essecome
security&safety

03

2015 · ANNO XXXV-III
ISSN 2384-9282

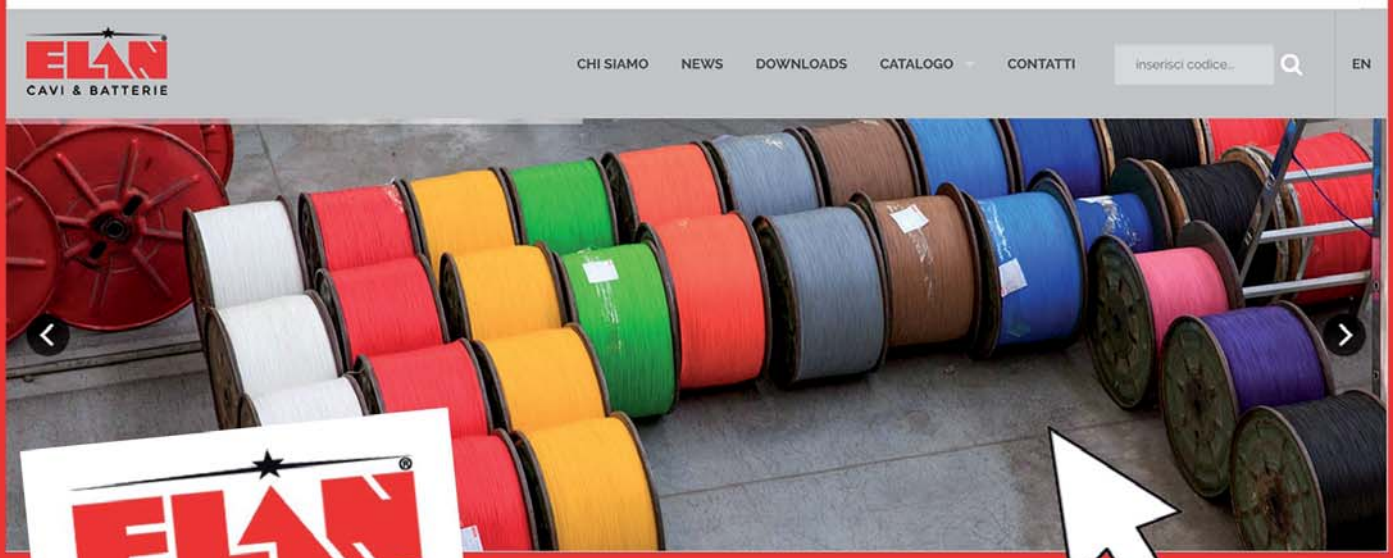
PERIODICO DI INFORMAZIONE SU PERSONE, TECNOLOGIE E APPLICAZIONI DELLA SICUREZZA

Cavi resistenti al fuoco
garantisce il funzionamento dell'impianto
in caso di incendio

Fire resistant cables
maintaining
circuit integrity

ElanFire

scopri il catalogo completo sul nuovo sito: **www.elan.an.it**



ELAN
CAVI & BATTERIE

ELAN srl
via Osimana, 70 - 60021 Camerano (An) - Italy
tel. +39.071.7304258 - fax +39.071.7304282 - www.elan.an.it - eMail: info@elan.an.it

Siamo gli unici ad aver preso un 4.
E ne siamo fieri.

CST. Gli unici sensori passivi al mondo brevettati e codificati **quadruplo bilanciamento**.

TSec
TECHNOLOGY FOR SECURITY

Coded Sensor Technology offre la massima sicurezza di varco oggi disponibile: il sensore CST riconosce il proprio magnete, pur essendo passivo e compatibile con ogni centrale. CST: un'esclusiva brevettata TSec. Seguiteci su www.tsec.it ›

dahua TECHNOLOGY

Segnale video HD su coassiale. HDCVI versione 2.0

Sempre leader dell'innovazione HD

Dahua Technology è sempre all'avanguardia nel settore HD. La seconda generazione di telecamere HDCVI completa la sua gamma con i modelli 1080p/720p, obiettivi varifocale, accessori di trasmissione e un nuovo chip di trasmissione HDCVI integrato con l'ISP, inaugurando la seconda versione della tecnologia HDCVI di trasmissione del segnale video HD su cavo coassiale.

