/1970, che insieme agli artt. 2, 3 e 6 costituisce un corpus normativo tipico di una dimensione "produttivistica".

ESCLUSIONE DAL CODICE PRIVACY

L'esclusione dal campo di applicazione della disciplina statutaria in tema di controlli a distanza non significa anche sottrazione alla disciplina prevista dal Codice della Privacy. Infatti - conclude la nota dell'ispettorato - nell'ambito domestico, il datore di lavoro, anche nel caso di trattamento di dati riservati per finalità esclusivamente personali, incontra i vincoli posti dalla normativa sul trattamento dei dati personali a tutela della riservatezza ed, in particolare, quanto previsto dall'art.115 del d.lgs. n.196/2003. Pertanto, alla luce della nota ministeriale, nel caso in cui si intenda installare un impianto di videosorveglianza in un'abitazione privata in cui operi un lavoratore domestico, non si dovrà chiedere alcuna autorizzazione alla sede competente dell'ispettorato territoriale, ma sarà necessario chiedere al lavoratore il consenso preventivo e fornirgli un'idonea informativa.



Marc Chevenoy^(*)

La sicurezza pubblica secondo la standardizzazione

La sicurezza è un elemento vitale per la società e presenta un forte impatto sul consolidamento sociale, politico ed economico dell'Europa. La sicurezza pubblica è infatti di cruciale importanza per sostenere la crescita economica e prevenire - o proteggere da - crimini e disastri. Sicurezza significa qualità della vita e maggiore attrattività dei luoghi, poiché la minaccia di crimini ma anche di disastri viene spesso interpretata come un segnale di careza di attenzione alla pubblica sicurezza. A ciò si aggiunge un costante aumento di attacchi di matrice terroristica, che esigono un'implementazione della cyber security per proteggere i sistemi informativi. Tutto questo contribuirà ad incrementare il mercato della sicurezza pubblica, ma le sfide da affrontare saranno molteplici.

Il principale ostacolo risiede nel connettere con successo numerose tecnologie per fornire nuovo valore aggiunto. Che lavoro è stato fatto, si sta facendo e si farà in questo campo e come questo lavoro influirà sulle aziende che operano nella sicurezza pubblica e nel mercato della security? I sistemi di allarme sono essenziali per il successo di quasi tutti i settori del mercato europeo ed i rapidi sviluppi tecnologici che l'hanno interessato hanno portato nuove sfide per il relativo mercato dell'allarmistica. Sia gli standard europei che quelli internazionali rappresentano tuttavia la base di partenza per qualunque business globale.

SAFETY

La safety è di primaria importanza, dal momento che riguarda la vita delle persone. Le Organizzazioni Europee di Standardizzazione quali CEN, CELELEC, ETSI hanno da tempo stabilito degli standard per prodotti e sistemi in grado di individuare situazioni che possano minacciare la vita delle persone e prendere le misure adeguate per organizzare una risposta appropriata. Tali esempi sono gli

^(*)Technical Manager Euralarm www.euralarm.org

standard del CEN Technical Committee 72 “Fire Detection and Fire Alarm Systems”, che coprono gli standard EN54 e i documenti armonizzati e non, che offrono un’eccellente base per realizzare soluzioni elettroniche/elettromeccaniche di protezione all’interno di un quadro europeo certificato. L’etichetta CE, associata alla Construction Product Regulation (CPR), rappresenta una valutazione affidabile dei componenti e dei sistemi selezionati, installati e mantenuti dalle aziende di servizi qualificate. Per completare la rilevazione dei pericoli, gli standard del CEN Technical Committee 191 “Fixed Fire Fighting Systems” specificano le soluzioni per combattere fumo e incendi all’interno di edifici, ad es. tramite sprinkler ad acqua, polvere, schiuma o altri sistemi a gas.

SECURITY

Quando si tratta di proteggere merci, proprietà e persone da attacchi di vario genere, le soluzioni principali vengono offerte dal CENELEC Technical Committee 79 “Alarm systems”, che ha a lungo contribuito alla definizione di standard di prestazioni per i sistemi di allarme, controllo accessi, protezione perimetrale, videosorveglianza, centri di ricezione e monitoraggio allarmi, ed altre applicazioni di security. Ovviamente la standardizzazione dei componenti per le applicazioni safety e security non è sufficiente per garantire sicurezza.

Gli standard di gestione della security e della safety giocano un ruolo importante nell’aumentare la consapevolezza rispetto al pericolo ed aiutano a sviluppare il giusto comportamento in situazioni critiche. Scopo del CEN Technical Committee 391 “Societal and Citizen Security”, assieme al pacchetto base sviluppato dall’ISO Technical Committee 292 sotto la dicitura “Security and Resilience”, è occuparsi del processo di gestione delle crisi e identificare ruoli e responsabilità dei vari attori. Alcuni obiettivi specifici del CEN TC391: offrire una guida per la gestione della crisi e la protezione civile nell’ambito dell’educazione sul rischio chimico, biologico, radiologico, nucleare e degli esplosivi (CBRNE) e formare ma anche proteggere le strutture sanitarie. Oltre agli standard, EN, ISO e IEC propongono soluzioni per tutti gli aspetti della security: si tratti di prodotti e sistemi, ma anche di strumenti di gestione per un monitoraggio efficace del rischio in spazi pubblici all’interno di città, edifici privati o pubblici o in situazioni quotidiane che minacciano la vita delle persone. L’armonizzazione e l’interoperabilità dei sistemi è poi spesso fonte di preoccupazione ed implica

la definizione di priorità nel presentare le informazioni nell’ordine giusto per mettere in campo azioni correttive rapide ed efficaci. Si fa sempre più attenzione a progetti che mirano a organizzare le Smart city in termini di protezione dei cittadini e infrastrutture critiche. Ciò implica la definizione e l’utilizzo di standard e processi esistenti e l’adattamento degli stessi per definire le responsabilità operative, considerando al contempo i molteplici aspetti legati ai comportamenti della cittadinanza.

SICUREZZA CYBER

Molti sistemi informativi a livello mondiale stanno rafforzando la sicurezza cyber e vanno valutati con grande attenzione, specialmente se si tratta di sistemi dedicati a safety e security. CEN, CENELEC, ETSI e altre organizzazioni stanno lavorando per adattare i sistemi di gestione della qualità e le certificazioni per gestire un obiettivo in continuo mutamento come la sicurezza cyber ed il Coordination Group collabora attivamente con l’agenzia European Union Agency for Network and Information Security (ENISA) e la Multi-Stakeholders Platform on ICT standardization. Particolare attenzione è stata data alle linee guida sulla standardizzazione di servizi che le aziende specializzate possono dare nel settore safety e security. Un nuovo standard di servizi è ora disponibile: si chiama EN 16673 “Services for fire safety systems and security systems”. I servizi, dal punto di vista safety e security, assommano la sicurezza antincendio negli edifici, la safety antincendio, la prevenzione del rischio in edifici e in fase di progettazione, la protezione antincendio strutturale, la prevenzione dell’allargamento degli incendi, la predisposizione di via di fuga all’interno di edifici, gli allarmi antincendio, i sistemi di allarme, i rivelatori antincendio e antifumo e i sistemi di controllo automatici. La progettazione, l’installazione, il commissioning e la manutenzione sono i temi principali per mostrare la competenza dell’azienda di servizi. In parallelo a questo standard si sta mettendo a punto un nuovo documento per specificare i servizi da remoto per i sistemi di safety e security. I membri di Euralarm partecipano attivamente allo sviluppo della standardizzazione assieme a CEN, CENELEC, ETSI e altre organizzazioni internazionali per definire un comune terreno di gioco per l’industria della sicurezza. Inoltre contribuiscono a migliorare costantemente il sistema di standardizzazione in numerosi paesi europei e con iniziative come la Joint Initiative on Standardisation.

La certificazione degli esperti in Impianti di Allarme Intrusione e Rapina

Due nuovi profili professionali per il comparto della sicurezza.

Con lo sviluppo di tecnologie sempre più evolute e l'emanazione di norme che regolano il loro utilizzo, la competenza tecnica e di governance nel comparto della sicurezza sono oggi elementi fondamentali per differenziarsi dal mercato e per proporre un servizio completo di qualità.

Per valorizzare le conoscenze e competenze dei professionisti, TÜV Italia ha sviluppato un nuovo schema per la certificazione degli esperti e degli installatori, manutentori e riparatori di impianti di allarme antintrusione e rapina.

www.tuv.it/cei



Italia

**Scegli la certezza.
Aggiungi valore.**



UNIVIEW BORN FOR EXCELLENCE

- ▶ **Expert in IP:** First introduced IP surveillance to China, Uniview has more than 10 years experience in IP video surveillance.
- ▶ **Quality-oriented:** Strict product development system with more than 680 tests. Qualified by CMMI5, CE, FCC, UL/CSA, NEBS, etc.
- ▶ **Innovative:** more than 1000 patents applied in China. More than 15% annual sales invested in R&D
- ▶ **Whole IP solution provider: IP Camera, NVR, Encoder, Decoder, IP SAN, VMS, APP & Cloud Service**



DISTRIBUTORE UFFICIALE **UNV**[®]
Uniview Technologies

TAV
TRANS AUDIO VIDEO GROUP

www.transaudiovideo.com

Trans Audio Video S.r.l.

Viale Lincoln 38-40 - 81100 Caserta (CE) - Tel. +39 0823 329970

Via Lodi, 1 - 20835 Muggiò (MB) - Tel. +39 039 791339

Email: cctv@transaudiovideo.com

Hikvision: un'azienda privata che si occupa di sicurezza

Di recente la stampa estera si è focalizzata a più riprese sulla natura societaria di Hikvision, riportando dati che potrebbero ingenerare confusione. Cogliamo quindi questo interessante assist per raccontare al mondo, con trasparenza, serietà e pragmatismo, la realtà Hikvision: come opera, quali valori e obiettivi persegue, come è composta e come si finanzia.

HIKVISION È UNA SOCIETÀ PRIVATA QUOTATA IN BORSA

Hikvision è una public-traded company, ossia un'impresa privata quotata in borsa. Ed è, com'è noto, una società cinese. In Cina le imprese private che mostrano il maggior potenziale di sviluppo o che seguono settori particolarmente delicati sono spesso oggetto di investimenti ad opera di capitale statale. Fatto peraltro consueto anche in Occidente, dove è comune che imprese dedicate a settori sensibili, o volte alla protezione di valori fondanti per la società, vengano partecipate anche dai governi. Hangzhou Hikvision Digital Technology Co., Ltd. è una società per azioni quotata in borsa e presenta una struttura proprietaria complessa, composta da un insieme eterogeneo di soggetti pubblici e privati. Al 30 giugno 2016, il 41.88% delle azioni di Hikvision era di proprietà congiunta della China Electronics Technology HIK Group Co., Ltd. (CETHIK) e dell'Istituto di Ricerca CETC No. 52; entrambi facenti parte di CETC, un'impresa di proprietà statale. Il 18.28% è di proprietà di Mr. Kung Hung Ka (residente ad Hong Kong); l'8.48% è posseduto dai fondatori e dirigenti della società ed il restante 31.36% è di proprietà di investitori A-share; investitori istituzionali internazionali quali UBS AG e JP Morgan (che sono tra i primi 10 azionisti di Hikvision). Hikvision si configura quindi come un'impresa privata quotata in borsa.

Non ha natura, né struttura, né finalità di tipo governativo, né è controllata dal governo cinese, poiché la partecipazione di capitale pubblico – peraltro esercitata in forma indiretta, tramite due imprese intermediarie – si configura in percentuale inferiore al 42%.

HIKVISION SI FINANZIA COME QUALUNQUE ALTRA IMPRESA

Come tutte le imprese private, Hikvision si finanzia con un mix di capitale, crediti bancari, IPO, titoli. La China Development Bank ha assicurato un credito a favore di Hikvision per 3,1 miliardi di dollari destinati a realizzare nuovi investimenti, progetti di espansione all'estero, apertura di nuove filiali e di nuovi mercati geografici e tecnologici. Non si tratta ovviamente di un finanziamento a fondo perduto (cioè volto a ripianare perdite o destinato alla vendita di sistemi al di sotto dei prezzi di mercato), ma di un comune prestito bancario, che dovrà essere restituito con gli interessi. L'ultimo bilancio di Hikvision evidenzia peraltro un 21,7% di utile: con simili standard di profitto, sarebbe davvero arduo ipotizzare che Hikvision possa caldeggiare politiche di svendita o di rivendita di prodotti a prezzi inferiori al costo. Hikvision, infine, come scelta etica e di rispetto verso i propri partner, condanna fermamente l'utilizzo di canali distributivi low cost non professionali, come i circuiti di e-commerce.

HIKVISION PRODUCE SISTEMI DI SICUREZZA

Unica e ambiziosa mission di Hikvision è quella di salvaguardare la vita delle persone, le loro proprietà, gli asset aziendali, le opere d'arte e dell'ingegno, la memoria e la salute attraverso la produzione di prodotti, sistemi e soluzioni in grado di fornire sicurezza. Qualunque altra finalità le venga attribuita, diretta o mediata, è del tutto priva di fondamento. E' da respingere quindi in maniera assoluta ogni insinuazione, come quella (totalmente infondata e già più volte smentita) avanzata dal leader di Genetec, che i prodotti Hikvision possano consentire al governo cinese o a chicchessia l'accesso al materiale video acquisito a scopi di spionaggio. Hikvision ha venduto decine di milioni di dispositivi collegati in rete, telecamere IP e NVR e non c'è una sola evidenza al mondo del fatto che mai sia stato consentito questo genere di accesso. Ogni modifica ad un dispositivo di bordo, ad esempio una telecamera, verrebbe peraltro immediatamente rilevata dai dispositivi di rete e dalle piattaforme di sicurezza. E soprattutto: la cyber security è in cima alle priorità di Hikvision.

HIKVISION PRODUCE SISTEMI SICURI

Per chiunque produca dispositivi di sicurezza fisica, la Cybersecurity dei dispositivi è la prima preoccupazione: a maggior ragione lo è per il primo produttore al mondo di prodotti e soluzioni di videosorveglianza e sicurezza. Hikvision ha istituito una task force presso gli Headquarters, la *Network and Information Security Lab*, che è responsabile della definizione delle norme di sicurezza e dell'esecuzione di valutazioni e test per la risoluzione di eventuali problemi. Hikvision ha collaborato con importanti organizzazioni esterne specializzate in test di sicurezza, tra cui Rapid7, nota azienda statunitense, per l'esecuzione di test di penetrazione e valutazioni di vulnerabilità dei prodotti. Attraverso una ricerca esaustiva e la convalidazione delle sue attrezzature, Hikvision non ha riscontrato alcuna vulnerabilità backdoor. Hikvision si impegna infatti da sempre a mantenere i più elevati standard di sicurezza e privacy e non consente in alcun modo l'accesso a soggetti terzi di qualsivoglia natura. Per mera completezza di informazione, si rammenta che la sicurezza di un sistema di videosorveglianza è legata

non solo all'impenetrabilità dei dispositivi di campo, ma anche - e soprattutto - alla qualità e al corretto dimensionamento della rete che veicola i dati. Tale aspetto, non di rado trascurato, rientra nell'alveo delle responsabilità dell'utilizzatore.

PARLANO I NUMERI

Hikvision è un'azienda privata che fa sicurezza: con 4,67 miliardi di dollari di fatturato nel 2016 e un tasso di crescita del 26,69%, detiene il 23,2% del mercato globale di network cameras per la videosorveglianza. Hikvision dispone di 25 filiali disseminate nel mondo che assistono, seguono e servono la clientela sul territorio. E' partner fiduciaria dei migliori system integrator e utenti finali in tutto il mondo e si confronta costantemente con leader tecnologici di primaria importanza. I prodotti Hikvision sono fabbricati, controllati e testati in industrie di prim'ordine ad Hangzhou, la "Silicon Valley cinese". Hikvision invita regolarmente System Integrator e professionisti della sicurezza di tutto il mondo a visitare gli Headquarters, perché crede che vedere sia sempre la strada migliore per credere. E crede che i numeri parlino più di mille voci di corridoio: Hikvision è il produttore numero 1 al mondo nel comparto security. Non occorre aggiungere altro.



Hikvision Italy

Via Abruzzo 12, Z.I. San Giacomo
31029 Vittorio Veneto
Tel +39 0438 6902
Fax +39 0438 690299
info.it@hikvision.com
www.hikvision.com/it

La Redazione

La Videoverifica degli eventi, un aiuto concreto

La videoverifica degli eventi, ovvero la possibilità di avere una conferma inequivocabile di quanto sta avvenendo in un determinato luogo in tempo reale, rappresenta un eccellente ausilio tecnologico per garantire sicurezza in maniera efficace ed efficiente.

Questa tipologia di soluzione è tuttavia utile ed efficace solo se è: realmente efficiente; di utilizzo immediato; economicamente sostenibile per una grande maggioranza di utenti; semplice da installare e da configurare (perché non risulti essere appannaggio di pochi). Se tutte queste condizioni sono soddisfatte, allora i vantaggi della videoverifica in termini di sicurezza risultano indiscussi.

I BENEFICI

I dati a livello mondiale sono molto chiari al riguardo: il 98% degli allarmi per "intrusione" risultano essere falsi allarmi. Inoltre il tempo medio di risposta delle forze dell'ordine alla comunicazione di un allarme "non verificato" risulta essere di circa 45 minuti, mentre il tempo medio di risposta delle forze dell'ordine ad un allarme "verificato" è di soli 7 minuti. Gli utenti dotati di sistemi di allarme connessi alla Vigilanza Privata beneficiano dunque fortemente di un servizio più accurato e puntuale. Alcuni paesi iniziano addirittura a multare gli utenti per le chiamate che si rivelano poi essere dei falsi allarmi.

UNA SCELTA PROFESSIONALE

Il mercato oggi mette a disposizione dell'utente svariate soluzioni: dalle più semplici, anche "fai da te" e spesso poco efficaci, alle più complesse, che non di rado finiscono con il superare le reali esigenze dell'utente. La soluzione sulla quale ci concentriamo in questo articolo è quella offerta da un sistema semplice ma efficace, che rivela immediatamente all'utente la presenza di un intruso all'interno della proprietà protetta da un sistema di sicurezza integrato. Un sistema così concepito ed articolato rientra nel mercato dei sistemi professionali ove è richiesta, soprattutto, competenza in fase di analisi dei locali da proteggere e poi una corretta installazione dei dispositivi scelti. Questi sistemi necessitano quindi della competenza di un installatore professionale di impianti di sicurezza.

VIDEOVERIFICA SU CLOUD

Perché la videoverifica sia davvero efficiente, di semplice utilizzo ed installazione ed economicamente sostenibile, la soluzione più adeguata, ad oggi, risulta essere quella del cloud. Il cloud è una piattaforma hardware e software gestita da aziende di riferimento nel panorama mondiale



Abbiamo visto vantaggi ed architettura di una soluzione di videoverifica su piattaforma cloud. Possiamo adesso fare un esempio di configurazione tecnica del servizio?

Risponde Ercole Caccese, Technical Manager RISCO Group

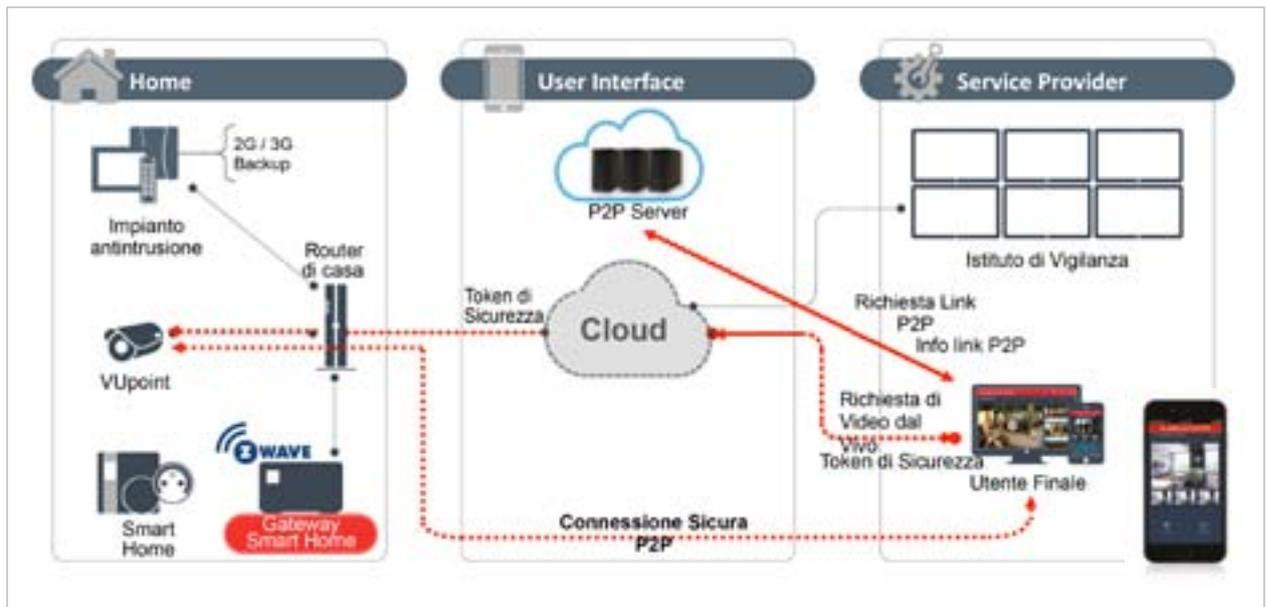
Nella videoverifica basata su una piattaforma cloud i dispositivi, come il sistema antintrusione e le telecamere IP, sono costantemente connessi al cloud: è quindi il software residente nel cloud il soggetto deputato a mettere in relazione questi dispositivi permettendone la completa integrazione. Con il software residente nel cloud, il tecnico definisce per quali specifiche aree o singoli sensori antifurto le telecamere installate debbano effettuare gli scatti-immagine di pre e post allarme e le clip video e defluiscono anche per quanto tempo tali dati dovranno essere conservati. Tramite semplici passaggi logici, il software residente nel cloud integra i vari dispositivi per un risultato finale che dovrà garantire all'utenza 13.03 27/04/2017 precisione ed immediatezza nella verifica video degli allarmi. E sulla sicurezza e qualità del nostro Cloud non vi sono dubbi: lo testimonia la recente Certificazione EN 50136-3:2013.

www.riscogroup.it

in grado di garantire servizi, continuità di funzionamento e quindi ridondanza completa, nonché sicurezza delle comunicazioni allo stato dell'arte e Privacy in conformità alla normativa europea vigente. E' ovviamente fondamentale affidarsi ad aziende specializzate nell'erogazione dei servizi cloud. La piattaforma cloud rende disponibile per tanti utenti una serie di risorse hardware e software che altrimenti dovrebbero essere acquistate, installate, configurate e mantenute singolarmente per ogni utente. La soluzione cloud, in definitiva, sembra oggi la migliore scelta per un sistema semplice, immediato ed efficiente di videoverifica, per tutti i segmenti di mercato, dal residenziale al commerciale.

COME FUNZIONA

Il funzionamento della videoverifica basata su una piattaforma cloud permette all'utente, ovunque egli sia, di ricevere sul proprio smartphone ed in tempo reale, una serie di immagini riferite ad un evento di intrusione che comprendono tutta la fase dell'evento: prima, durante e dopo. Oltre alle immagini che evidenziano la fase dell'intrusione - e quindi, eventualmente, la conferma della pre-



senza effettiva di un intruso - si può ottenere anche un filmato dell'evento, solitamente di circa 30 secondi, ed infine lo streaming live in tempo reale. Il grande vantaggio di questa soluzione è quello di avere tutto sul proprio smartphone nella stessa pagina senza doversi spostare, selezionare menu differenti o aprire più applicazioni. L'altro notevole vantaggio è quello di poter consultare immagini e filmati video degli allarmi anche successivamente, per un tempo predefinito e configurabile dall'installatore in riferimento alla specifica applicazione e, di conseguenza, alla normativa vigente. Immagini e video risiedono nell'area protetta del cloud dedicata alla specifica utenza e non possono essere manomesse o trafugate dagli stessi intrusi.

ARCHITETTURA

Ma quali sono le tecnologie usate, i componenti e i rispettivi compiti in un sistema di video verifica così strutturato? Parliamo di: a) sistema anti-intrusione installato nella proprietà dell'utente costantemente connesso alla piattaforma cloud via IP o GPRS/3G; b) numero virtualmente illimitato di telecamere IP, correttamente posizionate nei punti strategici al fine di garantire la rilevazione della presenza dell'intruso, e connesse via cavo o in WiFi al router dell'utente; c) area specifica dedicata, all'interno della piattaforma cloud, ove mettere in relazione i diversi sensori del sistema antifurto con le varie telecamere installate presso l'utente. Come si evince dall'elenco, la

soluzione richiede un hardware veramente minimo poiché tutta la gestione, il funzionamento e la sincronizzazione degli eventi avviene a livello cloud. Anche la fase di installazione e configurazione viene ridotta all'essenziale poiché, a parte la predisposizione del sistema antifurto in funzione dell'analisi del rischio e delle esigenze dell'utente, le telecamere IP sfruttano il sistema di comunicazione p2p, che non prevede alcuna modifica o configurazione del router dell'utente come apertura di porte o indirizzi IP statici/pubblici. Questa tipologia di telecamere, una volta alimentate e connesse alla rete dell'utente, viene subito presa in carico dal cloud e resa quindi disponibile per l'interazione con il sistema di antifurto.

IL P2P NELLA VIDEO VERIFICA

I vantaggi delle telecamere p2p nell'utilizzo dei sistemi di verifica video sono tanti rispetto all'utilizzo delle telecamere IP tradizionali. Ad esempio: non occorre un servizio DDNS; non serve programmare il router dell'utente con il port forwarding o il port mapping; la telecamera IP si connette ad internet anche senza IP pubblico; streaming video completamente cifrato a garanzia della propria Privacy; la connettività cloud viene ulteriormente protetta tramite l'utilizzo di un token temporale specifico per la singola sessione di connessione (streaming live). Tutto questo si traduce in un'installazione realmente Plug & Play.



NEXTtec

al servizio della sicurezza

PRODOTTI ITALIANI 



NSE100

IL NUOVO VOLTO DI NEXTtec NSE100 SIRENA PER ESTERNO INNOVAZIONE E RAFFINATO DESIGN UNITO AD UNA SUPERIORE VERSATILITA' FUNZIONALE E SEMPLICITA' DI UTILIZZO

- Forma, colori, prestazioni concorrono nella definizione di un prodotto nato per distinguere e accrescere la visibilità dell'attività dell'installatore.
- Sezione Acustica multisound programmabile disponibile in 4 suoni differenti per adattarli all'uso e al contesto
- Doppio comando di allarme per differenziare il livello sonoro in funzione della tipologia e dell'entità dell'allarme
- La Notifica ottica Informer aumenta la visibilità della protezione informando l'utenza. Gestita da ingressi di controllo programmabili, offre molteplici possibilità operative ai comandi differenziati grazie a differenti colori e frequenze di lampeggiamento dei led.
- Disponibili set di auto-protezione anti-schiuma, anti-avvicinamento
- Universale adatta a qualsiasi modello o marca di centrale

NEXTtec progetta e produce efficienti sistemi di sicurezza concepiti per agevolare l'installatore attraverso una programmazione facile ed immediata e per garantire una gestione intuitiva e semplificata, studiata ad hoc per l'utente.

visita il ns. sito www.nexttec.it

NEXTtec srl: Via Ivrea 71/b Rivoli (TO) Tel: 0119539214 info@nexttec.it

SEGNALAZIONE
STATO IMPIANTO
DI BEN 2 ZONE
CON LED
MULTICOLOR



La Redazione

Il problema delle riprese notturne: soluzioni tecnologiche

Tra i limiti più conosciuti delle telecamere IP c'è sempre stata la visione notturna; vista l'elevata risoluzione tipica delle telecamere IP rispetto al mondo analogico, è infatti sempre stato molto complesso ottenere immagini nitide senza quello che viene tipicamente definito "rumore". Il "rumore" delle immagini notturne è dovuto all'utilizzo di ISO elevati, unica soluzione fino ad oggi studiata per ottenere una visione notturna adeguata, ma con l'inconveniente del forte disturbo dovuto alla limitata sensibilità dei sensori. Riuscire ad ottenere una ripresa nitida di notte è quindi da sempre l'obiettivo di tutti i produttori.

La soluzione oggi più utilizzata rimane l'uso degli illuminatori ad infrarossi che permettono una visibilità elevata illuminando l'area interessata, ma non affrontano il problema principale: quello riguardante la sensibilità dei sensori.

ALCUNE SOLUZIONI

In campo fotografico le tecniche più note per affrontare la problematica della luce sono:

1. aumentare l'esposizione (ma in situazioni di ripresa non è possibile, in quanto elevati tempi di esposizione rendono l'immagine poco fluida e spesso non adatta);
2. aumentare gli ISO (creando però l'effetto "rumore" che rende l'immagine decisamente poco nitida e non utile, soprattutto in ambito sicurezza, poiché si perdono dettagli spesso indispensabili. Gli ISO riducono infatti i "pixel utili" dell'immagine facendo perdere il dettaglio necessario).

L'uso degli illuminatori, peraltro, presenta molti aspetti negativi. Tra questi segnaliamo il fatto che:

1. l'illuminazione è limitata ad un fascio, dunque l'area coperta sarà sempre vincolata ad esso;
2. non è possibile vedere sulle lunghe distanze, in quan-

to i tipici fasci luminosi sono in grado di illuminare in modo chiaro solo fino a 30/50mt;

3. l'Infrarosso - come qualsiasi "luce" - è passibile di riflesso e di aree sopra/sotto esposte, di ombre etc, quindi è molto difficile garantire una qualità di ripresa stabile nel tempo;
4. il costo dell'illuminazione artificiale può essere molto oneroso, soprattutto in aree particolarmente estese.

CHIPSET DI ULTIMA GENERAZIONE

Affrontare il problema "ripresa notturna" è sempre stata un'esigenza di tutti i produttori in ambito IP, ed oggi le tecnologie ci sono venute incontro grazie a Chipset di ultima generazione (*). Ma non è tanto l'hardware in sé, bensì l'integrazione di queste tecnologie a fare la differenza. Questi nuovi Chipset portano il limite della visione notturna fino a 0,008 lux (vedi immagine 1), ma presentano anche ulteriori vantaggi. In primo luogo viene offerta una visione notturna a colori, che permette di acquisire tutti i dettagli che abitualmente di notte si perdono, con un miglior riconoscimento dei volti e dei particolari. Non è inoltre previsto alcun limite nell'area di ripresa, in quanto sono sufficienti le normali condizioni di luce notturna. Non si deve poi utilizzare alcun illuminatore, garantendo quindi anche una visione a distanze elevate e non esistono rischi di aree non coperte o "in ombra" dovuti all'illuminazione artificiale.

(*Come Sony StarVis, utilizzato ormai da molti produttori per affrontare il problema della scarsa illuminazione.





Abbiamo letto di chipset integrati su telecamere che portano la visione notturna a 0,008 lux.

Ma cosa significa, in concreto, riprendere immagini video a 0,0008 lux?

Risponde Salvatore Scolaro, Marketing & SEO Setik

Consideriamo che una comune telecamera offre riprese qualitativamente sostenibili fino a 20-30 lux, mentre una tipica notte stellata priva di luna arriva al massimo a 0,003 Lux. Ciò significa che l'unico modo per garantire una visione adeguata in presenza di poca luce è l'utilizzo di immagini in Bianco e Nero combinata ad illuminatori. Si tratta però di una soluzione limitante perché riduce gli spazi operativi, nonché la stessa efficacia dell'impianto. Tenendo poi presente che la videosorveglianza è da tempo passata da semplice "visione" ad "analisi delle immagini", la necessità di disporre di immagini nitide e chiare è un must per analizzare correttamente i soggetti o l'area di ripresa. Esigenze come riconoscimento targhe o volti richiedono nitidezza dell'immagine, che oggi è possibile solo con tecnologie evolute ed applicate a strumenti di visione professionali. La maggiore risoluzione tipica delle telecamere IP moderne, integrata a soluzioni come quella descritta nell'articolo, garantiscono soluzioni uniche in ambito di videosorveglianza.

www.setik.biz

COME FUNZIONA?

L'implementazione dei chipset è diversa a seconda del produttore, l'integrazione Chipset-codec è necessaria al corretto sviluppo delle immagini, fino ad arrivare a soluzioni di visione quali a buio assoluto (0,0008 lux), adatti ad ambienti assolutamente privi di luce naturale o artificiale. Come per tutte le tecnologie, si può affrontare il problema da un solo punto di vista o da molti: in alcuni casi⁽¹⁾ si è

⁽¹⁾ Con "Super Starlight"

⁽²⁾ Telecamere "Super Starlight"

cercato di affrontarlo ottimizzando tutti i componenti che fanno parte del processo di ripresa. Per ottenere visioni di questo tipo sono ovviamente necessarie combinazioni di tecnologie differenti che coinvolgono più aree della telecamera, tecnologie oggi presenti solo su alcune telecamere⁽²⁾. Ad esempio: sensore ad elevata resa notturna di ultima generazione; elevata apertura del diaframma (F/1.2) che garantisce un'elevata quantità di luce; lenti trattate per ottenere un effetto ultra-trasparente e ridurre l'attenuazione dovuta alla lente; tecnologie che aumentano la sensibilità +7db e che riducono il disturbo fino al 38% (TVP). L'integrazione di più tecnologie applicate ad un unico prodotto è possibile anche grazie a processori più potenti, che permettono un'analisi più complessa dell'immagine pur mantenendo il frame rate necessario ad una ripresa fluida, tale da dar vita ad una generazione di telecamere adatte alla visione notturna anche senza alcun illuminatore.

APPLICAZIONI

Quali applicazioni traggono vantaggio da questo tipo di telecamere? Senza dubbio qualsiasi ripresa in area esterna, poiché vengono eliminati i punti ciechi dovuti all'illuminatore. La visione a colori notturna garantisce altresì maggiori dettagli, solitamente nascosti nella visione in Bianco e Nero. Non dovendo utilizzare illuminatori, è poi possibile ridurre il consumo energetico - aspetto sul quale molti produttori oggi spingono per ottimizzare i costi di mantenimento degli impianti di videosorveglianza. Inoltre l'assenza di illuminatori garantisce anche un elevato livello di sicurezza, in quanto non sono presenti i tipici led Infrarossi visibili. In sostanza: queste telecamere sono ideali ovunque occorra vedere di notte a distanza (campi fotovoltaici, perimetri, etc.).



NUOVE CENTRALI DI ALLARME

eclipse

Centrali di allarme fino a 32 zone con comunicatore PSTN a bordo, modulo GPRS aggiuntivo per gestione da smartphone, espandibili filo e radio con i benefici di una vera bidirezionalità



Nuova gamma di centrali adatta per soluzioni residenziali e small business. Sistemi facili da programmare e utilizzare, tastiere e telecomandi accattivanti nell'aspetto, sono la soluzione ideale per le esigenze degli installatori che necessitano di un prodotto di qualità elevata ma dai costi contenuti.

Possono gestire fino a 8 aree indipendenti e accettano numerosi tipi di cablaggi a singolo e doppio bilanciamento. Supportano un ricevitore radio che permette al sistema di riconoscere sensori, contatti e telecomandi wireless bidirezionali.



Segnale sicuro e risparmio della batteria



Protezione Jamming



Installazione veloce, semplice e sicura



Segnalazione sul telecomando dello stato impianto

ETER

BIOMETRIC TECHNOLOGIES

ETER Biometric Technologies Srl

Via Cartesio, 3/1

42122 Bagno (RE) - ITALY

Tel. +39 0522 262 500

Fax +39 0522 624 688

E-mail: info@eter.it - www.eter.it

Eter Biometric Technologies

Telefono +390444946360 - Fax +390444298217 - E-mail info@studioscambi.com - Internet www.studioscambi.com

studioscambi

progettazioni
consulenze
formazione



PROGETTAZIONE

Videosorveglianza Urbana

Zona a traffico limitato

Smart City

Digital Signage

Antintrusione e riconoscimento

Domotica

Fibra ottica, wireless, cablaggi strutturati

Impianti elettrici

Rilevazione incendio

CONSULENZE

Tecnico legali

Video forensi

Stesura contratti di manutenzione

RISCHIO AZIENDALE

Analisi del rischio ISO 31000

Crime prevention trough environmental - CPTED

Security plan

Studio delle difese fisiche ed elettroniche

E-mail info@studioscambi.com - Internet www.studioscambi.com

E-mail info@studioscambi.com - Internet www.studioscambi.com

Telefono +390444946360 - Fax +390444298217 - E-mail info@studioscambi.com - Internet www.studioscambi.com

Roberta Rapicavoli(*)

Qual è l'ambito di applicazione del DM 37/2008?



Le imprese installatrici e i progettisti sono tenuti a rispettare gli obblighi previsti dal decreto ministeriale n. 37 del 2008, riguardante il riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici. Ma quando trova concretamente applicazione tale normativa? Come espressamente previsto dall'art. 1 del DM 37/2008, il decreto si applica "agli impianti posti al servizio degli edifici, indipendentemente dalla destinazione d'uso, collocati all'interno degli stessi o delle relative pertinenze". Un primo aspetto da considerare, in ordine all'ambito di applicazione definito dal citato articolo 1, è legato alla destinazione degli edifici al servizio dei quali gli impianti vengono posti. Infatti, mentre la previgente Legge 46 del 1990 si applicava agli impianti presenti negli edifici destinati unicamente ad uso civile, con la sola eccezione degli impianti elettrici, adesso, ai fini dell'applicazione del DM 37/2008, non rileva in nessun caso la destinazione d'uso dell'edificio al cui servizio l'impianto è posto.

QUALI EDIFICI

Chiarito allora tale aspetto relativo alla destinazione d'uso, considerando che il citato decreto disciplina l'installazione degli impianti all'interno degli edifici, occorre chiedersi cosa debba intendersi con tale termine. In base a quanto riportato nel previgente DPR 447/1991 (Regolamento di attuazione della legge 46/90), per "edificio" si intende un'unità immobiliare. Interessante però considerare che, secondo l'art. 812 del codice civile, rientrano tra i beni immobili gli edifici e le altre costruzioni anche se unite al suolo a scopo transitorio. Ciò che rileva, pertanto, è il collegamento della struttura al suo-

lo, a prescindere dal fatto che la stessa abbia o meno un carattere provvisorio. Per tale ragione il DM 37/2008 trova applicazione anche nel caso di impianti posti al servizio di strutture provvisorie, purché unite al suolo - quali sono solitamente quelle utilizzate, ad esempio, in occasione di fiere o mostre.

DOVE DEV'ESSERE L'IMPIANTO

Ulteriore profilo da analizzare è legato alla collocazione dell'impianto. Il DM 37/2008 si applica infatti non solo nel caso in cui gli impianti posti al servizio dell'edificio siano collocati all'interno dello stesso, ma anche nell'ipotesi in cui siano collocati all'interno delle relative pertinenze. Anche in tal caso, al fine di comprendere cosa debba intendersi per "pertinenze", occorre richiamare l'art. 817 del codice civile, che definisce, con tale termine, le cose destinate in modo durevole a servizio o ad ornamento di un'altra cosa. Per pertinenze si intendono dunque quelle opere che, pur conservando la propria individualità fisica, sono complementari e funzionalmente subordinate, in modo attuale e permanente, all'edificio. Così, ad esempio, costituiscono pertinenza di un edificio i garage o i parcheggi. Esaminati alcuni dei profili di maggior rilievo per definire l'ambito di applicazione del DM 37/2008, rimane da chiedersi quali siano gli impianti disciplinati da tale normativa.

QUALI IMPIANTI

Gli impianti che ricadono nell'ambito di applicazione del DM 37/2008 sono classificati, all'art. 1 comma 2 del decreto, in sette tipologie:

(*) Roberta Rapicavoli, Avvocato esperto in Information Technology e privacy e Docente Ethos Academy www.robentrapicavoli.it

- a. impianti di produzione, trasformazione, trasporto, distribuzione, utilizzazione dell'energia elettrica, impianti di protezione contro le scariche atmosferiche, nonché gli impianti per l'automazione di porte, cancelli e barriere;
- b. impianti radiotelevisivi, le antenne e gli impianti elettronici in genere;
- c. impianti di riscaldamento, di climatizzazione, di condizionamento e di refrigerazione di qualsiasi natura o specie, comprese le opere di evacuazione dei prodotti della combustione e delle condense, e di ventilazione ed aerazione dei locali;
- d. impianti idrici e sanitari di qualsiasi natura o specie;
- e. impianti per la distribuzione e l'utilizzazione di gas di qualsiasi tipo, comprese le opere di evacuazione dei prodotti della combustione e ventilazione ed aerazione dei locali;
- f. impianti di sollevamento di persone o di cose per mezzo di ascensori, di montacarichi, di scale mobili e simili;
- g. impianti di protezione antincendio.

E LA SICUREZZA?