- Telecamere 1080P/720P; disponibili fisse o varifocali o motorizzate, e speed dome PT
- Prestazioni HD ancora migliorata, ad un prezzo aggressivo
- Accessori per fibra ottica: ricevitori, convertitori ed extender sono già disponibili
- La tecnologia Dahua HDCVI è ad accesso aperto
- Sono stati venduti finora oltre 2 milioni di dispositivi HDCVI
- La tecnologia HDCVI 2.0, con HDcctv Alliance, è ora uno standard globale

Principali modelli HDCVI :

4/8CH 1U Tribrido (HDCVI & Analogico & IP) DH-HCVR7204/7208A-S2	4/8/16CH 1,5U Tribrido (HDCVI & Analogico & IP) DH-HCVR7404/7408/7416L	4/8/16CH 2U Tribrido (HDCVI & analogico & IP) DH-HCVR7804/7808/7816S
Telecamera bullet IR HDCVI 720p/1080p da esterno DH-HAC-HFW2120R/2220R-Z/VF	Telecamera dome IR HDCVI 720p/1080p antivandalo DH-HAC-HDBW 2120R/ 2220R-Z/VF	Telecamera IR HDCVI, 2 Mp, 1080p, da esterno DH-HAC-HFW2220S

CE FC ISO 9001:2000

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

Videotrend S.r.l.
Distributore ufficiale Dahua
Tel. 0362 1791300
www.videotrend.net / info@videotrend.net

alhua TECHNOLOGY

Eco-Savvy Serie 2.0

Telecamera IP 4-Megapixel

- 4Mp@20fps; 3Mp@25fps
- uscita video a tripla risoluzione
- protezione IP67, IK10
- analisi video intelligente
- WDR fino a 120dB
- zoom ottico 30x (modello PTZ)

4Mp | 1080p FULL HD | ICR D/N | IP67 | PoE | IK10

Modelli consigliati

>> IPC-HFW5121/5220/5221/5421E-Z <<
>> IPC-HDBW5121/5220/5221/5421E-Z <<
>> IPC-HFW4421S <<
>> IPC-HDW4421M <<
>> SD59212T/220T/230T-HN (2MP) <<
>> SD50220T/230T-HN (2MP) <<

CE FC UL ISO 9001:2000

www.dahuasecurity.com

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

Videotrend S.r.l.
Distributore ufficiale Dahua
Tel. 0362 1791300
www.videotrend.net / info@videotrend.net

GLI EVENTI DI ESSECOME

LE ECCELLENZE PER LA SICUREZZA

Milano
21 settembre 2015

Le Gallerie d'Italia Piazza Scala

axitea SECURITY EVOLUTION
ISEO
MICRONTEL
MIRASYS
SAMSUNG SAMSUNG TECHWIN
Tsec TECHNOLOGY FOR SECURITY

IoT, cancellato il confine tra la sicurezza fisica e quella logica

Nel febbraio 2014, un commando non identificato ha messo fuori uso a fucilate 17 trasformatori di una sottostazione elettrica nella Silicon Valley, dopo aver disattivato con un'azione informatica i sistemi di sicurezza e videosorveglianza; a dicembre, degli hacker hanno provocato ingenti danni agli impianti di una fonderia in Germania, mandando in tilt il sistema di controllo delle colate degli altoforni; all'inizio del 2015, si è saputo che "Carbanak", una banda internazionale di criminali informatici, sta svuotando da anni gli ATM di un centinaio di banche in tutto il mondo, con un bottino di almeno 1 miliardo di dollari in banconote trafugate fino ad oggi. La banda ha trovato il modo di programmare l'erogazione automatica dei bancomat, che si svuotano da soli al momento voluto.