Negli impianti elencati nella citata disposizione non sono espressamente indicati impianti molto diffusi per finalità di sicurezza, quali, ad esempio, gli impianti di antintrusione, di videosorveglianza o di controllo accessi. Il fatto che gli stessi non siano però espressamente richiamati non vuol dire che siano esclusi dall'ambito di applicazione del decreto. Si tratta infatti di impianti che rientrano nella tipologia di cui alla già citata lettera b) dell'art. 1, comma 2, ossia negli "impianti radiotelevisivi, antenne e impianti elettronici in genere". Interessante, sul punto, richiamare la Circolare 279/2013 del Consiglio Nazionale degli Ingegneri, che contiene un'elencazione, seppur non esaustiva, degli impianti elettronici di cui al DM 37/2008, tra cui sono indicati, appunto, per quanto di interesse, gli impianti di videosorveglianza, controllo accessi, identificazione targhe. Pertanto, nel caso in cui un'impresa dovesse installare uno di tali impianti all'interno di un edificio o delle relative pertinenze, dovrebbe sicuramente operare nel rispetto di quanto stabilito dal DM 37/2008, rischiando, in caso contrario, di incorrere nelle sanzioni individuate nel citato decreto (si pensi, tra le altre, alla sanzione prevista dall'art. 15 per mancato rilascio della dichiarazione di conformità).



FORMAZIONE PER INSTALLATORI E PROGETTISTI

CORSI RICONOSCIUTI DI PREPARAZIONE ALLA
CERTIFICAZIONE CEI – TÜV ITALIA:

- **Norme CEI**
Sistemi antintrusione e antirapina
- **Norme CEI**
Sistemi di Videosorveglianza
- **Videosorveglianza e**
Privacy Corso Base
- **Obblighi, responsabilità civile**
e penale per gli operatori
del settore Sicurezza

Ethos Academy srl

academy@ethosacademy.it - www.ethosacademy.it

media partner

a&S ITALY
tecnologie e soluzioni per la sicurezza professionale

sec solution
security online magazine



info
corsi



info
certificazione

La centralità del cavo in un sistema di videosorveglianza

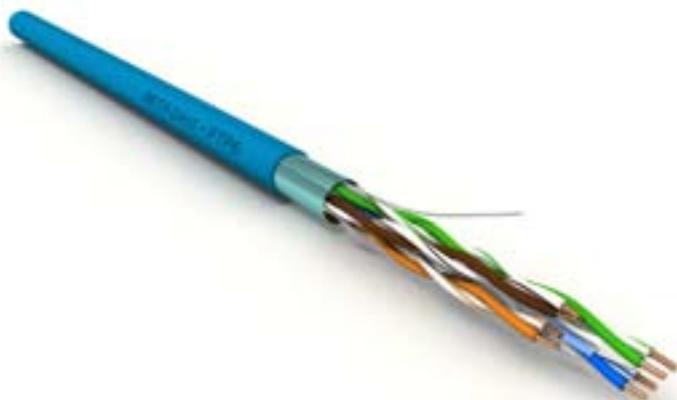
S spesso visto come un complemento secondario dell'impianto di videosorveglianza a cui non viene riconosciuta la corretta importanza, il cavo rappresenta invece la linea di interconnessione di tutte le apparecchiature sulla quale transitano informazioni e segnali video. Immagini sfuocate, perdita di dettagli, ombre sui bordi e presenza di disturbi sono solo alcuni dei fenomeni che possono essere direttamente correlati alla tipologia del cavo impiegato, e che invece molto spesso sono essere attribuiti esclusivamente alla qualità dei dispositivi installati. Risulta quindi essenziale operare delle scelte oculate dando la giusta importanza all'elemento di connessione del sistema, soprattutto a fronte dell'evoluzione tecnologica raggiunta grazie ai cavi HD 8035 e HD 14055.

UN CASO PRATICO

Presentiamo il caso pratico del rifacimento del sistema di videosorveglianza di uno dei carceri più grandi (in termini di personale recluso e di estensione su-

perficiale) a livello nazionale. In considerazione dell'elevato rischio del sito e dell'elevato livello di sicurezza richiesto per tutelare sia detenuti che personale interno, nonché per controllare luoghi di aggregazione comune e varchi di accesso, si è deciso di rinnovare l'intero impianto di videosorveglianza mediante l'impiego di telecamere di nuova generazione HD-TVI nelle aree sensibili, e di telecamere IP con risoluzione 4K per alcune aree sensibili dove non era richiesto il vincolo del real time, ma era comunque indispensabile disporre di immagini in alta definizione a scopo di indagine. La decisione dello staff di progettazione di accostare queste due tecnologie risiede nelle considerazioni che seguono.

1) Le telecamere HD-TVI permettevano la visualizzazione di immagini 3Mpixel in tempo reale, garantendo una qualità d'immagine superiore,



in grado di permettere l'identificazione di qualsiasi particolare in un'eventuale scena sospetta; 2) le telecamere IP 4K fornivano immagini di elevata qualità in tutti i siti dove sussisteva l'esigenza di avere immagini in alta risoluzione ma non necessariamente in tempo reale. L'intera gestione dei due flussi video fu quindi affidata ad un videoregistratore ibrido in grado di gestire contemporaneamente segnali IP4K e HD-TVI.

L'équipe di progettazione decise di impiegare linee di interconnessione appositamente sviluppate per applicazioni di videosorveglianza, quali: linee analogiche per alta definizione cavi HD8035 e cavi HD14055 di BETA CAVI e linee dell'infrastruttura di rete con cavi HDIP 3220.

La fase di riprogettazione dell'architettura del sistema poté così sfruttare distanze utili decisamente superiori rispetto ai vecchi RG59 (fino a 400m in HD-TVI3Mpixel con un cavo di soli 3,3 mm o 800m con un cavo di 5,0mm e fino a 220m di tratta diretta tra videoregistratore e switch e switch e telecamera Ip con PoE), semplificando l'architettura dell'intero sistema.

Da un punto di vista tecnico l'impiego di un cavo con Guaina in Duraflam® LSZH garantiva poi l'idoneità alla posa sia in esterno che in interno, eliminando una serie di problematiche, dovute alle escursioni termiche e alla presenza di umidità e raggi UV, che la guaina o la doppia guaina in PVC non prevenivano a causa della loro composizione molecolare, che non assicura un corretto isolamento del conduttore dalle particelle d'acqua. Inoltre la conformità dei cavi alla normativa CEI UNEL 36762, che ha eliminato in maniera definitiva il concetto di grado, frutto di un retaggio storico errato, ne garantisce l'impiego in coesistenza a cavi di energia (es: 230V, 400V).

SCELTA DEL CAVO E VALORE AGGIUNTO

Nella progettazione del nuovo sistema di videosorveglianza, il cavo è risultato fondamentale, in quanto mezzo di connessione dell'intero sistema. Le sue caratteristiche innovative hanno garantito una trasmissione eccellente del segnale video, mantenendo inalterate le performance degli apparati utilizzati anche su distanze ad oggi considerate irraggiungibili. Questo dimostra che la scelta di BETA CAVI di distinguersi nella realizzazione di un cavo, prestando molta attenzione alle caratteristiche trasmissive e alle caratteristiche tecniche richieste



dai più importanti produttori di sistemi di videosorveglianza, è stata vincente. Pensare che ci sia un'evoluzione tecnologica solo sui sistemi e non sul mezzo di connessione sarebbe infatti come pensare di utilizzare un'automobile da corsa di ultima generazione su una strada sterrata. Le due evoluzioni devono per forza avanzare di pari passo affinché una non comprometta il naturale sviluppo dell'altra.

IN BREVE

Location dell'installazione: uno dei più grandi carceri italiani

Tipologia di installazione: videosorveglianza HD-TVI nelle aree sensibili e telecamere IP 4K per alcune aree ove non era richiesto il real time

Ragioni della scelta del componente: il cavo è stato fondamentale per mantenere le performance delle telecamere

Tratti salienti del componente: distanze utili superiori rispetto ai vecchi RG59, idoneità alla posa sia in esterno che in interno

Brand dei componenti: cavi HD4019, HD8035, HD 14055 e HDIP3220 di Beta Cavi
www.betacavi.com



International Security Conference & Exhibition

CCIB
Centro de Convenciones
Internacional de Barcelona

17 e 18 de maggio
BCN2017



VEDERE PER **CREARE**

#SFBCN2017

 www.securityforum.es

 info@securityforum.es

 +34 914 768 000

 @SecurityForumES

 **Peldaño**



PILLOLE FORMATIVE

DI APPROFONDIMENTO



**Pillole di
approfondimento
valide anche ai fini
del mantenimento
della Certificazione
CEI - TÜV Italia
per n. 3 crediti**

EXCLUSIVE EXPERIENCE STORE
VIA ORAZIO 136 B • NAPOLI

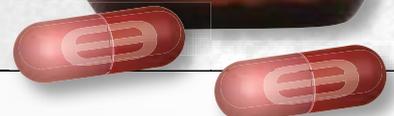
Venerdì **9 Giugno** **VIDEOSORVEGLIANZA E PRIVACY**
"Con l'arrivo del nuovo regolamento Europeo, cosa sapere e cosa fare"

Venerdì **15 Settembre** **ANALISI E VALUTAZIONE DEL RISCHIO**
"La progettazione di un impianto di allarme deve essere coerente con il rischio di attacco ai locali protetti, aspetti e fattori da considerare" - rif. Norma CEI 79-3

Venerdì **20 Ottobre** **PROTEZIONI PERIMETRALI - SCELTE E DIFFERENZE**
"Sempre più richiesta dal cliente ma la progettazione e installazione richiedono specifica attenzione e competenza: le Protezioni Perimetrali"

Venerdì **10 Novembre** **DM 37/08 - COMPILAZIONE ED OBBLIGHI**
"Il DM n. 37/08: adempimenti tecnici e responsabilità dell'installatore di sistemi di sicurezza"

Venerdì **15 Dicembre** **CALCOLO LIVELLI PRESTAZIONE IMPIANTI DI ALLARME**
"Prestazione impianti di allarme: classificazione, calcolo livelli di rischio e metodi" - rif. Norma CEI 79-3



Ethos Academy srl

Via Caduti di Amola, 31 - 40132 Bologna (Italy) - Tel. +39 051 0475136 - Fax +39 039 3305841
academy@ethosacademy.it - www.ethosacademy.it

La Redazione

Bonus sicurezza: al via il canale telematico per la dichiarazione precompilata

Dal 18 aprile è aperto il canale telematico di accesso ai dati della dichiarazione precompilata 2017: resterà attivo fino al 24 luglio (ultimo giorno per presentare il modello tramite web app. In autunno saranno comunque possibili correzioni e integrazioni attraverso Caf e intermediari abilitati). Tra le tante novità, debuttano nel 730 precompilato le spese sostenute nel 2016 per l'installazione di sistemi di videosorveglianza digitale o di sistemi di allarme o connesse ai contratti stipulati con istituti di vigilanza privata. Per queste spese, volte a prevenire atti criminosi, è riconosciuto un credito d'imposta nella misura del 100%.

Ma come si accede alla dichiarazione precompilata? Occorre possedere le credenziali Fisconline o Entratel, oppure quelle rilasciate dall'Inps con il Pin dispositivo o dal Portale della pubblica amministrazione (NoiPa), o con il Sistema pubblico dell'identità digitale (Spid) o con la Carta nazionale dei servizi (Cns). E attenzione: la nuova dichiarazione presenta numerose novità sia nella formulazione precompilata che nella versione ordinaria e lascia spazio per nuove deduzioni e detrazioni d'imposta e anche per l'integrazione delle dichiarazioni degli anni passati.

LIMITI E MODALITÀ

Ricordiamo che dal 20 febbraio al 30 marzo scorsi era possibile inviare le domande relative al bonus fiscale per l'acquisto di sistemi di videosorveglianza, allarme e relativi contratti con istituti di Vigilanza Privata. I criteri e le procedure per fruire del credito d'imposta, introdotto dalla legge di Stabilità 2016 e relativo alle spese per la sicurezza affrontate dai privati nell'anno passato, erano reperibili nel decreto del ministero dell'Economia del 6 dicembre 2016: bastava collegarsi al sito delle Entrate ed inviare la richiesta (anche tramite intermediario) usando il software "Creditovideosorveglianza".

ENTITÀ DEL BONUS

Nella domanda andavano indicati: codice fiscale del beneficiario e del fornitore del bene o servizio, numero, data e importo delle fatture (Iva inclusa), precisando se erano relative a un immobile "promiscuo", cioè ad uso abitativo/professionale. In quest'ultimo caso, si rammenta che il credito spettava solo nella misura del 50%. L'Agenzia delle Entrate ha specificato che si poteva presentare una sola richiesta, comprensiva dei dati di tutte le spese sostenute nel 2016: in caso di presentazione di più domande, sarebbe stata ritenuta valida soltanto l'ultima (quindi era più conveniente presentare per ultima la richiesta relativa alle spese più onerose).

Il credito d'imposta, indicato nella dichiarazione dei redditi relativa al 2016, è utilizzabile in compensazione, a mezzo modello F24, tramite i servizi telematici delle Entrate. Le persone fisiche non titolari di redditi d'impresa o di lavoro autonomo possono utilizzare il credito spettante anche in diminuzione dalle imposte dovute in base alla dichiarazione dei redditi.



B2B

IEH!

ITALIAN ELECTRONICS HUB

E' nata una **nuova** realtà distributiva esclusiva.

OPTONICA LED

www.optonicaled.com

PRASTEL

www.prastel.com

CAME art

<http://www.came.com/artcollection/>

Fondata da un gruppo di **professionisti** con esperienza tecnica e commerciale consolidata da quasi **30 anni di attività** è attiva nei settori **illuminotecnica, sicurezza e automazione.**

Italian Electronics Hub
Sede operativa: via San Silvestro 166/168 | 48018 Faenza (RA)
Tel. 0546 061091

info@iehsrl.it www.iehsrl.it

Global Offshore Technology

Innovation Conference

1st-2nd June
Amsterdam
Netherlands
2017

“Bringing underwater treasures to the surface”

Offshore Exploration & Production Technology

- Strategies for managing major off-shore projects
- Mitigating risks involved in E&P Projects
- Improved Oil & Gas Discovery and Recovery Methods (IOR/ EOR)
- Production Optimization and Real Time Monitoring
- Managing mature offshore fields

Offshore Engineering Technology

- Innovation in Offshore Production Technology
- Techniques for improving drilling accuracy
- Discussing the evolution of directional and horizontal drilling
- Challenges of different types of drilling activities in ultra – deep fields
- Making drilling platforms and pipeline infrastructure smart

Offshore Assets Management & HSE

- Reservoir monitoring and production optimization
- Asset Management and Operational Excellence Strategies
- Measures for preventing undesired shutdowns
- Evolving from “information revolution” into a “knowledge revolution”
- Achieving safe and efficient Platforms.
- Designing systems to avoid human error consequences

20+
Speakers

100+
Companies

120+
Attendees

250+
Business
Meetings

Register Now for OTIC 2017

centrica

Digital Energy
Technology
Services Pvt.Ltd.



GOODREEB COMPANY LIMITED



Lundin
Petroleum

MOLGROUP



مستشارية النخيل الوطنية
NATIONAL DRILLING COMPANY

OMV
OMV





FORMAZIONE PER INSTALLATORI E PROGETTISTI

CORSI RICONOSCIUTI DI PREPARAZIONE ALLA CERTIFICAZIONE CEI – TÜV ITALIA:

- Norme CEI Sistemi antintrusione e antirapina
 - Norme CEI Sistemi di Videosorveglianza
 - Videosorveglianza e Privacy Corso Base
 - Obblighi, responsabilità civile e penale per gli operatori del settore Sicurezza
-

BARI • 25 MAGGIO 2017

THE NICOLAUS HOTEL – VIA CARDINALE A. CIASCA, 27 – BARI

Ethos Academy srl

academy@ethosacademy.it - www.ethosacademy.it

media partner



secsolution
security online magazine



info
corsi



info
certificazione

Nuovo sistema wireless: integrazione bidirezionale supervisionata

I know-how acquisito nel tempo da Tecnoalarm e l'alto livello tecnologico raggiunto, consentono oggi, all'Azienda torinese, di annunciare l'uscita della nuova gamma wireless bidirezionale supervisionata a doppia banda di frequenza. I dispositivi wireless Tecnoalarm si integrano ai sistemi antintrusione in modo organico e completo, consentendo la realizzazione di efficaci soluzioni di protezione, capaci di combinare semplicità di installazione ed alti standard di sicurezza.

IL NUOVO PROTOCOLLO SYNC@BWL: DOPPIA BANDA BIDIREZIONALE SUPERVISIONATA

Il protocollo di comunicazione controlla i dispositivi della nuova famiglia di periferiche "500 BWL". Le sue caratteristiche esclusive, di assoluto rilievo, lo contraddistinguono da ogni altra soluzione attualmente disponibile: il Sistema utilizza indifferentemente in rice-trasmissione due bande di frequenza 433MHz ed 868MHz, il che garantisce la certezza dell'informazione, offrendo un alto livello di sicurezza. I canali sono delimitati da



intervalli di guardia che eliminano i rischi di interferenza tra canali contigui. In aggiunta, la modulazione digitale FSK irrobustisce il protocollo in presenza di forti interferenze radio. Il protocollo consente di utilizzare da 1 fino a 16 canali per banda con sintonizzazione automatica, cinque tipologie di modulazione digitale, potenza di trasmissione RF autoregolata e doppio livello di crittografia, per il massimo livello di sicurezza.

IL SISTEMA: MODULARITÀ

Il cuore del Sistema è costituito da un coordinatore a cui è affidato il compito di gestire i Nodi di rilevazione, attuazione e comando. Il coordi-

natore supervisiona la rete, conserva e allinea il database con la centrale, infine mappa le tabelle di routing. Il numero di dispositivi gestibili dai Sistemi e le proporzioni numeriche dei nodi gestibili dal coordinatore sono modulari: l'aumento dei nodi sirena decrementa il numero dei nodi sensore e radiocomando. L'apprendimento dei nodi può essere effettuato in pochissimi secondi nelle immediate vicinanze del coordinatore o in loco.

La gamma è composta, oltre che dall'elemento principale rappresentato dal coordinatore, da altre periferiche, come il trasmettitore multifunzione, che gestisce, oltre al classico contatto, anche il conteggio tapparella e il filtro inerziale. Inoltre, sono disponibili il rivelatore ad infrarosso passivo per interni con diverse tipologie di copertura e il rivelatore perimetrale infrarosso che oltre rilevare tentativi di penetrazione può assumere la funzione contatto, tapparella o inerziale. Inoltre, i rivelatori per la protezione volumetrica esterna, con funzione di anti-mascheramento attivo. Il componente ottico-acustico, la sirena autoalimentata per esterni, incorpora tutte le funzioni e regolazioni presenti nella sirena filare. Ultimo componente, non meno importante, è il radiocomando innovativo e personalizzabile con sei tasti programmabili secondo le esigenze del cliente.

SINCRONISMO ANTICOLLISIONE E INTERFERENZE RIDOTTE AL MINIMO

Grazie alla sintonia automatica, il coordinatore esercita un controllo continuo sui canali disponibili che individua ed utilizza, per ognuna delle due bande di frequenza, il canale meno affetto da disturbi. Questa funzione consente di raggiungere impareggiabili livelli di immunità ai disturbi, anche di natura indotta. Il rischio di collisioni tra i diversi dispositivi diventa prossimo a zero, grazie alle caratteristiche del protocollo che utilizza una trasmissione sincronizzata che interroga i nodi del Sistema in sequenza, in base a precisi time-slot temporali.

DOPPIA CHIAVE DI CRITTOGRAFIA: ALTISSIMA SICUREZZA

I dispositivi sono gestiti con una doppia chiave di crittografia che consente di far convivere Sistemi adiacenti che condividono la stessa banda e lo stesso canale senza che si verifichino delle interferenze. Il protocollo, particolarmente selettivo, aumenta l'immunità al mascheramento.

POTENZA DI TRASMISSIONE RF

Mentre la potenza di trasmissione RF del coordinatore è fissa per ognuna delle due bande di frequenza, quella dei nodi si autoregola dinamicamente secondo un algoritmo che tiene conto della programmazione RF del coordinatore, delle condizioni climatiche e di propagazione rilevate nel sito protetto. Ciò consente una portata media in campo aperto che può variare da circa 600 a 1500 metri.

GESTIONE INTELLIGENTE DEGLI ASSORBIMENTI

Il consumo energetico è un aspetto fondamentale che non è stato tralasciato: grazie ad una ricca fase di ricerca, si è giunti a consumi estremamente ridotti per una lunga autonomia di servizio.

DIAGNOSTICA E PROGRAMMAZIONE DEI COMPONENTI DA PC

Oltre ad effettuare analisi funzionali come il "Test ricezione", il "Test zone" ed il "Test di collegamento", che esaminano in pochi secondi la qualità della trasmissione e la presenza dei componenti del Sistema, Tecnoalarm, grazie alla tecnologia RSC® (Remote Sensitivity Control) offre all'Installatore la possibilità di gestire tutti i parametri di regolazione e configurazione, anche da remoto.

La nuova gamma wireless evolve e completa la vasta gamma di prodotti Tecnoalarm, tecnologicamente avanzati, modulari e caratterizzati dalla prestigiosa firma di Pininfarina. Un altro importante passo avanti per l'Azienda torinese che quest'anno celebra il suo 40° anniversario di attività.

Tecnoalarm
Via Ciriè, 38
10099 San Mauro Torinese (TO)
Tel. +39 011 2235410
Fax +39 011 2735590
info@tecnoalarm.com
www.tecnoalarm.com

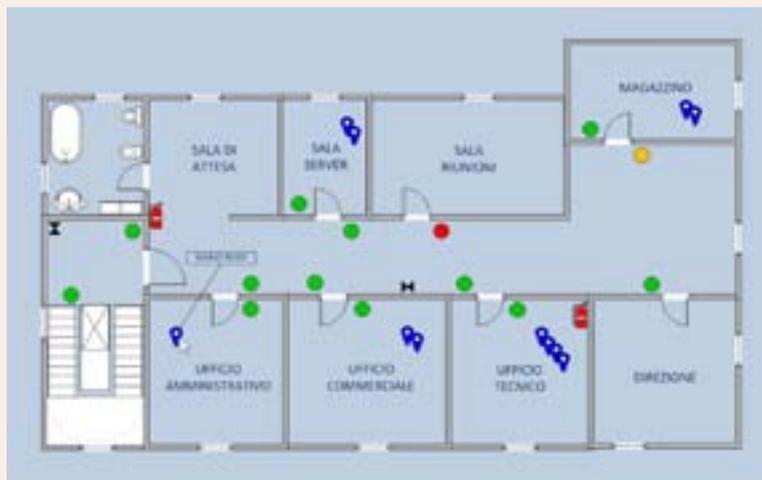
Piccoli e medi impianti: software per controllo accessi

È l'ultimo nato di una nota famiglia di software per controllo accessi. Si chiama Censor®, come il capostipite al lavoro in Italia da circa trenta anni anche se, ancora prima di venire alla luce, gli è stato affibbiato il nomignolo di "nano". Nano perché destinato a gestire sistemi di piccole e medie dimensioni: cinquecento utenti e cinquanta varchi controllati (uni o bidirezionali). Piccolo ma orientato a un mercato molto vasto, considerando le dimensioni delle imprese italiane potenzialmente interessate.

Censor® Nano è sviluppato, venduto e assistito dalla Elex srl di Torino, da tre decenni con le mani in pasta nei sistemi elettronici di controllo accessi, hardware e software, e con un'esperienza maturata nel settore che risale ai primi anni Settanta del secolo scorso.

SEMPLICE E FLESSIBILE

Il primo punto di forza del prodotto è la semplicità, intesa sia come facilità d'uso da parte dell'operatore sia come rapidità d'installazione, configurazione e messa in servizio a cura dell'impiantista.



Uno dei punti di forza del software Elex Censor® Nano è l'interfaccia uomo-macchina la quale si avvale di una grafica molto intuitiva e largo uso delle planimetrie

Censor® Nano ha un'interfaccia uomo-macchina molto evoluta che consente, anche a chi non si è ancora cimentato con il controllo accessi, di apprenderlo in brevissimo tempo e instaurare una immediata familiarità. La facilità d'uso è stata la stella cometa che ha guidato i progettisti durante il lungo cammino impiegato per ideare e sviluppare il prodotto. La seconda caratteristica distintiva è la modularità. Censor® Nano può essere installato su un personal computer (dedicato o adoperato anche per altre attività) che funge da stazione di lavoro oppure su un Server (reale o virtuale) e una o più workstation connesse in rete. L'ambiente di lavoro è Microsoft Windows, il database relazionale SQL express. L'applicazione, tuttavia, dà il meglio di sé nella versione web. Il sistema, infatti, può essere gestito via Internet o Intranet attraverso qualunque strumento di

lavoro personale (PC fisso o portatile, tablet, smartphone ecc.). Nella versione web sono disponibili numerose funzionalità che rendono ancora più immediato e agevole l'uso e la manutenzione dell'impianto, anche da remoto.

POTENTE PER DAVVERO

Un altro aspetto che contraddistingue Censor® Nano è la sua potenza. Piccolo sì ma completo e potente nelle prestazioni. Tutte le funzionalità tipiche di questa classe di software disponibile sul mercato italiano ed estero sono state implementate, compresa la registrazione e la gestione dei visitatori. Non solo. Il prodotto sfrutta le enormi potenzialità offerte dalla nuova linea di Controller per accessi Elex Idris®, unità elettroniche di ultima generazione, polivalenti e multivarco. Questi Controller – che, abbinati ai lettori e ai dispositivi input/output dei varchi, costituiscono le braccia operative del software – oltre alla classica funzione di aprire la porta a riconoscimento avvenuto e diritti di accesso verificati, sono in grado di gestire ben trentasei funzioni supplementari. Si va dalle più conosciute come il controllo passo-passo del transito attraverso il varco o l'anti pass-back (logico e temporale) alle meno note e sofisticate quali la possibilità di schedare differenti credenziali di accesso sullo stesso varco (ad esempio: di giorno si usa il badge, di notte e festivi il badge abbinato al PIN), il controllo della defluenza (il sistema non apre a un utente che sta per abbandonare un locale se nello stesso non resta un numero minimo di persone), il sorteggio all'uscita per le ispezioni corporali e così via.

UNO STRUMENTO PER L'RSPP

Censor® Nano nasce sotto il segno della sicurezza, non solo nel senso tradizionale del termine (nel caso specifico quello di regolare gli accessi agli edifici e alle aree interne riservate) ma anche intesa come prevenzione e protezione dei lavoratori nei luoghi di lavoro (d. lgs. 81/2008). Installando strutture fisiche adeguate e adottando procedure appropriate, infatti, il datore di lavoro o il responsabile della sicurezza (RSPP), può disporre di un formidabile strumento sia per far rispettare le regole di accesso a determinati luoghi che possono comportare rischi per la salute sia in caso di evacuazione ed emergenza. Tanto per fare due esempi: in



Elex Censor® Nano offre un dashboard attraverso cui è possibile tenere sotto controllo gli accessi nell'ambito di un edificio

qualsiasi momento è possibile conoscere chi è presente in azienda (funzione "Chicè") oppure localizzare uno o più utenti ("Dové"). Nella versione web, tutto questo avviene in modo grafico e interattivo attraverso l'integrazione di planimetrie relative ai vari edifici, ali, piani, zone, ambienti ecc.

SOLUZIONE MADE IN ITALY

In fatto di sistemi di controllo accessi basati su badge, transponder o impronte biometriche, l'Italia è agli ultimi posti in Europa ma le aziende e le organizzazioni che ne fanno uso, spesso hanno esigenze molto particolari che gran parte dei prodotti in commercio non sono in grado di soddisfare. Censor® Nano nasce dall'esperienza maturata in campo da Elex a stretto contatto con una clientela molto eterogenea, esigente e diffusa in tutto il Paese. È anche grazie alla loro collaborazione che è stato possibile mettere a punto una soluzione completa, potente, economica e in grado di dare una risposta efficace quando la protezione del patrimonio e delle persone non è solo una questione di facciata.

Elex
Corso Moncalieri, 77
10133 Torino
Tel. +39 011 6601822 (r.a.)
Fax +39 011 6601700
commerciale@elex.it
www.elex.it

Centrali per la sicurezza industriale e residenziale

La gamma UTC distribuita da HESA si compone di una vasta proposta di prodotti e soluzioni complete per il settore della sicurezza. Al suo interno si distinguono per l'alta affidabilità, la semplicità di installazione, manutenzione e gestione e le elevate prestazioni, la centrale XGEN e la centrale ZeroWire.

PER L'INDUSTRIA

La serie XGEN nasce su barra DIN e rappresenta un'ottima scelta per la sicurezza in ambito industriale. Offre funzioni avanzate di gestione utente che possono essere collegate a pianificazioni complesse e ad eventi di automazione anche con l'integrazione di telecamere IP per video verifica. Le opzioni utente, le uscite e anche le zone possono comportarsi in modo diverso e cambiare in tempo reale a seconda delle condizioni di sistema specificate per il progetto. La serie XGEN è caratterizzata da quattro differenti modelli, di cui tre con scheda di rete IP, che vanno a soddisfare le più svariate esigenze di protezione. In particolare si evidenziano alcune centrali



dalle caratteristiche estremamente avanzate: la centrale NXG-64IP, da 8 a 64 zone, 16 aree e 64 uscite da 100 utenti. La centrale NXG-256IP da 8 a 256 zone, 32 aree e 256 uscite da 256 utenti. E infine la centrale NXG-512IP, da 8 a 512 zone, 96 aree e 256 uscite da 256 utenti. Tutte e tre le centrali sono in grado di offrire una gestione avanzata dell'automazione e comunicazione tramite IP, GPRS, e-mail e notifiche push e dispongono della tastiera touch NXG-1820-EUR, che consente un facile accesso a tutte le funzioni utente e ai comandi di sistema. Sia i comandi di menu per l'utente, sia i messaggi di sistema vengono visualizzati con testo in chiaro su uno schermo da 3,5". Inoltre l'app consente all'utente di comandare il sistema XGEN da iPhone/iPad o da dispositivo Android, e permette all'installatore di eseguire in modo facile e veloce

sia programmazioni di base sia programmazioni avanzate del sistema. Tra le caratteristiche più rilevanti: 8 zone a bordo; massimo 32 dispositivi (espansioni e tastiere); integrazione con telecamere IP, per la visualizzazione di video in diretta e la riproduzione di eventi video di allarmi catturati o attivati da azioni; ingresso manomissione principale e secondaria; 5 uscite programmabili a bordo; programmazioni di uscite e scenari; porta Ethernet 10/100 integrata (RJ-45); connessione a cloud; modem cellulare opzionale progettato per un'installazione rapida.

PER LA CASA

La ZeroWire è una centrale senza fili con browser web integrato ideale per la protezione in ambito residenziale. La centrale dispone di 64 zone (di cui 4 possono essere cablate) di rilevazione intrusioni e di protezione dal rischio incendio e fughe di gas, e di 4 aree per la protezione separata di più ambienti di una stessa proprietà. ZeroWire si distingue per le funzionalità altamente innovative, quali l'integrazione con telecamere IP per video verifica, il collegamento e la gestione del sistema tramite la nuova applicazione mobile "UltraSync" con funzioni cloud avanzate, disponibile per dispositivi iOS e Android, e infine l'automazione domotica tramite il protocollo Zwave. Un Wi-Fi radio integrato per le segnalazioni di allarme e i servizi interattivi consente la massima flessibilità nel posizionamento della centrale, in qualsiasi punto dove un router senza fili possa ricevere un segnale. Quando è installata in un'area comune, le funzioni della centrale sono facilmente gestibili utilizzando la tastiera LED integrata con un menù vocale per una grande semplicità di installazione e di funzionamento. In aree poco frequentate la centrale può operare come un centro di controllo di sicurezza, in modo che l'applicazione mobile, disponibile per smartphone e tablet, possa funzionare come metodo principale di controllo. ZeroWire è anche dotata di sirene da esterno e da interno bidirezionali, ed è disponibile nella versione certificata EN50131-2 se abbinata alla nuova gamma di trasmettitori a 433 MHz a 80-bit. La centrale può essere collegata alla rete Internet tramite cavo IP o Wi-Fi, ZeroWire garantisce inoltre la massima libertà di scelta grazie al modulo 3G disponibile in due versioni: la ZW-7001 compatibile con i maggiori gestori telefonici e quindi in grado di garantire la massima qualità del segnale scegliendo il gestore più performante per il luogo dell'installazione,



e la ZW-7000 con scheda SIM del produttore soggetta a canone mensile. La centrale ZeroWire è compatibile con tutti i sensori via radio appartenenti alla gamma di UTC a 433 MHz, oltre che ad alcuni tra i dispositivi più performanti oggi presenti sul mercato, resi disponibili da HESA già assemblati con i trasmettitori. Molto apprezzata è la telecamera TVW-1121 Wi-Fi con 3 Megapixel 1/3", H.264, D&N meccanico, ottica fissa 2.8mm, Led IR, SD, IP66, 12Vc.c.

Tra le caratteristiche più rilevanti: 64 utenti; 25 telecomandi; porta Ethernet 10/100 integrata (RJ-45); integrazione con telecamere IP, per la visualizzazione di video in diretta e la riproduzione di eventi video di allarmi catturati o attivati da azioni; pulsante di stato a colori per una facile identificazione visiva dello stato del sistema; nomi di zona registrati vocalmente e messaggi per il ritardo di entrata/uscita; connessione a cloud; modem cellulare opzionale progettato per un'installazione rapida; 2 uscite (ciascuna da 100mA); 4 aree; nomi di zona registrati vocalmente e messaggi per il ritardo di entrata/uscita; design compatto, a basso profilo, ideale per installazioni con fissaggio a parete o da tavolo.

HESA
Via Triboniano 25
20156 Milano MI
Tel. (+39) 02 380361
Fax (+39) 02 38036701
info@hesa.com
www.hesa.com

Più di un sistema d'allarme: sicurezza e comfort

Se si possiede un'attività, la sicurezza dell'esercizio dovrebbe essere all'ordine del giorno. Ma la sicurezza non è tutto: l'utente vuole infatti anche tenere il sistema sotto controllo e farlo con semplicità, ovunque si trovi. JABLOTRON 100 offre una vasta gamma di opzioni di sicurezza e funzioni intelligenti. Può essere installato ed esteso in sistemi filari o wireless, che consentono l'installazione in interni riducendo i costi. Oltre alla protezione contro intrusioni, è possibile aggiungere vari rilevatori che avvisano di eventuali incendi o allagamenti, ma anche di una temperatura elevata nella camera o di un eccessivo consumo di energia elettrica. È possibile attivare l'automazione del garage lampeggiando i fari dell'auto o spegnere le luci dopo aver inserito l'allarme. Possono essere impostati, per i singoli utenti, dei diritti di accesso per una particolare attività o anche per alcune parti di accesso dell'azienda. È possibile controllare tutte le funzioni in remoto da qualsiasi luogo con l'APP MyJABLOTRON mobile e applicazione web, che è parte integrante del sistema JABLOTRON 100. Si otterrà



quindi un controllo costante di ciò che accade in azienda (si vedranno foto dei rivelatori, si controlleranno il posto di lavoro, le funzioni di automazione o il consumo di energia elettrica e si potranno ricevere notifiche in caso di evento, es. incendio).

SICUREZZA IN AZIENDA

L'immagine più sopra rappresenta una piccola azienda in un edificio dove si vogliono proteggere gli uffici e le aree comuni. Questa installazione è focalizzata sulla sicurezza contro furto e incendio, quindi comprende essenzialmente la protezione da parte di rilevatori di movimento e di

fumo. La base del sistema è una centrale che valuta le informazioni dei rivelatori e reagisce alle richieste degli utenti. L'installazione può essere filare, wireless o in combinazione e si estende fino a 15 diverse sezioni. La sicurezza dell'azienda è quindi molto flessibile: è possibile collegare fino a 120 dispositivi aggiuntivi e assegnare fino a 300 codici utente. Le impostazioni desiderate e le dimensioni del sistema sono programmati da un software F-Link. La centrale ha combinatori GSM/GPRS e LAN integrati che consentono l'invio di messaggi vocali, SMS e comunicazioni GPRS e LAN, con gli utenti finali o i centri ARC. È dotata di una scheda di memoria per l'archiviazione di eventi, messaggi vocali, immagini ecc

SEMPLICITÀ

Per controllare il sistema JABLOTRON 100 è possibile utilizzare un modulo di accesso con segmenti di controllo per ogni sezione protetta della struttura. Il grande vantaggio è la semplicità del controllo, che non richiede complicate interazioni con la tastiera, e la possibilità di verificare a colpo d'occhio lo stato del sistema. L'utente preme semplicemente un pulsante per inserire o disinserire la sezione specifica e autorizza posizionando un tag RFID o digitando un codice. Ogni utente ha il suo tag o il codice in modo da identificare facilmente chi ha controllato il sistema e quando. Un'altra possibilità è un telecomando progettato per inserire o disinserire da remoto il sistema o per attivare un allarme panico. Il controllo è possibile anche con l'applicazione MyJABLOTRON. Il design dell'applicazione riflette una progettazione fisica dell'allarme tale per cui il controllo risulta intuitivo e semplice da utilizzare. L'applicazione consente agli utenti di interagire e di controllare il sistema di allarme ovunque e in qualsiasi momento.

RILEVATORI

Rilevatori e sirene sono parte integrante del sistema di allarme. Oltre ai sensori di movimento normali, i rilevatori con fotocamere di verifica sono adatti e utilizzati per la verifica visiva. Quando viene rilevato un movimento in un'area protetta, la fotocamera del rivelatore cattura un'immagine a colori. L'immagine può essere anche su richiesta, ad esempio per avere una conferma di allarme incendio. La fotocamera è dotata di un flash per la



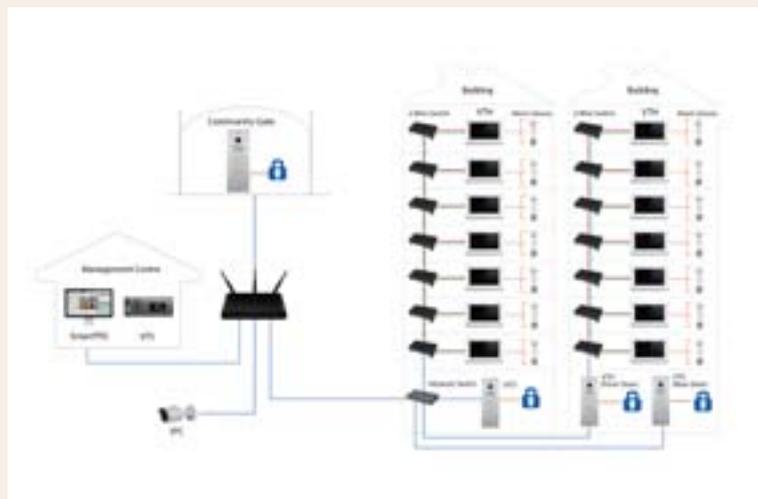
visualizzazione al buio. Gli utenti possono visualizzare le immagini con facilità nell'applicazione MyJABLOTRON. Per garantire la protezione perimetrale e ricevere quindi un allarme prima che un intruso entri nell'abitazione, è necessario installare rilevatori di apertura finestra o di rottura vetri. Il loro rilevamento si basa sulla doppia tecnologia (rilevamento di variazioni di pressione dell'aria accompagnati da un suono caratteristico di rottura del vetro), e la sensibilità è regolabile. Naturalmente, i sensori tapparella e i sensori esterni sono disponibili nel sistema JABLOTRON 100. Anche i rilevatori antincendio sono necessari nelle aziende. Essi combinano rilevatori di fumo e di temperatura e consentono varie impostazioni di rilevamento: fumo e innalzamento di temperatura, fumo o innalzamento di temperatura, solo fumo o solo innalzamento di temperatura.

JABLOTRON 100 è in sintesi più di un sistema di allarme. È in grado di controllare vari tipi di apparecchiature o elettrodomestici. Le attivazioni possono essere effettuate in modalità remota o impostato come un'azione automatica.

Jablotron
Pod Skalkou 4567/33
466 01 Jablonec nad Nisou
Repubblica Ceca
export@jablotron.cz
www.jablotron.it

Tutti i vantaggi della videocitofonia ibrida bifilare

I rapido evolversi della società richiede un innalzamento del livello tecnologico dei servizi a disposizione dei residenti in appartamenti: nel campo della videocitofonia ciò si traduce nella conversione dei sistemi analogici tradizionali in sistemi IP di ultima generazione. Questo ovviamente comporta anche un appesantimento delle infrastrutture esistenti, talvolta al punto di renderne necessario un laborioso e dispendioso ammodernamento. Seppur la tecnologia IP porti ad un nuovo livello la qualità del sistema di videocitofonia, quando si chiede al condominio di mettere mano al portafoglio, tutte queste spese di rado risultano poi essere ancora giustificate. Per non parlare delle difficoltà installative: qualsiasi installatore sarebbe felice al pensiero di vedere tra le proprie referenze gli impianti videocitofonici di importanti palazzi nei centri di grandi città, ma perderebbe il sonno conoscendo i problemi (moltiplicati per N appartamenti) ai quali si va incontro mettendo mano ad un impianto obsoleto.



VIDEOCITOFONIA IBRIDA BIFILARE

La risposta di Dahua a questa problematica è un sistema videocitofonico ibrido bifilare.