Sono episodi che aprono scenari del tutto nuovi per la sicurezza. Gli attacchi informatici non servono più "solo" a sottrarre dati, ma possono anche produrre direttamente (o a consentire di arrecare) danni fisici agli obiettivi, sia a fini terroristici che predatori. Siamo appena agli albori dell'Internet delle Cose, e già si può affermare che ha cancellato i confini tra la sicurezza fisica e quella logica. *Nomen Omen,* un nome un destino, in fondo già presente nell'apparente ossimoro tra la Rete e le Cose...

Secondo l'Internet Security Treath Report 2015 di Symantec, il trend è inesorabilmente destinato ad aumentare nei prossimi anni: "*A seguito dello sviluppo del mercato IoT, alcuni attacchi hanno già dimostrato di poter agire sui routers e i sistemi IoT basati su Linux. Già alla fine del 2013 i ricercatori di Symantec avevano scoperto un nuovo virus per Linux chiamato Darlloz che puntava a piccoli dispositivi su Internet, come routers domestici, set-up box e videocamere di sicurezza. A marzo del 2014, Symantec aveva trovato 31.716 dispositivi infettati con questo virus. Quando si consolideranno i leader di mercato e si rafforzeranno i loro ecosistemi, è prevedibile che anche i loro dispositivi verranno attaccati con modalità adeguate"* (ISTR 20, pag. 26). Symantec afferma, in sostanza, che i dispositivi basati su Iot già adesso sotto attacco fanno solamente presagire quello che succederà quando l'Internet delle Cose avrà preso definitivamente piede.

È evidente che gli effetti determinati da questa situazione nei confronti del mondo intero che si occupa delle protezione delle persone, dei beni e delle organizzazioni nei confronti delle minacce e degli attacchi volontari, saranno imponenti. La prima conseguenza è nella gestione della sicurezza in termini di funzioni decisionali, di strumenti, di procedure e di addestramento. Solo a titolo di esempio, quali competenze dovranno avere i security manager e da quali percorsi formativi dovranno arrivare? Quali esperienze verranno richieste ai progettisti, che devono prevedere tutti i punti deboli, fisici e logici, di un sistema? E, soprattutto, cosa devono fare i fornitori, dal momento in cui le loro soluzioni, efficacissime per proteggere da ogni possibile attacco fisico, possono venir fatte svanire con un semplice click su una tastiera remota?

Sommario

News

Technologies

Security for Retail

Cultura e Formazione

Fire & Smoke

Denaro Sicuro

Vigilanza & Dintorni

Fiere

in copertina...

SAET ITALIA S.p.A., distributrice in esclusiva dei prodotti a marchio SAET, rappresenta, con la sua rete di concessionari, l'unica iniziativa di questo genere in Italia e forse in Europa nel campo degli operatori della sicurezza: un punto di riferimento di un numero sempre crescente di concessionari in tutto il territorio nazionale, integrati nel tessuto locale e sintonizzati tra loro. L'obiettivo di SAET ITALIA è di consentire ai concessionari di utilizzare la qualità dei prodotti e la professionalità degli operatori SAET, per ottenere il miglior risultato possibile.

SAET ITALIA mette a disposizione un catalogo di prodotti vastissimo e completo per ogni categoria dell'impiantistica di sicurezza: dall'antifurto all'antincendio, dai sistemi tvcc a quelli di controllo accessi e gestione presenze, con innumerevoli accessori che completano l'offerta, per rappresentare il fornitore di riferimento per i concessionari.

Si aggiunge a questo l'assistenza post-vendita con help-desk tecnico, al quale rivolgersi per avere aiuto in tempo reale o per richieste di informazioni e documentazione, disporre di continui corsi di aggiornamento e di formazione tecnica o commerciale. Il concessionario SAET dispone quindi di un catalogo di apparecchiature completo e concorrenziale da un unico fornitore, potendo ottenere una concessione anche in esclusiva per la propria zona di competenza. Può contare su un magazzino fornito e veloce; su un gruppo di colleghi sparsi in tutta Italia; sulla partnership di aziende produttrici disponibili a soddisfare anche richieste specifiche; su un knowhow tecnico e professionale condiviso tra i colleghi concessionari. Può inoltre beneficiare di una campagna pubblicitaria su scala locale e nazionale.