Questa tecnologia consente di trasportare il protocollo TCP/IP, oltre all'alimentazione per il dispositivo, su due fili, permettendo così di sfruttare i doppini dell'impianto citofonico esistente che già raggiungono gli appartamenti. Il sistema viene definito "ibrido" perché questa tecnologia, nel caso di un condominio, si applica solo ai posti interni, mentre è possibile usare come posti esterni i normali dispositivi IP Dahua serie VTO, che funzionano su cavo di rete.

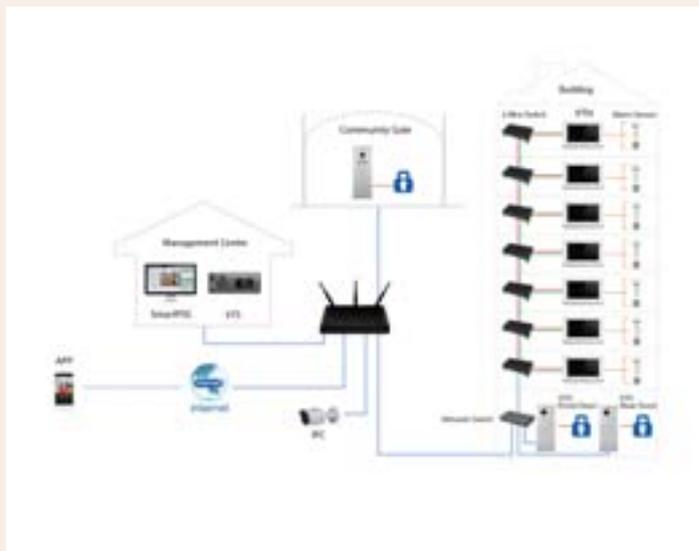
SWITCH BIFILARE E POSTO INTERNO

Fino a poco tempo fa la tecnologia IP bifilare limitava l'estensione dell'impianto a quattro dispositivi tra posto esterno monotasto VTO2000A-2 e display VTH1550CHW-2, utile per soddisfare le esigenze di una villa. Il discorso cambia quando l'ammodernamento di cui sopra riguarda un intero palazzo, dove la quantità di unità abitative raggiunge velocemente anche numeri a tre cifre. È qui che Dahua interviene introducendo a catalogo dei nuovi prodotti, le cui differenze rispetto a quelli appena menzionati, seppur piccole, ampliano notevolmente le potenzialità di questa soluzione.

Lo switch VTNS1006A-2 dispone di sei porte bifilari: vi si possono connettere quindi fino a sei posti interni VTH5222CH e anche due porte bifilari per la connessione di più switch in cascata, fino ad un massimo di trenta unità, ed una porta ethernet per la connessione con il resto della rete e quindi ai posti esterni. Come abbiamo detto, i due fili trasportano dati e alimentazione: lo switch andrà quindi alimentato da un alimentatore 24 VDC. Il sistema può prevedere fino a 20 posti esterni serie VTO e fino a 1000 posti interni.

I PLUS

Oltre al semplice sistema di cablaggio tipico di questi dispositivi, i vantaggi del passaggio dalla tecnologia analogica all'IP sono molteplici. Il primo è rappresentato dalle *Notifiche Push*: tramite l'App DMSS disponibile sugli store Apple e Android, gli utenti saranno in grado di ricevere la chiamata direttamente sullo smartphone, avviare la comunicazione bidirezionale audio/video ed aprire all'ospite. Un altro vantaggio è la *gestione intelligente centralizzata*: l'intero sistema, per quanto esteso, può essere supervisionato e gestito da un'unica postazione PC client grazie a SmartPSS 1.16, il software Dahua di centralizzazione che consente ad esempio di ricevere le chiamate in orari prestabiliti, di comunicare audio/video con tutti i dispositivi e di inviare messaggi sui display dei condomini. Un terzo plus è la *supervisione impianto TVCC*: la postazione interna VTH5222CH, seppur bifilare, si integra infatti perfettamente con il resto dei dispo-



sitivi IP di interesse presenti all'interno delle rete, come ad esempio un impianto TVCC preesistente, permettendo di visualizzare l'immagine live delle telecamere.

Questi sono solo alcuni dei vantaggi di cui Dahua permette di beneficiare nel campo della videocitofonia, portando su due fili quello che normalmente si trasporta su un cavo di rete.

Dahua Italy
Via Torri Bianche 9
Palazzo Quercia Int. 14
20871 Vimercate (MB)
sales.italy@global.dahuatech.com
www.dahuasecurity.com/it

Personal Tracker/APP per la sicurezza personale

La sicurezza, in tutte le sue espressioni, è diventata una delle priorità principali del nostro vivere quotidiano. Privacy e riservatezza, difesa della proprietà e integrità personale, soccorso e tranquillità sono esigenze da sempre fortemente sentite all'interno della nostra società. Sulla base di queste necessità SICEP ha iniziato, nel 1978, la sua attività di produzione dei primi dispositivi di allarme, entrando ufficialmente nel settore della sicurezza. Negli anni SICEP è cresciuta, si è profondamente specializzata ed è cambiata fino a diventare un importante punto di riferimento del mercato italiano.

PERSONAL TRACKER/APP

Tra gli ultimi nati di casa SICEP, il Personal Tracker/APP è un'applicazione per smartphone pensata per la sicurezza personale, come pure delle persone a noi più care e di tutte quelle categorie considerate ad alto rischio (donne, bambini, anziani, invalidi, lavoratori isolati, guardie giurate, imprenditori, rappresentanti, ecc. ecc.). In caso di pericolo



è possibile inviare, mediante la pressione di un apposito tasto o tramite scuotimento del dispositivo (anche con la funzione "uomo a terra"), una richiesta di aiuto ad una Centrale di Vigilanza con sistema gestionale MvsNET (SICEP) con le relative coordinate geografiche per garantire un tempestivo intervento di soccorso.

L'utilizzo della rete GSM DATI consente un trasferimento delle segnalazioni ad alta velocità, con costi di traffico contenuti ed un utilizzo su tutto il territorio senza limiti (in relazione alla copertura del gestore telefonico scelto). Ma addentriamoci nelle caratteristiche funzionali di Personal Tracker/APP di SICEP.

CARATTERISTICHE FUNZIONALI

- APP antiaggressione/soccorso con funzione GPS;
- rilevamento della posizione mediante GPS o triangolazione di celle;
- compatibilità con sistemi operativi iOS ed Android;
- utilizzo delle sue funzioni mediante connessione GSM Dati;
- invio di allarme, con pressione di un apposito tasto, di tipo istantaneo o ritardato (pre-allarme, programmabile in secondi);
- funzione uomo a terra impostabile (ritardo programmabile in secondi) – Solo Android;
- attivazione allarme su scuotimento (sensibilità settabile) e combinazione di tasti - Solo Android;
- invio della posizione/tracciamento su più modalità:
 - *mai*: non invia mai la posizione
 - *periodico*: invia la posizione a scansione di tempo
 - *su allarme*: invia la posizione con tracciamento continuo
 - *default*: invia una posizione pre-registrata;
- registrazione delle posizioni su un apposito storico (con data/ora, tipo di evento e posizione consultabile su mappa);
- disattivazione APP mediante opzione Privacy (sbloccabile su allarme);
- chiamata rapida verso un numero pre-impostato;
- possibilità, in caso di pericolo, di scattare foto ed inviarle in Centrale Operativa;
- menù locale con opzioni impostabili dall'utente;
- gestione pulsante di soccorso via Bluetooth;

MVSNET

Il Sistema MvsNET è stato progettato con un'architettura hardware e software ideata per creare un gestionale dalle elevate prestazioni, mantenendo ed incrementando i principi di multivettorialità, polifunzionalità e modularità. Il sistema è composto da una struttura Client/Server, con sistema operativo Linux, per archiviare, catalogare e proteggere i dati, e di uno o più PC/Client con sistemi operativi Microsoft Windows. Il Server MvsNET garantisce una maggiore stabilità ed affidabilità al gestionale, lasciando agli operatori la possibilità di accedere al sistema soltanto tramite i Client. Punti salienti del sistema: mantenuti i principi di multi-



vettorialità, polifunzionalità e modularità; sistema completamente telegestibile da remoto; struttura hardware dalle elevate prestazioni; architettura Client/Server nativa con sistema operativo Linux; gestione dei dati e delle segnalazioni sia localmente che da accessi remoti; possibilità di gestire dati e segnalazioni da varie sedi; 1.000.000 di eventi mese gestibili efficientemente; struttura gestionale arricchita da una serie di servizi integrati ed opzionali.

OPERATIVITÀ DELLA CENTRALE OPERATIVA SICEP MVSNET

- completa autoconfigurazione delle sue funzioni da Centrale Operativa;
- completa gestione della APP da Centrale Operativa:
 - ricezione segnalazione di allarme/soccorso
 - ricezione della posizione/tracciamento
 - ricezione soccorso "uomo a terra"
 - ricezione delle foto scattate
 - richiesta manuale della posizione (solo con Privacy OFF)
 - consultazione storico eventi;
- APP gestibile mediante attivazione di una Licenza su MvsNET in base al numero di dispositivi collegabili.

SICEP
 Via Calabria, 14
 50052 Certaldo (FI)
 Tel. (+39) 0571 664166
 Fax (+39) 0571 652285
 sicep@sicep.it
 www.sicep.it

Centrali di evacuazione vocale compatte e certificate

Comelit è presente da qualche anno sul mercato dei sistemi di rivelazione automatica di incendio con un'intera gamma di centrali, rivelatori, pulsanti, barriere lineari, sistemi di aspirazione, sistema wireless... Per offrire una gamma ancora più completa, è stata realizzata una nuova centrale compatta di evacuazione vocale.

I sistemi di evacuazione vocale stanno diventando sempre più un elemento essenziale nei sistemi antincendio. Guidare l'esodo con messaggi vocali personalizzati e focalizzati sulla tipologia di impianto, facilita le persone all'interno dell'edificio ad eseguire le procedure di evacuazione nel modo più fluido ed ordinato possibile. È stato dimostrato che una procedura di evacuazione guidata da messaggi vocali è molto più efficace rispetto ai tradizionali segnalatori acustici. Questi sistemi di evacuazione hanno la possibilità di emettere messaggi vocali preregistrati che vengono riprodotti durante l'evacuazione o l'allerta. Lo stesso sistema può essere poi utilizzato per diffondere la musica durante condi-

zioni normali dando sempre priorità, in caso di emergenza, a messaggi di evacuazione e allerta.

IL PRODOTTO PERFETTO

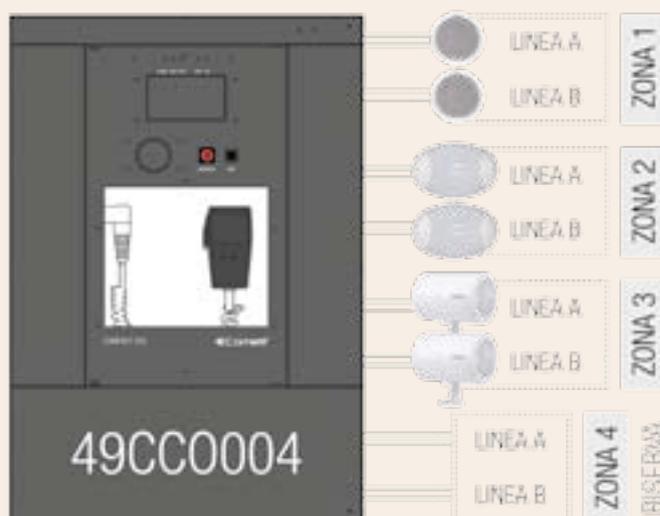
Le centrali di evacuazione vocale sono solitamente ingombranti ed antietiche, tuttavia sono un elemento cardinale negli impianti per i quali la



normativa ne obbliga l'utilizzo (ad esempio negli esercizi commerciali con superficie superiore a 400mq). Comelit ha trovato la soluzione che unisce prestazioni, ingombro ridotto e design in un solo piccolo, ma potente, sistema di evacuazione. Con una dimensione di 62 x 43 x 24 cm ed un peso estremamente ridotto, la centrale compatta di Comelit è installabile a parete ed è l'ideale per applicazioni in ambito terziario, istituti scolastici, strutture alberghiere, musei e molti altri luoghi. Il sistema EVAC compatto è facilmente interfacciabile con le centrali antincendio indirizzate Comelit. Nel caso di un evento di evacuazione generato dalla centrale antincendio, si avviano automaticamente i messaggi audio di allerta o evacuazione della centrale EVAC. È possibile inoltre ricevere la segnalazione di anomalia del sistema EVAC (batterie scariche o mancanza alimentazione) direttamente sulla centrale antincendio.

POTENZA E COLLEGAMENTO IN RETE

La centrale compatta di evacuazione Comelit è disponibile in 3 differenti versioni che si differenziano per il numero di zone audio gestite, 2, 4 o 6. Ognuna delle zone audio è dotata di doppia linea A e B di backup. La potenza audio totale gestibile è di 500W ripartibili liberamente sulle zone audio gestite con un massimo di 250W per ogni zona. Per un'ulteriore garanzia di continuità di funzionamento anche in caso di guasto di un amplificatore, è possibile impostare una delle zone audio come riserva senza dover aggiungere altri prodotti. Per impianti di dimensioni più importanti, è possibile collegare in rete tra loro fino a 6 centrali compatte per ottenere un impianto con 36 zone e 3000W di potenza totale. Nel momento in cui si renda necessario evacuare un edificio, è importante essere il più veloci ed efficienti possibile. Per questo le persone addette all'evacuazione potrebbero aver bisogno di inviare messaggi personalizzati direttamente da un microfono. A tal fine le centrali di evacuazione vocale Comelit sono tra le poche ad essere dotate di un microfono palmare VVF per l'invio di messaggi durante l'evento di evacuazione. È possibile gestire e visualizzare lo stato dell'impianto, attivare le procedure di evacuazione o inviare messaggi di allarme personalizzati anche da postazioni di emergenza remote con microfono incorporato. Per inviare messaggi di servizio (ad esempio per comunicazioni di servizio nei su-



permercati) sono disponibili le postazioni microfoniche con 6 o 12 pulsanti.

SICUREZZA ASSICURATA

Le centrali di evacuazione vocale compatte di Comelit Group sono certificate EN54-16 (norma di prodotto europea dedicata ai sistemi di rivelazione e segnalazione incendio nello specifico per apparecchiature di controllo e segnalazione per i sistemi di allarme vocale) e EN54-4 (per apparecchiature di alimentazione). I diffusori audio del sistema EVAC di Comelit sono tutti certificati EN 54-24, che è invece la norma europea dedicata appunto agli altoparlanti per sistemi di allarme vocale. Da sempre Comelit si è contraddistinta per affidabilità, qualità e l'elevata prestazione dei prodotti. Oltre a questo Comelit è vicina ai clienti anche nel post vendita offrendo un servizio di assistenza tecnica in tutto il territorio italiano ed un servizio di formazione con corsi dedicati anche al catalogo Fire.

Comelit Group
Via Don Arrigoni 5
24020 Rovetta S. Lorenzo (BG)
Tel. (+39) 0346 750011
Fax (+39) 0346 71436
info@comelit.it
www.comelitgroup.com/it-it

La Redazione

Verona goes vertical con IP Security Forum

Non tradisce le aspettative la piazza di *IP Security Forum* dislocata lo scorso 8 marzo a Lazise (VR). Un format collaudato e tematiche rivisitate sulla base delle esigenze formative emerse dalle precedenti edizioni hanno reso la puntata veronese di *IP Security Forum* un importante momento di aggiornamento, testimoniato dalla compatta “resistenza” dell’uditorio fino al tardo pomeriggio.

Da rimarcare la presenza di molti prestigiosi vendor e distributori, che hanno portato nella piazza itinerante di *IP Security Forum* il loro knowhow e le loro ultime tecnologie. Da rimarcare, ancor prima, l’alta profilazione e lo straordinario livello di attenzione e partecipazione della platea, letteralmente instancabile nel seguire la ricca offerta espositiva della giornata. Particolarmente apprezzato da visitatori e sponsor il format di *IP Security Forum*: un percorso in cui il pubblico veniva letteralmente “accompagnato” attraverso e lungo gli stand, per acquisire una formazione tecnica capace di spaziare dalla teoria alla pratica senza soluzione di continuità.

GO VERTICAL

Una novità partita lo scorso anno e molto apprezzata anche in Veneto è stata la verticalizzazione di IP Security Forum sui principali mercati verticali. Sul solco di questo approccio, quest'anno in parallelo alla sessione plenaria si è tenuta una Tavola Rotonda, Verticale appunto e ad invito, che ha visto confrontarsi manager e professionisti sul tema: "Sicurezza Urbana, riflessioni e opportunità". Un momento di condivisione con gli utenti finali sui temi più caldi della security per studiare nuovi approcci alla sicurezza.

ADVISORY BOARD E AUDIT PRIVACY

Altra novità di quest'anno molto apprezzata è stata l'esperienza di ben tre Advisory Board messa in campo su diversi ambiti: Normativa, Data Protection e Scenari di mercato. Gli esperti hanno regalato "pillole di formazione" che preludevano ai 4 Corsi di Formazione che hanno poi avuto luogo in forma integrale nel giorno successivo all'evento. Tutti di primaria importanza i temi: Norme CEI su Sistemi Antintrusione, Antirapina, Videosorveglianza, e poi responsabilità civile e penale degli operatori; Videosorveglianza e Privacy. In tema di privacy, altra novità molto apprezzata da sponsor e visitatori è stata la possibilità di ottenere una verifica preliminare ed un primo check up delle realtà aziendali gratuitamente. Un vero sold out.

FORMAZIONE E MERCATO

Leit-motiv della giornata era però il tema della formazione come percorso e strumento di differenziazione in



GRAZIE A

Advanced Innovations, Anixter, Artec, Aura Sicurezza, Avigilon, Bettini, Cavel, Electronic's Time, Elmat, Hikvision, Melchioni, Mitech, Select, Sice Telecom, Trans Audio Video

un mercato sempre più inflazionato, dove il fai da te imperversa anche nel mondo "professionale" e diverse figure di altri comparti sono attratte dall'interessante redditività del settore sicurezza. Focus della giornata: la possibilità, oggi concreta, di accedere ad un sistema di certificazione dei professionisti serio ed affidabile – il cui presupposto è però un percorso formativo altrettanto serio ed affidabile. Ebbene, Ethos Media Group, organizzatore di IP Security Forum, per somministrare formazione professionale di alto profilo ha dato vita ad Ethos Academy e ha messo a punto, assieme al TÜV Examination Institute, dei percorsi di certificazione perché gli operatori possano differenziarsi e proporsi sul mercato della qualità. Perché il mercato, quello industriale e commerciale, è in fase di particolare effervescenza, come mostrato in anteprima nazionale da due indagini sul valore della sicurezza in Italia e sul mercato dell'IoT e le sue applicazioni.

Insomma: gli ingredienti ci sono tutti. C'è il mercato, ci sono le norme, ci sono gli strumenti per differenziarsi. Tocca al comparto saperli cogliere.

La prossima tappa di *IP Security Forum* si terrà il 26 maggio 2017 a Bari: stay tuned!



La Redazione

Smart City e sicurezza: innovazione, condivisione, competenze

La sicurezza è oggi uno dei parametri fondamentali delle “Smart City”. Parallelamente il modo in cui si garantisce la sicurezza urbana è mutato radicalmente nel corso di questi ultimi anni, sia per l'incremento delle criticità, che con le maggiori opportunità di integrazione, garantite dai progressi della tecnologia. Ricordiamo che il mercato mondiale della Safety e Security nel 2016 valeva 247 miliardi di dollari. Le proiezioni parlano addirittura di un valore di circa 456 miliardi di dollari già nel 2021. Nella cornice di IP Security Forum (08/03/2017, Lazise – VR), la tavola rotonda “Sicurezza Urbana, riflessioni e opportunità” condotta da Mark Perna, giornalista ed esperto in Digital Life, ha riunito comandanti delle Forze dell'Ordine locali ed esperti del settore, per definire prospettive e criticità di un efficiente sistema di sicurezza urbana.

Osservando lo scenario complessivo, ci si domanda innanzitutto a che punto siamo arrivati nel nostro Paese e cosa manca. Secondo **Raffaele Zanon**, Presidente ANCSI (Associazione Nazionale Città Sicurezza Integrata): “La sicurezza è sempre più prevenzione e l'evoluzione è ormai costante. Le realtà locali rappresentano sempre di più degli attori fondamentali delle politiche di sicurezza urbana. Anche se, purtroppo, ogni questione di progettazione rimane legata ai bilanci. La sicurezza territoriale dovrebbe basarsi su dati locali, oggettivi e validati. Mentre resta ancora una mancanza di formazione condivisa e di cultura della sicurezza”. I conti economici sono elemento di approfondimento anche per **Luigi Altamura**, Comandante Polizia Municipale di Verona, che sottolinea: “il legislatore attuale cerca di aiutare le forze dell'ordine a cui mancano strumenti normativi. Ma rimane la questione relativa alle manutenzioni, che fanno parte delle spese correnti di un Comune: prima voce ad essere tagliata. Servono invece risorse umane e piani

di controllo integrati. Anche se, è bene ricordarlo sempre, la tecnologia non può sostituire la sicurezza partecipata". Nel frattempo però la tecnologia sta mostrando un'evoluzione rapida e radicale, di pari passo con l'incremento delle criticità e le amministrazioni locali faticano realisticamente a tenere il passo. Prospettive molto simili e allineate sono anche quelle di **Massimiliano Gianfriddo**, Comandante Polizia Municipale di Lazise: "Nei comuni piccoli è difficile fare assunzioni mirate, con competenze specifiche in tecnologie e sicurezza. Anche se la questione relativa alle manutenzioni rimane di stretta attualità anche dal mio punto di vista, considerando che bilanci spesso limitati possono creare difficoltà nel gestire nel tempo un sistema e ampliarlo. Parallelamente però è importante migliorare la sensibilità dei cittadini, per integrarli e coinvolgerli nel modo giusto". Una criticità confermata anche da **Pierdavid Scambi**, Progettista e Professionista Pubblica Sicurezza, che ha evidenziato come la manutenzione pesi molto: circa il 10% dell'impianto. Queste spese vanno certamente sbloccate e slegate dalle "spese correnti" di un Comune. Anche se spesso le infrastrutture non sono prima di tutto state studiate bene, per mancanza di competenze specifiche.

IL RUOLO DELLA CYBER SECURITY

Occorre rivolgere lo sguardo anche al tema della Cyber Security - cui, come sostiene **Filippo Novario**, Consulente Informatico Giuridico e Forense, già docente Universitario di Informatica Giuridica, occorre assolutamente dare rilievo, per il ruolo sempre più determinante, ma anche assolutamente strategico che va rivestendo. Bisogna dunque prestare attenzione alla sicurezza del dato intesa come "genuinità del dato" e la prova video deve a tal fine esse-

re acquisita in maniera corretta e con i giusti strumenti. I sistemi però, prima di essere utilizzati nella maniera corretta, vanno progettati al meglio, in funzione delle esigenze specifiche: "Se gli esperti di tecnologia non si basano sugli elementi forniti dai professionisti della sicurezza e, soprattutto, dalle Forze dell'Ordine, probabilmente si creeranno progetti tecnicamente perfetti, ma che non risolvono le esigenze e i problemi di sicurezza, che le stesse Forze dell'Ordine devono affrontare ogni giorno".

LO SCENARIO DI DOMANI

Cosa è emerso sulla stretta attualità e cosa da fare "domani" per migliorare lo scenario? La sicurezza è oggi più che mai una strategia, che deve passare anche da una revisione normativa assolutamente necessaria. Il Garante della Privacy sta infatti lavorando su un nuovo provvedimento sulla videosorveglianza: bisogna prima di tutto aggiornare la normativa. Su questo ambito, conclude **Marco Soffientini**, avvocato, coordinatore del Comitato Scientifico di Federprivacy: "A volte le PA locali esagerano con telecamere e video analisi. Spesso si finisce con l'aver un controllo esasperato e neanche utile. I Big Data, termine di stretta attualità, non sono solo tanti ma anche complessi da gestire. Per questo è importante che gli impianti di sicurezza siano si aggiornati e tecnologici, ma anche che siano gestiti da persone adeguatamente formate: determinante la figura del Data Protection Officer". Parallelamente, aggiungiamo, occorre che le istituzioni e gli addetti ai lavori si impegnino per migliorare le iniziative e il coordinamento tra gli attori deputati alla sicurezza del territorio. Bisogna lavorare sempre di più sulla condivisione delle informazioni, integrando gli vari impianti e favorendo così l'accesso a dati di maggiore qualità.





MILANO

L'Innovazione senza sicurezza è una falsa innovazione

Si sono concluse con successo le tre giornate ASIS Europe 2017 (29-31 marzo, al MiCo di Milano). Il messaggio? In un mondo sempre più digitale, la sicurezza è un elemento diffuso e imprescindibile. Occorre perciò cercare e raggiungere il coinvolgimento di tutte le parti in causa, dai CdA delle aziende con i loro dipendenti, ai clienti, passando per i produttori di sicurezza. È di Thomas J. Langer, CPP - ASIS International President, la frase "L'Innovazione senza sicurezza è una falsa innovazione", a sottolineare l'importanza dell'assunzione di responsabilità della filiera. L'intervento del General Manager di Microsoft Italia, Carlo Purassanta, ha poi suscitato grande interesse, con la sua chiamata a una formazione continua e costante, così come quello di Genseric Cantournet, Chief Security Officer di Rai sulla creazione di un team della sicurezza integrato a livello aziendale. All'evento è anche stato dato spazio a Stéphanie Bergouignan, che ha portato la voce di Women in Security. Prossimo appuntamento con ASIS Europe sarà all'Aja, nei Paesi Bassi, dal 18 al 20 aprile 2018.

www.asiseurope.org



RAVENNA

OMC: sicurezza e innovazione nell'industria Oil&Gas

L'evento biennale Offshore Mediterranean Conference, che si è svolto a Ravenna dal 29 al 31 marzo, si è confermato come la principale opportunità di incontro per l'Oil&Gas nella regione mediterranea. L'edizione 2017 ha visto la partecipazione di diversi rappresentanti governativi - tra cui il Sottosegretario del Ministero Sviluppo Economico, Ivan Scalfarotto, e il Ministro del Petrolio dell'Egitto, Tarek El Molla - e dei Ceo di Eni, Claudio Descalzi, ed Edison, Marc Benayoun. Su un'area espositiva di 30 mila mq, l'evento ha ospitato 650 espositori provenienti da oltre 30 Paesi e ha richiamato oltre 1.300 delegati da Paesi produttori e 22.000 visitatori, confermando il successo del 2015. Tra i temi affrontati, il ruolo dei combustibili fossili nella transizione verso l'energia sostenibile e l'importanza di ricerca e innovazione per affrontare la sfida dal cambiamento climatico. a&s Italy, presente all'evento, ha portato le proposte del mondo security a questo interessante mercato verticale, che sta vivendo una fase di ripresa dei prezzi dei prodotti energetici con auspiciabili effetti positivi sull'intera supply chain del settore. La prossima edizione si terrà nel 2019.

www.omc2017.it

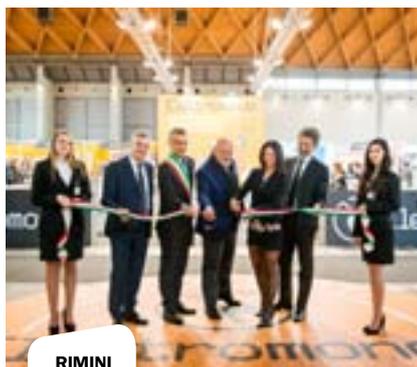


GUBBIO

Richmond Forum: il successo 2017, le novità 2018

Con la conferenza del Generale Roberto Vittori, primo cosmonauta italiano, si è aperta la quinta edizione di Safety & Security Forum, che si è svolta a Gubbio il 9 e il 10 marzo scorsi: due giorni di conferenze, networking e incontri di business dedicati a chi si occupa di HSE, Safety e Security. Organizzato da Richmond Italia, il programma è stato scandito da una fitta agenda di incontri volti a soddisfare le esigenze dei partecipanti sia in termini di business che di aggiornamento, attraverso sessioni plenarie, seminari, workshop e gruppi di lavoro volti a valorizzare la figura professionale di chi si occupa di Safety e Sicurezza all'interno delle aziende. Ethos Academy ha collaborato al programma formativo curando un partecipato focus di aggiornamento sulle novità in tema di "Privacy e Videosorveglianza dopo l'uscita del Nuovo Regolamento Europeo", condotto dall'avvocato Marco Soffientini, docente Ethos Academy e Coordinatore Nazionale del Comitato Scientifico di Federprivacy. Per la prossima edizione, Safety & Security Forum lascerà il posto a due distinti eventi, per rispondere a 360 gradi alla complessità nel settore della sicurezza: Security Director Forum, in calendario il 18 e il 19 giugno 2018, sempre a Gubbio; Health, Safety & Environment, l'8 e il 9 marzo a Rimini.

<http://www.richmonditalia.it/safety-security/>



RIMINI

Elettromondo 2017: oltre le aspettative

Si è conclusa con un bilancio decisamente positivo, presso Rimini Fiera, la sesta edizione di Elettromondo, l'evento fieristico dedicato a installatori, impiantisti, professionisti e operatori del settore elettrico, che il 17 e il 18 marzo ha visto il passaggio di 4.680 visitatori. L'evento, ideato e promosso da Elettroveneta e Ferri Elettroforniture, ha saputo soddisfare ancora una volta le aspettative del pubblico professionale presentandosi come una rassegna completa di marchi (oltre 150), prodotti e soluzioni innovative, su oltre 11.000 mq di superficie espositiva. Notevole l'interesse manifestato dai visitatori anche per l'attività convegnistica e per i workshop curati dalle aziende espositrici. L'argomento scelto per la seconda giornata di manifestazione è stato quello della relazione tra innovazione ed evoluzione normativa nel settore della videosorveglianza. All'approfondimento ha contribuito il focus di aggiornamento "Privacy e videosorveglianza dopo il Nuovo Regolamento Europeo", curato da Ethos Academy e tenuto dall'avvocato Marco Soffientini, tra i più noti esperti della materia.

www.eventoelettromondo.it



LONDRA (UK)

IFSEC 2017: sicurezza di persone, proprietà e asset

Anche quest'anno ad IFSEC International (presso l'ExCel di Londra, 20-22 giugno) vendor, installatori, progettisti ed integratori potranno trovare le soluzioni di sicurezza più adatte tra le oltre 10.000 proposte, assistere a dimostrazioni live e scoprire le ultime novità in tema di videosorveglianza, IT e cybersecurity, controllo accessi, sicurezza integrata, perimetrale e antintrusione. Confermando le previsioni degli analisti riguardo alla crescita della domanda di sicurezza in ambito Frontiere e Infrastrutture, l'edizione 2017 dedicherà a questo tema l'area "Borders & Infrastructure", con una mostra di prodotti e soluzioni specifiche e un programma di formazione sui vari aspetti della security in questo specifico segmento. In quest'area verrà allestita la BRE Global/LPCB Attack Testing Zone, dove per la prima volta verranno condotte prove live su recinzioni perimetrali, porte di sicurezza e saracinesche. Grazie al successo ottenuto nella scorsa edizione, verrà riproposta la SmartZone, con le ultime tecnologie per la sicurezza integrata, home automation e smart building. Non mancherà una sezione dedicata ai droni, in collaborazione con The UK Drone Show.

www.ifsec.co.uk



LONDRA (UK)

Euralarm Symposium: security e fire

Sono stati annunciati gli speaker del prossimo Euralarm Symposium, che l'8 maggio a Londra riunirà installatori professionisti dell'impiantistica di sicurezza e antincendio, system integrator, produttori e utilizzatori finali, manager ed enti di certificazione. Alla prima sessione, focalizzata sul nuovo Standard Europeo dei servizi per la sicurezza antincendio e i sistemi di security EN 16763, che dovrebbe garantire gli stessi livelli qualitativi in tutta Europa, contribuiranno Lance Ruetimann, Senior Manager Industry Affairs di Siemens, John Battersby, Managing Director presso Sunfish Services, e Alex Carmichael, Chief Executive del Security Systems and Alarm Inspection Board. Il punto focale della seconda sessione sarà la digitalizzazione nel mercato dell'antincendio e della sicurezza e, in particolare, come le aziende possono trarre il massimo vantaggio dall'evoluzione tecnologica in atto. Nel corso dell'incontro si parlerà, con la doppia prospettiva installatori ed utilizzatori, dei servizi a distanza in questo settore e dei centri di monitoraggio (MARC). Interverranno Rolf Sigg, CEO di Sigg Security Consulting, Bob Bantock, Heritage Fire Safety Specialist presso National Trust, e Rob King, Head of Strategic Engagement di Kings Security.

www.jointogethergroup.com/meetingpoint/EGA2017/



NEBBIOGENI A ELEVATA VELOCITÀ DI SATURAZIONE

La linea EOS è l'innovativa gamma di nebbiogeni dalle caratteristiche uniche creata da Aura Sicurezza. Grazie alla brevettata tecnologia Vortex è stata aumentata la velocità di saturazione riducendone in maniera incredibile le dimensioni. Gli 8 cm di spessore, un'estetica completamente personalizzabile e materiali all'avanguardia che dimezzano i consumi energetici rispetto ad un normale nebbiogeno ne permettono la facile installazione anche nel mondo civile.

Ogni modello Aura è dotato di scheda IP e di una scheda elettronica programmabile negli ingressi e uscite aumentandone la flessibilità di utilizzo e dando la possibilità di gestire il nebbiogeno da remoto.

La linea EOS oltre ad aver ottenuto la certificazione EN 50131-8 eroga una nebbia certificata IMQ ed ha ottenuto il CSI/FOOD CONTACT.

AURA SICUREZZA
www.aurasicurezza.com



RILEVATORE DOPPIA TECNOLOGIA WIRELESS

Arriva in casa CIAS AQUARIUS WL, il nuovo rilevatore doppia tecnologia (mw+IR) da esterno a basso assorbimento per sistemi completamente via radio. La tecnologia del sensore è quella ormai conosciuta e apprezzata del modello cablato già disponibile sul mercato da qualche anno nelle versioni XL e XS.

Ottimo prodotto come rapporto qualità/prezzo nato per installazioni a tenda, è adatto per tutti i contesti dove l'area da proteggere richiesta non supera gli 8m. Immune agli animali di piccola taglia e in grado di compensare automaticamente le differenze di temperatura presenti negli ambienti esterni, AQUARIUS WL è ottimo per la protezione di villette o piccole aziende.

La versione WL è interfacciabile a tutte le centrali con accessori Radio oppure, nella versione TAURUS, si integra perfettamente alla centrale Full IP QUASAR.

CIAS
www.cias.it



RICEVITORE TCP/IP PER SEGNALAZIONI DA CENTRALI

Multilink IP è un ricevitore TCP/IP per la ricezione di segnalazioni digitali su IP provenienti da centrali Combivox con comunicatore GPRS integrato o dotate di modulo LAN (Amicaweb Plus o Smartweb).

La gestione delle segnalazioni digitali, con protocollo proprietario Combivox, si realizza attraverso un software di semplice utilizzo in grado di archiviare e trattare i dati, memorizzandoli su HD a stato solido. Il centro è in grado di funzionare senza operatore grazie all'esclusiva funzione rimbalzo, ossia l'invio automatico di email, liberamente configurabili per ciascun evento (anomalia tecnica, allarme, mancata segnalazione di sopravvivenza).

E' possibile programmare un tempo di supervisione delle centrali fino ad un minimo 5 minuti, con notifica via email in caso di anomalia o sabotaggio provocato.

COMBIVOX
www.combivox.it



SISTEMA DI ALLARME WIRELESS CON VIDEO-VERIFICA

SerenityTM è un sistema di allarme Crow wireless 868MHz completamente bidirezionale con possibilità di video-verifica sia in interni che in esterni gestibile tramite cloud e APP CrowCloud gratuite.

La centrale è dotata di 32 zone (di cui 2 filari o radio), 4 aree con 1 parziale ciascuna, tastiera touch capacitiva retroilluminata e display LCD grafico, lettore RFID, interfaccia PSTN, TCP/IP, GSM/GPRS (dati/messaggi vocali/sms/formati codificati per vigilanza), sirena piezo interna, microfono e altoparlante, 2 uscite ausiliarie (open collector), 1 ingresso chiave, alimentatore a spina 9V e pacco batteria in tampone 2050mAh. Disponibili accessori Full Radio; tastiere e radiocomandi, rilevatori con telecamera CMOS a colori integrata, rilevatori doppio PIR da esterno con antimask, sensori antiallagamento e di fumo, attivatori prese 220V, ripetitori e moduli uscite a rele' via radio.

DEATRONIC
www.deatronic.com



VIDEOCAMERA FULL HD FISHEYE

La nuova DCS-4622 di D-Link è la più recente aggiunta alla gamma Vigilance che include videocamere di sorveglianza professionali, facili da installare e altamente convenienti. Progettata per soddisfare i requisiti di diversi contesti ambientali, questa videocamera è dotata di una lente fisheye che inquadra un ambiente a 360° compensando la distorsione dell'immagine, ed è equipaggiata con un sensore ad alta risoluzione da 3 megapixel. La correzione della distorsione rende possibile l'utilizzo del PTZ per analizzare al meglio un dettaglio dell'immagine.

Giorno e notte, la DCS-4622 sorveglia qualsiasi ambiente anche grazie agli illuminatori a infrarossi che consentono di vedere fino a 8 metri; altre funzioni avanzate sono il rilevamento dei movimenti, l'audio bidirezionale e la registrazione su scheda Micro SD (la scheda non è inclusa).

D-LINK
www.dlink.com/it



RILEVATORE DOPPIA TECNOLOGIA PER PROTEZIONE VARCHI

Il MYNI DT CUT è il rilevatore doppia tecnologia per la protezione dei varchi.

La prerogativa di questo dispositivo è che può essere applicato sia in modalità verticale o orizzontale, a seconda delle esigenze di installazione; questo consente la protezione di pareti finestrate, sia in ambienti interni che in esterni protetti, come, ad esempio, porticati, verande, sotto-balconi.

Inoltre, grazie agli accessori parzializzatori che lo rendono immune agli animali di piccola taglia, si può passare facilmente dalla parzializzazione che si limita a tagliare i fasci bassi dell'infrarosso fino ad arrivare all'applicazione del parzializzatore a cono, che, nella pratica, concentra la rilevazione su un mono-fascio orizzontale.

EEA
www.eea-security.com



RIVELATORI VOLUMETRICI PER INTERNO

Il rivelatore passivo d'infrarossi per interno RXC-ST di OPTEX distribuito da HESA è la soluzione ideale per le installazioni di alto livello in ambienti residenziali e commerciali.

Grazie alla Logica Quad, almeno quattro fasci devono essere attraversati prima di generare un allarme, in modo da distinguere gli esseri umani dagli animali domestici, consentendo di ottenere un'elevata immunità ai falsi allarmi.

In condizioni di elevata temperatura ambientale, assume un'importanza fondamentale l'accurata funzione di compensazione della temperatura di cui è dotato RXC-ST, perché permette di aumentare automaticamente la sensibilità di rilevazione, soprattutto quando la temperatura arriva a valori simili a quella del corpo umano.

Il dispositivo è conforme a EN50131-2-2 Grado 2.

HESA

www.hesa.com



APP PER GESTIONE IMPIANTI

L'APP Ksenia Pro, tramite il server remoto Ksenia SecureWeb, consente all'installatore la programmazione, la centralizzazione e la gestione di lares wls 96-IP attraverso qualunque dispositivo portatile.

Si associa alle modalità di gestione impianto via tastiera o PC, con nuove funzionalità che distinguono la piattaforma lares wls 96-IP Self-Contained/All-In One come protagonista nel mercato di Sicurezza e Domotica.

L'acquisizione con geolocalizzazione e notifiche push delle centrali avviene scansionando, tramite l'APP, il QR-code riportato sul PCB della centrale.

Permette di sviluppare il profilo dell'Installatore Ksenia, di tenerlo aggiornato sui punti maturati attraverso il programma di fidelizzazione, di centralizzare più impianti e di accedere a tutta la manualistica e alla sezione news con notifiche push, per una continua informazione anche in caso di allarmi tecnici o guasti.

KSENIA SECURITY

www.kseniasecurity.com



TERMINALE DI CONTROLLO ACCESSI

Il terminale Kaba 96 00 si contraddistingue per la sua semplicità di utilizzo, per le dimensioni compatte e un design accattivante con display touchscreen. E' un dispositivo ideale per applicazioni semplici di controllo accessi e rilevazione presenze. L'interfaccia utente è personalizzabile in funzione delle specifiche esigenze dell'utente: è possibile cambiare i tasti funzione, lo sfondo del display oppure visualizzare il logo aziendale. E' anche facile da installare con l'aiuto di un kit d'installazione. L'integrazione nel sistema host è possibile tramite l'interfaccia Ethernet con alimentazione POE o esterna 12 V DC.

Dispone opzionalmente di un lettore RFID integrato o Magstripe.

Il nuovo terminale Kaba 96 00, inoltre, è dotato di altoparlante incorporato e di porta mini USB che consente di collegare dispositivi esterni di lettura (per es. scanner per codici a barre 2D).

DORMAKABA

www.dormakaba.com/it-it/



TELECAMERA IP PTZ

Milesight PTZ Bullet è la nuova linea di prodotti con sensore da 2/4MP che consente di catturare maggiori dettagli in ogni condizione di luce (grazie alla funzione Starlight e WDR a 140db) e coprire una zona molto più vasta (grazie alla funzione PTZ ed all'ottica 5.3-64mm motorizzata 12x).

Supporta il protocollo di compressione H.265 per ottenere una minor occupazione di banda e un risparmio di spazio sull'HDD. La funzione Sensitive PTZ Motion Detection permette di delimitare un'area di Motion classica, ma con la differenza che, qualora la telecamera dovesse riconoscere il motion nell'area delimitata, andrà automaticamente a stringere sul soggetto e continuerà a inquadrare l'area fino a quando non terminerà l'evento.

Illuminatori IR 60mt utilizzano una funzione che si auto imposta in rapporto allo zoom così da avere sempre un'immagine ben illuminata ad ogni distanza.

MELCHIONI

www.melchioni.it



SOLUZIONE PROFESSIONALE PER UNA CASA SICURA E SMART

Smart Home è la nuova soluzione di RISCO Group per una casa sicura, connessa ed ecosostenibile, nata combinando sicurezza e verifica video professionale ad accessori intelligenti completamente integrati nel sistema, purché connessi al Cloud di RISCO.

Consente agli utenti di gestire la protezione della propria abitazione in maniera semplice e immediata direttamente dal proprio smartphone grazie all'app iRISCO, oltre ad abilitare la gestione smart dei consumi energetici, di tapparelle, elettrodomestici e accessi.

Smart Home può funzionare in autonomia rispetto al sistema di sicurezza e alla verifica video. Qualora, oltre a Smart Home, siano installati un sistema di sicurezza RISCO e video verifica, si può pensare di personalizzare gli scenari preimpostandoli sulla base di eventi specifici. Inoltre, la soluzione è compatibile con Aglity™3, LightSYS™2 e ProSYS™Plus di RISCO.

RISCO GROUP

www.riscogroup.it



TELECAMERA DI VIDEOSORVEGLIANZA PTZ

AEW PTZ TIANDY ha un evoluto sistema di riconoscimento di un intruso nella parte delimitata precedentemente che attiva un avviso acustico, anche parlato tramite messaggio registrato. Inoltre se l'intruso rimane nella zona per più di 30 secondi la PTZ attiva un laser verde e autotracciamento, affiancato a un diffusore sonoro, per una notevole forza deterrente.

La TVP tecnologia Starlight è in grado di offrire immagini di qualità pur in presenza di poca luce, mentre le distanze elevate sono ampiamente coperte grazie all'utilizzo di un LED IR varifocale che si aggusterà automaticamente in base allo zoom.

Per questo device è disponibile una APP con interfaccia all-in-one che offre anteprima, riposizione del filmato, configurazione veloce e una serie di operazioni di facile e intuitivo utilizzo.

A questo link: youtu.be/eoKcm196NaM trovate un video che chiarirà ogni aspetto.

TIANDY

www.tiandy.it



APP ANTIAGGRESSIONE/SOCCORSO CON FUNZIONE GPS

Il Personal Tracker/APP di SICEP è una applicazione per smartphone pensata per la propria sicurezza, delle persone a noi più care e di tutte quelle categorie considerate ad alto rischio.

In caso di pericolo è possibile inviare, mediante la pressione di un tasto rosso della APP installata sul proprio cellulare o tramite un apposito pulsante bluetooth collegato allo stesso, una richiesta di aiuto ad una Centrale di Vigilanza con sistema gestionale Mv-SNET (SICEP) con le relative coordinate geografiche per garantire un tempestivo intervento di soccorso.

La funzione GPS con tracciamento, l'attivazione su pressione/scuotimento o uomo a terra, la chiamata rapida impostabile, la telecamera attivabile, il collegamento con una Vigilanza in ascolto H24 rendono il Personal Tracker/APP di SICEP uno strumento indispensabile per vivere e sentirsi al sicuro, sempre ed ovunque.

SICEP
www.sicep.it



SENSORE PER PROTEZIONE PERIMETRALE

GAPID è un sensore MEMS, che sfrutta le capacità di un accelerometro triassiale in grado di discriminare e/o rilevare ogni tipo di vibrazione o spostamento su: recinzioni, grate, cancelli, inferriate, muro, vetrate, box e portoni.

Completo di 6 funzioni preset e 3 di autoapprendimento, tamper anti-rimozione del coperchio, contenitore anti-urto IP66 e alimentazione a basso assorbimento per sistemi wireless o da 8-30 Vcc, GAPID rappresenta la più moderna evoluzione nel campo delle protezioni perimetrali.

Il cavo di collegamento da 2-4-6m è schermato e precablato. Fra le altre caratteristiche: raggio di azione fino a 15mq; dispositivo di analisi e regolazioni integrato tramite buzzer e LED per la regolazione e la taratura; uscita allarme a relè.

GAPID è un prodotto Politec distribuito da Sicurtec Brescia.

SICURTEC BRESCIA
www.sicurtecbrescia.it



SISTEMA DI MONTAGGIO PER TELECAMERE

Spark è attenta alle esigenze di chi installa ed usa CCTV. UNICA, un sistema di montaggio brevettato, rende facile la messa in opera delle telecamere. Con poche e semplici azioni è possibile installare i dispositivi su pali, pareti e soffitti.

La sostituzione della camera non implica la sua riconfigurazione, né impone di intervenire sulla struttura di sostegno, rendendo il processo semplice, veloce e alla portata di tutti, siano essi installatori o utilizzatori. Un indubbio vantaggio, poiché si limita di gran lunga il tempo di disservizio del sistema in caso di guasto o aggiornamento: il fatto che la sostituzione non richieda particolari competenze, né coinvolga diverse strutture dell'organigramma aziendale, accelera la ripresa delle attività a pieno regime.

Con UNICA la massima efficienza è possibile.

SPARK
www.spark-security.com



UNITÀ PER INTERFACCIAMENTO DI CENTRALI DI SICUREZZA

Sincrobox è un'unità di campo che permette di accedere a diverse centrali di sicurezza da una postazione remota, in rete locale o raggiungibile tramite Internet. L'integrazione con la centrale è completa e bidirezionale, e consente sia la verifica degli stati che l'invio dei comandi anche ai singoli elementi (aree, gruppi, ecc...).

Fra le principali funzionalità: web server interno; comunicazione sicura HTTPS con cifratura lato server e/o lato client con certificati; consultazione stato centrale e suoi elementi; invio comandi; archiviazione eventi ed allarmi (max. 50.000); invio tramite email configurabili per evento; fino a 50 account locali configurabili a livello di permessi.

Queste le caratteristiche generali: porta Ethernet 10/100 GJ45; seriale RS232; seriale RS422; temperatura operativa: da -20° a +70°; alimentazione: da 10Vdc a 30Vdc; assorbimento: 250mA @ 12Vdc.

SINCROLOGICA
www.sincrologica.com



DVR E HVR PER VIDEOSORVEGLIANZA VEICOLI

La nuova serie DigiEye MOBILE DVR e HVR di SYAC TB è l'applicazione automotive della videosorveglianza. Costruiti per soddisfare le richieste di un mondo sempre più esigente rispetto alla sicurezza, i DVR e HVR Mobile sono pensati per la sorveglianza sui veicoli nelle aree metropolitane come autobus e scuolabus, ma anche mezzi di trasporto operanti in aree remote, grazie alle numerose opzioni di connettività integrate: WiFi, rete mobile 3G/4G, GPS, CAN.

Il software di centralizzazione consente di integrare la sorveglianza sulle flotte con la centrale di controllo, permettendo di gestire in tempo reale qualsiasi situazione di pericolo e di allarme.

Perfetti sia per applicazioni semplici che per architetture complesse, i sistemi DigiEye MOBILE sono pronti per essere sviluppati e personalizzati secondo specifiche esigenze e progetti speciali.

TECHBOARD
www.techboard.it



RILEVATORE RADIO PERIMETRALE CON DOPPIA RILEVAZIONE

Tecnoalarm presenta DRED500 BWL, il nuovo rivelatore radio perimetrale con doppia modalità di rilevazione infrarosso e contatto, compatibile con i protocolli di comunicazione radio monodirezionale ASYNC@WL (Serie 300) e bidirezionale SYNC@BWL (Serie 500), a banda di frequenza 868MHz.

DRED500 BWL offre la miglior soluzione per la protezione perimetrale di porte e finestre. Al posto del contatto magnetico interno è possibile collegare, in alternativa, un contatto magnetico esterno, un contatto a fune per tapparelle o un rivelatore inerziale. Infrarosso e ingresso contatto possono essere gestiti unitamente dal sistema: in modalità singola sola zona o in modo indipendente con due zone di rilevazione, per consentire massima flessibilità.

TECNOALARM
www.tecnoalarm.com



SIRENA-CENTRALE SENZA FILI CON GSM

CT7 è la nuova sirena-centrale che integra funzionalità di una centrale wireless con GSM. Possiede 7 linee (5 wireless e 2 filari), GSM integrato capace di gestire fino a 6 numeri di telefono.

CT7 è programmabile e gestibile tramite l'APP multilingue dedicata, permette l'invio di tutti gli eventi di allarme, anomalia e gestione attraverso SMS, è equipaggiata di un alimentatore da 800mA per la carica della batteria e l'alimentazione dei dispositivi collegati. Le uscite di alimentazione sono protette da fusibili auto-ripristinanti e CT7 dispone anche di un'uscita a relè dedicata per la gestione di una sirena interna ed esterna, oltre che di 4 uscite digitali già programmate. Un prodotto innovativo studiato per consentire un'installazione veloce e una gestione dell'impianto facilitata e alla portata di tutti.

VENITEM
www.venitem.com



AUTOMAZIONI PER CANCELLI SCORREVOLI E A BATTENTE

Le automazioni BXV per cancelli scorrevoli e AXI per cancelli a battente sono caratterizzate dalla completa connettività del sistema e, grazie alle linee essenziali e alla forma accattivante, possono essere integrate in qualsiasi contesto abitativo. Grazie alla tecnologia Came Connect, che assicura il collegamento del sistema al Cloud di Came, il proprietario può controllare facilmente, ovunque si trovi, le automazioni tramite l'APP dedicata CAME Automation, utilizzando un tablet o uno smartphone. Anche l'installatore, con un semplice collegamento Internet, può geolocalizzare gli impianti, effettuare diagnosi da remoto, cambiare le impostazioni di settaggio o risolvere eventuali problemi. La tecnologia di nuova generazione, con controllo del movimento a Encoder, garantisce massima sicurezza e affidabilità a livello di funzionamento, permettendo di rilevare eventuali ostacoli.

CAME
www.came.com/it/



TELECAMERE FISSE A CUPOLA PER APPLICAZIONI NAVALI

Axis Communications amplia e aggiorna la serie di telecamere AXIS Q35 con modelli dotati di sensori di immagine di ultima generazione, un'elaborazione ottimizzata con tecnologia Lightfinder e una sensibilità alla luce straordinaria grazie alla modalità Wide Dynamic Range - Forensic Capture. Inoltre, due nuovi modelli sono dotati di custodia in acciaio inox per applicazioni navali e di cupola trasparente in nylon, per resistere agli effetti corrosivi dell'acqua marina e di sostanze chimiche.

AXIS Q3505-V/-VE/-SVE Mk II offrono una qualità video HDTV 1080p a 30 fps (con modalità WDR attiva) e 1080p fino a 60 fps o 720p fino a 120 fps (con modalità WDR disattivata). AXIS Q3504-V/-VE hanno una qualità video HDTV 720p a 30 fps con modalità WDR attiva e fino a 120 fps con modalità WDR disattivata. Tutti i nuovi modelli AXIS Q35 offrono lo zoom e la messa a fuoco da remoto.

AXIS COMMUNICATIONS
www.axis.com/it/



SENSORI PASSIVI DA ESTERNO

SPECTRUM è la gamma di sensori passivi da esterno disponibile in nove diversi modelli per ogni esigenza, partendo dai via filo, SPECTRUM PA WALL AM ad infrarosso passivo e SPECTRUM DT AM a tripla tecnologia per arrivare ai via radio, SPECTRUM PA WALL WS AM e DT WS AM dedicato ai sistemi radio AVS e concludere con le versioni universali a basso assorbimento SPECTRUM PA WALL WS STD AM e SPECTRUM DTWS STD AM.

I sensori si avvalgono della tecnologia con accelerometro, capace di riconoscere immediatamente il disorientamento e i tentativi di manomissione.

Il dispositivo antimascheramento ad infrarosso permette di rilevare con efficacia ostacoli posti a copertura del sensore.

La funzione PET IMMUNE, ottenuta mediante la lente di Fresnel, discrimina gli animali di piccola e media taglia fino ai 70 cm.

AVS ELECTRONICS
www.avselectronics.it



SOLUZIONI INTERFONICHE PER CAMERE DI SICUREZZA

Le soluzioni Commend per camere di sicurezza soddisfano sia le semplici esigenze per poche celle fino alle necessità di interi istituti penitenziari.

I sistemi sono perfetti per gestire comunicazioni semplici, veloci ed affidabili.

L'ampia gamma di dispositivi e soluzioni permette di risolvere le più svariate necessità: la scalabilità dei sistemi permette inoltre, con poca spesa, di gestire dalle comunicazioni con gli ingressi alla struttura fino alla gestione proattiva del perimetro. I sistemi interfonici Commend garantiscono elevata qualità delle conversazioni; protezione antivandalò; scalabilità; economicità. Commend offre un unico sistema integrato in grado di garantire comunicazioni di qualità rapide, sicure, affidabili con ingressi alla struttura penitenziaria e alle varie aree; celle di detenzione; uffici; sistema radio mobile; sistema di diffusione sonora.

COMMEND
www.commend.it



TRANSPONDER "MANI LIBERE" PER SISTEMI DI ALLARME

Il transponder "mani libere" di DAITEM (SH808AX) consente di essere riconosciuti dalla centrale ed entrare tranquillamente in casa. Inoltre permette, senza digitare codici o passare tag sulla tastiera, l'accesso diretto a tutti i pulsanti per comandare l'impianto.

Utile per gli utenti che richiedono semplicità di utilizzo, come bambini e anziani, è possibile spegnere automaticamente il sistema d'allarme attraverso un rilevatore di movimento o di apertura posizionato a livello della porta d'ingresso o attraverso una tastiera con sensore di prossimità che, quando una persona dotata di transponder entra nella zona, innesca lo spegnimento automatico del sistema.

Il transponder è in grado di controllare direttamente il sistema di allarme attraverso 2 pulsanti di comando personalizzabili.

DAITEM
www.daitem.it



CENTRALE IP CON VIDEOVERIFICA

La centrale Genesy VEDO integra la videosorveglianza esistente con l'impianto di allarme per fornire la videoverifica. La centrale ha la stessa forma e aspetto delle tastiere ed è indipendente dalla soluzione di alimentazione che si intende adottare.

Dalla centrale si diparte un Bus 485 per la gestione di tutte le periferiche. Il Bus non richiede particolari accorgimenti, né terminazioni e può essere diramato a oltre 1.000 metri.

Dalla centrale partono anche 2 linee codificate per chiave elettronica o di prossimità, utili per il comando dei vari stati di impianto o per comandi specifici di domotica. La centrale può essere connessa a un pc dove uno specifico programma consente l'accesso e la prova di tutte le funzioni nonché il BackUp del sistema e lo scarico degli eventi.

WOLF SAFETY BY ELP
www.wolfsafety.it



MODULO COM EXPRESS CON SUPPORTO PER PROCESSORI INTEL

CPU-161-18, un modulo COM Express compatto di tipo 6 che supporta processori Intel Xeon D, amplia la famiglia HPEC (High Performance Embedded Computer) di Eurotech, per fornire capacità di calcolo e performance di I/O elevate in sistemi con architetture compatte e rugged.

È ottimizzato per applicazioni avanzate quali la guida autonoma, l'elaborazione di immagini, i rilievi geologici, la robotica, il deep learning, che richiedono di elaborare "sul campo" grandi quantità di dati raccolti dai sensori su veicoli, aeromobili ed imbarcazioni in luoghi isolati.

Unisce una CPU ad alte prestazioni con un'innovativa architettura RAM ibrida che offre la solidità della memoria saldata e l'espandibilità delle SO-DIMM. La configurazione standard prevede 8GB di memoria e uno slot SO-DIMM per aggiungere fino a 24GB di memoria DDR4 con correzione degli errori ECC.

EUROTECH
www.eurotech.com/it/



RILEVATORI DI MOVIMENTO DA INTERNO

L'IS312 e l'IS312B, sensori cablati da interno, possono soddisfare i requisiti di ogni installazione. Grazie alle loro performance superiori e all'esclusiva tecnologia di installazione "Plug-in" di Honeywell, offrono un eccellente livello di protezione dei locali e permettono agli installatori di risparmiare tempo e denaro poiché prevedono una implementazione più rapida e semplice.

Fra le caratteristiche: ottica a specchio avanzata; rilevamento alle alte temperature; livello ottimale di immunità ai piccoli animali domestici; funzionalità antimascheramento; superiore immunità alla luce bianca.

Sono la soluzione ideale per ambienti commerciali che richiedono un elevato livello di sicurezza e per i quali è indispensabile l'immunità dal mascheramento e dai falsi allarmi, come ad esempio musei, banche e gioiellerie.

HONEYWELL SECURITY
www.honeywell.com/security/it



VIDEO CLOUD NODE (VCN)

Basandosi sull'architettura avanzata per il cloud storage distribuito, Huawei Video Cloud Node (VCN) aumenta l'efficienza nell'utilizzo delle risorse attraverso le tecnologie cloud computing.

La tecnologia brevettata SafeVideo aiuta il sistema VCN a essere automaticamente ripristinato in caso di criticità e assicura un'affidabilità dei dati fino al 99.999%.

L'intero sistema VCN supporta un'agile espansione e mostra un incremento delle performance in linea con la crescita della capacità, supportando lo sviluppo sostenibile del business dei clienti.

Il Video Cloud Node (VCN) integra svariati servizi di videosorveglianza in un unico dispositivo, come la videosorveglianza live, i controlli PTZ, il rilevamento allarmi e i relativi collegamenti, le comunicazioni voce e le mappe elettroniche e molto altro.

HUAWEI
www.huawei.com



OTTICHE TELECENTRICHE PER VISIONE INDUSTRIALE

La linea MagniStar® di Navitar, Inc, comprende sei ottiche bi-telecentriche con attacco tipo C e diaframma integrato regolabile ed è specificamente progettata per applicazioni di misura e ispezione che richiedono estrema precisione. Le ottiche sono disponibili con ingrandimenti di 0,128X, 0,528X, 0,05X, 0,243X, 1X e 2X.

Si caratterizzano per telecentricità elevata, diaframma incorporato, ottime prestazioni MTF, nessun errore di parallasse e distorsione dell'immagine inferiore al 10%. Queste ottiche ad alta risoluzione e bassa distorsione sono progettate per operare con telecamere in formati di 2/3 di pollice e inferiori, oltre a supportare telecamere a megapixel con pixel da 3,5um. Le ottiche MagniStar sono ideali per l'ispezione di componenti industriali ed elettronici e, in generale, per le applicazioni di visione industriale che richiedono maggiore profondità di campo.

IMAGE S
www.imagessrl.com



RELEASE VMS PER SOLUZIONI DI GRANDE DIMENSIONI

XProtect 2017 R1 è la nuova release del VMS Milestone, che, grazie alla tecnologia a piattaforma aperta XProtect, consente un notevole risparmio dei costi nelle grandi installazioni.

La performance del server di registrazione è infatti di 3,1 Gigabit /s e prevede un numero ridotto di server, o server ancora più piccoli, risparmiando sull'hardware.

Grazie alla collaborazione con Intel e Microsoft, è stata attuata l'accelerazione hardware: il lavoro video di decodifica (rendering) viene affidato al sistema grafico dedicato (GPU, lasciando il processore principale libero di svolgere altri compiti. La GPU è ottimizzata per gestire grafica e video computerizzati, il che significa una notevole accelerazione.

La release include diversi miglioramenti per la cybersecurity, tra cui la verifica in due passaggi e un maggiore controllo nel concedere le autorizzazioni utente.

MILESTONE SYSTEMS
www.milestone.com

ISSN 2037-562X a&S Italy
ANNO 8 – Numero 44 – aprile 2017

Direttore responsabile
 Andrea Sandrolini

Coordinamento editoriale
 Ilaria Garaffoni
 redazione@ethosmedia.it

Direzione Commerciale
 Roberto Motta
 motta@ethosmedia.it

Ufficio Traffico
 Carolina Pattuelli
 pattuelli@ethosmedia.it
 tel. +39 051 0475136

Ufficio estero
 international@ethosmedia.it

Pubblicità
 Ethos Media Group srl
 pubblicita@ethosmedia.it

Privacy (banche dati)

Le finalità del trattamento dei dati dei destinatari del Periodico consiste nell'assicurare informazioni tecniche e specializzate a soggetti che per la loro attività sono interessati ai temi trattati. Tali dati sono trattati nel rispetto del D.Lgs. 196/2003. Responsabile del trattamento dei dati raccolti in banche dati ad uso redazionale è il direttore responsabile a cui gli interessati potranno rivolgersi per esercitare i diritti previsti dall'art. 7 del D. Lgs. 196/2003

Grafica / impaginazione
 www.zeronovecomunicazione.it

Stampa
 MIG - Moderna Industrie Grafiche s.r.l.
 Bologna

Rivista certificata secondo il Regolamento CSST

Ethos Media Group s.r.l. è associata ad



TUTTI I DIRITTI SONO RISERVATI

CSST CERTIFICAZIONE EDITORIA SPECIALIZZATA E TECNICA



A member of IFABC International Federation of Audit Bureau of Circulations

Testata volontariamente sottoposta a certificazione di tiratura e diffusione in conformità al Regolamento CSST Certificazione Editoria Specializzata e Tecnica

Per il periodo 1/1/2016-31/12/2016
 Periodicità: bimestrale
 Tiratura media: 9167
 Diffusione media: 9034
 Certificato CSST n. 2016 - 2605 del 2/3/2017
 Società di Revisione: REFIMI

Il portfolio delle riviste a&S, editate da Messe Frankfurt New Era Business Media (già nota come a&S Group), comprende: a&S International, a&S International China Best Buys, a&S Asia (pubblicate in inglese), a&S China, a&S Installer, a&S Solution, a&S Taiwan, Fire & Safety and Info Security (pubblicate in cinese). a&S Turkiye, a&S Adria, a&S Italy, a&S India e a&S Japan sono edizioni concesse in licenza.

INSERZIONISTI

ADRIA SECURITY SUMMIT 2017 - SIBENICO	pag.	92
ADVANCED INNOVATIONS	pag.	47 - 74
AURA by MOD SECURITY	pag.	59
AXIS COMMUNICATIONS	pag.	55
BENTEL SECURITY	pag.	32
CIAS EKETRONICA	pag.	62
COMBIVOX	pag.	10
D-LINK	pag.	71
DAHUA TECHNOLOGY CO.	pag.	3 - II COP.
DALLMEIER	pag.	8
DEATRONIC	pag.	63
DIMAR ELECTRONICS	pag.	50
EEA SECURITY	pag.	29
ELECTRONIC'S TIME	pag.	89
ERMES	pag.	84
ETER BIOMETRIC TECHNOLOGIES	pag.	109
EUROTEK	pag.	85
HANWHA TECHWIN	pag.	51
HIKVISION ITALY	pag.	11 - 93 - 100 - Cartino
IP SECURITY FORUM 2017 - BARI	pag.	66 - III COP.
IFSEC 2017 - LONDRA	pag.	24
ITALIAN ELECTRONICS HUB	pag.	117
KSENIA SECURITY	pag.	9 - I COP Sticker
MELCHIONI	pag.	6-7
NEXXTEC	pag.	105
OFFSHORE TECHNOLOGY - AMSTERDAM	pag.	118
SATEL ITALIA		I COP. Bandella
SECURITY FORUM 2017 - BARCELONA	pag.	114
SECURITY TRUST	pag.	75
SETIK	pag.	79
SICURTEC BRESCIA	pag.	25
SPARK	pag.	33
STUDIO SCAMBI	pag.	109
SURVEYE	pag.	37
TECNOALARM	pag.	14 - 15
TRANS AUDIO VIDEO	pag.	99
URMET		IV COP.



vai su Secsolution



vai su a&S Italy



vai su Ethos Media Group

LO PUOI TROVARE ANCHE PRESSO QUESTE AZIENDE

ABRUZZO - AGV Distribuzione Sicurezza - Via Mazzini, 17/A - 66020 San Giovanni Teatino (CH) - Tel. +39 085 8423161 ● **ASCANI Elettrocomm** - filiali di Pescara - via Talete, n° 18 - 66020 San Giovanni Teatino (CH) - Tel. +39 085 4406260 ● **CENTRO SICUREZZA** - Via Mulino del Gioco, 8 - 65013 Città Sant'Angelo (PE) - Tel. +39 085 95510 ● **DIME** - Divisione Sicurezza - Via Aterno, 11 - 66020 San Giovanni Teatino (CH) - Tel. +39 085 4463759 ● **ITS Italelettronica** - Via Po, 72 - 66020 San Giovanni Teatino (CH) - Tel. +39 085. 4460662 ● **V&V** - F.lli Verrocchio - Via Barnabei, 69/77 - 65126 Pescara - Tel. +39 085 691399 ● **VIDEOTREND L&S** - Via Fondo Valle Alento, 19 - 66010 Torrevecchia Teatina (CH) - Tel. +39 0871 361722

CALABRIA - ACC - Via Sbarre Superiori, 19 - 89129 Reggio Calabria - Tel. +39 0965 55468 ● **EL.SI.** - Via E. Ferrari - Località Zigari - 88900 Crotona - Tel. +39 0962 930786 ● **PROMIR** - Via N. Da Recco, 2-4 - 88100 Catanzaro - Tel: 0961 737121 ● **STRANO** - Z.Industriale C.da Lecco - Via Duca degli Abruzzi 12 - 87036 Rende (CS) - Tel. +39 0984 404024 ● **STRANO** - via Modena Chiesa, 81 - 89131 Reggio Calabria - Tel. +39 0965 51805

CAMPANIA - CIBF - Via Galileo Ferraris, 185 - 80142 Napoli - Tel. +39 081 7349175 ● **DHS Benevento** - Piazza San Lorenzo, 2 - 82100 Benevento - Tel. +39 0824 25350 ● **DODIC ELETTRONICA** - Via Ferrante Imparato, 198 (CM2 lotto A5) - 80146 Napoli - Tel. +39 081 5591787 ● **DSPRO Sicurezza ed Automazione** - Via Lima, 2/A2 - 81024 Maddaloni (CE) - Tel. +39 0823 405405 ● **GAM Service** - Via Nazionale delle Puglie, 178 - 80026 Casoria (NA) - Tel. +39 081 7591915 ● **PROFESSIONE SICUREZZA** - Via Romaniello, 87 - 81038 Trentola Ducenta (CE) - Tel. +39 081 18740456 ● **VITEKNA Distribuzione** - Via delle industrie, 33 - 80147 Napoli - Tel. +39 081 7524512

EMILIA ROMAGNA - ADRIACAME Group - Via O.Lazzaridetto Tavien, 20 - 47841 Cattolica (RN) - Tel. +39 0541 968588 ● **ARGO Elettronica** - Via Leoni, 4 - 41126 Modena - Tel. +39 059 331708 ● **DSA Med** - Via Cicogna, 103 - 40068 San Lazzaro di Savena (BO) - Tel. +39 051 6259633 ● **EDI Elettronica** - Via M.M. Plattis, 12 - 44124 Ferrara - Tel. +39 0532 64891 ● **HDI Distribuzione** - Via Morigi Nicola, 9/A - 43122 Parma - Tel. +39 0521 1912450 ● **IEH** - Via San Silvestro, 166/168 - 48018 Faenza (RA) - Tel. +39 0546 061091 ● **LIFE365 Italy** - Via Fleming 22 - 47122 Forlì (FC) - Tel. +39 0543 795988 ● **SICURIT Emilia Romagna** - Via del Sostegno, 24 - 40131 Bologna - Tel. +39 051 6354455 ● **SICURTEC Romagna** - Via Caduti del Lavoro, 31 - 48012 Bagnacavallo (RA) - Tel. +39 0545 62006 ● **TRS Standard filiale di Bologna** - Via Ferrarese, 108 - 40128 Bologna - Tel. +39 051 355817 ● **WISE** - Via Monti Urali, 29 - 42122 Reggio Emilia - Tel. +39 0522 272788 ● **VOYAGER** - Via Rivani, 59/B - 40138 Bologna - Tel. +39 051 531944

FRIULI VENEZIA GIULIA - SICURT - Via della Dogana, 46/B - 33170 Pordenone - Tel. +39 0434 571478

LAZIO - ADI Roma - Via Prenestina, 16 - 00176 Roma - Tel. +39 06 70305380 ● **BDF** - Via Torre Nuova, 1 - 04100 Latina - Tel. +39 0773 610476 ● **CERQUA** - Via Monti Lepini km.0,200 - 03100 Frosinone - Tel. +39 0775 874681 ● **CHECKPOINT** - Viale della Musica, 20 - 00144 Roma - Tel. +39 06 5427941 ● **DEATRONIC** - Via Giulianello - 00178 ROMA - Tel. +39 06 7612912 ● **DODIC ELETTRONICA** - Via Casale, 13 (Trav. Via A. Fabi) - 03100 Frosinone - Tel. +39 0775 840029 ● **ITALTEC** - Piazza di Villa Carpegna, 55/56 - 00165 Roma - Tel. +39 06 6623891 ● **SICURIT Lazio** - Via Luigi Perna, 37 - 00142 Roma - Tel. +39 06 5415412 ● **SECURITY ACILIA** - Via G. Boldini, 66/68 - 00125 Acilia (RM) - Tel. +39 06 5257479

LIGURIA - MP Distribuzioni - Via V. Capello, 56/58 - 16151 Genova - Tel. +39 010 6443090 ● **S.E.P.E.S.** - Via Del Faggio, 5r - 16139 Genova - Tel. +39 010 3626697

LOMBARDIA - ADI Milano - Via della Resistenza, 53/59 - 20090 Buccinasco (MI) - Tel. +39 02 4571791 ● **COM.PAC.** - via A. Luzzago 3 - 25126 Brescia - Tel. +39 030 48497 ● **D.S.A Brianza** - Via Maestri del Lavoro 20/22 - 20813 Bovisio Masciago (MB) - Tel. +39 0362 1791905 ● **ELP** - Via Tornago, 36 - 21010 Arsago Seprio (VA) - Tel. +39 0331 767355 ● **GULLIVER** - Via E. Mattei, 2 - 22070 Bregnano (CO) - Tel. +39 031 938642 ● **HESA** - Via Triboniano, 25 - 20156 Milano - Tel. +39 02 300361 ● **MOVITECH** - Via Vittorio Veneto, 63 - 22060 Carugo (CO) - Tel. +39 031 764275 ● **NIBRA** - Via Bellini 23 - 20093 Cologno Monzese (MI) - Tel. +39 02 2531592 ● **SACCHI ELETTRONICA** - Viale della Vittoria, 51 - 23897 Viganò (LC) - Tel. +39 039 9545211 ● **SETIK** - Via del Commercio 1/3 - 20851 Lissone (MB) - Tel. +39 0362 1855440 ● **SICURIT Alarmitalia** - Via Gadames, 91 - 20151 Milano - Tel. +39 02 380701 ● **SICURTEC Bergamo** - Via Zanca, 52 - 24126 Bergamo - Tel. +39 035 316600 ● **SICURTEC Brescia** - Via Bernini, 14 - 25010 S. Zeno Naviglio (BS) - Tel. +39 030 3532006 ● **TECNOCITY** - Via Lincoln Abramo, 65/67 - 20092 Cinisello Balsamo (MI) - Tel. +39 02 66043013 ● **TELEVISTA** - Via Orzinuovi, 46/D - 25125 Brescia - Tel. +39 030 6700140 ● **ZENIT Sicurezza** - Via Alessandro Volta, 3 - 24064 Grumello del Monte (BG) - Tel. +39 035 0900041 ● **ZENIT Sicurezza** - Via Rondinera, 87 - 24060 Rogno (BG) - Tel. +39 035 0900042

MARCHE - ASCANI Elettrocomm - Via Lame 113 - 63066 Grottammare (AP) - Tel. +39 0735 77446 ● **SICURIT - Marche - Abruzzo - Molise** - Via Guido Rossa, 12 - 60020 Ancona - Tel. +39 071 804514

MOLISE - ITS Italelettronica filiale di Campobasso - Via XXV Aprile, 31 - 86100 Campobasso - Tel. +39 0874 481762

PIEMONTE - ABES - Via Traversella, 13/A - 10148 Torino - Tel. +39 011 2290703 ● **DOPPLER** - Via Curiel, 14 - 10024 Moncalieri (TO) - Tel. +39 011 644451 ● **DOPPLER** - C.so Lombardia 13 - 10078 Venaria Reale (TO) - Tel. +39 011 4530709 ● **DOPPLER** - Via Della Chimica 4/G - 15100 Alessandria - Tel. +39 0131 227406 ● **DOPPLER** - Str. Borra 8/A - Fraz. Cinzano - 12069 Santa Vittoria D'Alba (CN) - Tel. +39 0172 499227 ● **DOPPLER** - Via Bra, 1 - 12100 Cuneo - Tel. +39 0171 417094 ● **DOPPLER** - Via Gibellini 94/A - 28100 Novara - Tel. +39 0321 474256 ● **DOPPLER** - C.so Venezia 112/A - 14100 Asti - Tel. +39 0141 320418 ● **ELCA** - Viale Indipendenza, 90 - 14053 Canelli (AT) - Tel. +39 0141 834834 ● **GEDICOM** - SS 231 B.go San Martino, 32 - 12042 BRA (CN) - Tel. +39 0172 413649 ● **GEDICOM** - Via Bisalta, 3 - 12100 CUNEO - Tel. +39 0171 346672 ● **GEDICOM** - Via Druento, 150 - 10078 Venaria Reale (TO) - Tel. +39 011 436827 ● **GOBBO** - Strada Bertolla, 162 - 10156 Torino - Tel. +39 011 2735720 ● **ITALTECH** - Via S. Antonio Da Padova, 8 - 28068 Romentino (NO) - Tel. +39 0321 868537 ● **SICURIT Piemonte** - Via Lesna, 22 - 10095 Grugliasco (TO) - Tel. +39 011 7701668 ● **SMART** - Via Amendola 197 - 13836 Cossato (BI) - Tel. +39 015 980079

PUGLIA - CPS GROUP - Via Baione, 198/L - 70043 Monopoli (BA) - Tel. +39 080 9303392 ● **DIGITAL SYSTEM** - Via Giuseppe Chiarelli, 8 G-H-I - 74015 Martina Franca (TA) - Tel. +39 080 4838949 ● **ELECTRONIC'S TIME** - Via Madonna Piccola - 74015 Martina Franca (TA) - Tel. +39 080 4802711 ● **FOR.TECH** - Via Eroi dello Spazio, 85 - 72010 Pezze di Greco (BR) - Tel. +39 080 4898815 ● **IEMME** - Via Acquari, 28 - 73030 Tiggiano (LE) - Tel. +39 0833 532020

SARDEGNA - L'ANTIFURTO - Viale Monastir, 112 - 09122 Cagliari - Tel. +39 070 291712 ● **PORTA** - Via Calamattia, 21 - 09134 Cagliari - Tel. +39 070 504500 ● **PORTA** - Strada Cinque, 30 - Z.I. Predda Niedda Nord St. 5 - 07100 Sassari - Tel. +39 079 2678016

SICILIA - CAME.COM - Via Giuseppe Patané, 8, 10, 12 - 95128 Catania - Tel. +39 095 447466 ● **DA.DO. TECNA** - Via B. Molinari, 15/17 - 90145 Palermo - Tel. +39 091 226244 ● **DECIBEL** - Via Alcide de Gasperi, 100 - 92019 Sciacca (AG) - Tel. +39 0925 22710 ● **RIL Elettronica** - Via delle Zagare, 6 - 98123 Messina - Tel. +39 090 2926562 ● **S.C.S.** - Via Alcide De Gasperi, 173/A - 90146 Palermo - Tel. +39 091 6199131 ● **SICURIT Sicilia** - Via Giuffrida Castorina, 11/13/15 - 95128 Catania - el. +39 095 7167423 ● **STRANO** - Zona Industr. 3a Strada, 36 - 95121 Catania - Tel. +39 095 523411 ● **STRANO** - P.zza Pietro Lupo, 6 - 95131 Catania - Tel. +39 095 7471111 ● **STRANO** - Via Casale Dei Greci 5, - 95031 Adrano (CT) - Tel. +39 095 7692617 ● **STRANO** - Via Vincenzo Florio, 4 - 95045 Misterbianco (CT) - Tel. +39 095 484148 ● **STRANO** - Via Galileo Galilei, 87 - 90145 Palermo - Tel. +39 091 201292 ● **STRANO** - Via Tommaso Marcellini 8/M - 90129 Palermo - Tel. +39 091 8889470 ● **STRANO** - Via Tonnara, 196 - 98057 Milazzo (ME) - Tel. 090.9414006 ● **STRANO** - Via Isola Zavorra, snc - 91100 Trapani - Tel. +39 0923 031876 ● **STRANO** - Viale 4 n° 8 - zona industriale 1ª fase - 97100 Ragusa - Tel. +39 0932 667129 ● **STRANO** - Via Archimede, 92 - 97100 Ragusa - Tel. +39 0932 662469 ● **STRANO** - S.S. 114, n. 30, C.da Targia - 96100 Siracusa - Tel. +39 0931 496068 ● **STS Elettrosolar di Stassi Giovanni** - Via Mazzini, 8 - 90030 Bologneta (PA) - Tel. +39 091 8737210

TOSCANA - ADI Firenze - Via Siena, 45 - Interno 31 - 50142 Firenze - Tel. +39 335 6359548 ● **AST** - Via Ilaria Alpi, 3 - 56028 San Miniato Basso (PI) - Tel. +39 0571 419804 ● **S.I.C.E.** - Via Tazio Nuvolari, 53 - 55061 Carraia (LU) - Tel. +39 0583 980787 ● **SICURIT Toscana** - Via di Porto, 17/19/21/25/27 - Località Badia a Settimo - 50010 Firenze - Tel. +39 055 7310214

TRENTINO - PAMITRON - Via Piave, 24 - 38122 Trento - Tel. +39 0461 915600 ● **TROLESE filiale di Bolzano** - Via Pillhof, 65 - 39057 Eppan (BZ) - Tel. +39 0471 502708

UMBRIA - A.E. - Via Ponte Vecchio, 73 - 06135 Ponte S. Giovanni (PG) - Tel. +39 075 395659

VENETO - ADI Padova - Via Risorgimento, 27 - 35010 Limena (PD) - Tel. +39 049 767880 ● **B&B TECNOSYSTEMS** - Viale del Lavoro, 2B - 35010 Vigonza (PD) - Tel. +39 049 8095820 ● **ELETTRO SIDI'S** - Via Monsignor Filippo Pozzato, 20/D - 45011 ADRIA (RO) - Tel. +39 0426 42496 ● **L'AUTOMAZIONE** - Via Parini, 1 - 30020 Eraclea (VE) - Tel. +39 0421 231781 ● **RRE ELETTRO FORNITURE** - Viale della Navigazione Interna, 51 - 35129 Padova - Tel. +39 049 775297 ● **SICURIT Veneto e Friuli** - Viale dell'industria, 23 - 35100 Padova - Tel. +39 049 7808387 ● **TELEVISTA** - Via Dei Fiori, 7/d - 36040 Meledo di Sarego (VI) - Tel. +39 0444 823036 ● **TELEVISTA** - Via Staffali, 44G - 37062 Dossobuono di Villafranca (VR) - Tel. +39 045 8240053 ● **TELEVISTA** - Via Zamenhof, 693 - 36100 Vicenza - Tel. +39 0444 914304 ● **TELEVISTA** - Via Nona Strada, 23/F - 35129 Padova - Tel. +39 049 9670027 ● **TROLESE** - Via Nona Strada, 54/56 - 35129 Padova - Tel. +39 049 8641940 ● **TRS Standard** - Via Roveggia, 108 - 37135 Verona - Tel. +39 045 584477 ● **TRS Standard filiale di Padova** - Via Risorgimento, 27 - 35010 Limena (PD) - Tel. +39 049 8841727 ● **TVS Italia** - Via dell'Artigianato, 8 - 35010 Roveggia (PD) - Tel. +39 049 5791126 ● **TVS Italia** - Via Newton, 25 - 31020 Villorba (TV) - Tel. +39 0422 444525

IP Security forum 2017

LAZISE (VR) • 8 MARZO 2017

HOTEL PARCHI DEL GARDA • CENTRO CONGRESSI • LAZISE (VR)

Grazie a tutti gli sponsor!



in collaborazione con:

un evento di:



Ethos Media Group srl
www.ipsecurityforum.it