SAET ITALIA Sistemi di sicurezza e controllo
Sede legale: Via F. Paciotti 30, 00176 Roma
Sede operativa: Viale A. Filarete 122/128, 00176 Roma
Tel. 06.24.40.20.08 – **Fax** 06.24.40.69.99
www.saetitalia.it E-mail: saetitalia@saetspa.it

Responsabilità degli installatori di impianti: la parola al legale

contributo dell'avv. Piero Ricciardi, Studio legale Ricciardi, Napoli

Il tema della responsabilità contrattuale dell'installatore è di vecchia data, derivando dalle disposizioni del Codice Civile in materia di appalti. Tuttavia, è entrato nella sfera di attenzione degli operatori del settore sicurezza in tempi relativamente recenti, per effetto dell'entrata in vigore di norme specifiche come la CEI 79/3 pubblicata nel 2012, ma soprattutto per la produzione da parte dei tribunali di sentenze di condanna a risarcire danni per somme anche importanti, per negligenza o colpa dell'installatore, in casi di comprovato mancato o cattivo funzionamento dell'impianto di allarme in occasione di furti o rapine.

Essendo dunque un argomento di notevole rilevanza, cercheremo di fornire agli operatori un servizio di connotazione tecnico-giuridica con il contributo dell'Avv. **Piero Ricciardi,** esperto delle problematiche del settore e che collabora con **essecome** fin dal 2011 in materia di privacy e videosorveglianza.

Intendiamo così fornire ai nostri lettori un contributo tecnico di ampio spettro circa le tematiche più insidiose dal punto di vista tecnico-applicativo per i produttori, gli installatori e gli altri stakeholders del settore della safety e security.

Per iniziare, quale disciplina deve essere applicata alle imprese di installazione di impianti e quali sono i soggetti interessati?

In primo luogo, evidenzierei che i soggetti interessati all'applicazione delle normative di cui discuteremo sono tutti coloro che operano di fatto nel settore della sicurezza e dell'impiantistica nel senso più ampio: **progettisti, installatori e manutentori,** operanti come soggetti tecnico-professionisti, ovvero come **imprenditori**. Per ciò che concerne invece la normativa nel settore delle installazioni, occorre premettere, per evitare di incorrere in divieti e violazioni di legge, che esistono discipline sia di natura civilistica che di natura penalistica.

È necessario inoltre distinguere che esistono una **disciplina di carattere generale** e **una disciplina specifica.** La prima si fonda sull'applicazione del contratto di appalto stipulato tra l'azienda di installazione (o quella che si occupa della manutenzione degli impianti oppure della progettazione) ed il committente (l'utente finale). È bene ricordare che, con l'appalto, **l'imprenditore assume su di se l'obbligo dell'organizzazione per il compimento di un'opera o un servizio**, quindi a rischio dei propri mezzi

tecnici e materiali; inoltre, è tenuto a **garantire che l'opera o il servizio concordato col committente sia scevro da difformità e vizi.**

Si tratta di situazioni in cui, quando sorge un problema che genera "patologie" come, ad esempio, la presenza di **difformità o di vizi dell'opera** oppure come il **malfunzionamento dell'impianto** dopo il rilascio della dichiarazione di conformità, **scaturisce una responsabilità per la società appaltatrice** (installatore, manutentore o progettista) nei confronti del committente.

Bisogna pertanto prestare una grande attenzione nel concordare i contenuti del contratto di appalto: qualunque incertezza può offrire al committente il motivo scatenante per una richiesta di inadempimento contrattuale, con la conseguente richiesta di risarcimento dei danni subiti.

Il principio generale che guida la materia dell'appalto stabilisce che la **responsabilità civile** è dell'appaltatore per tutti i danni derivanti dalla non perfetta esecuzione del progetto, essendo l'appaltatore chiamato a rispondere della realizzazione del risultato convenuto nel contratto (infatti, **l'appaltatore assume in proprio una obbligazione circa il raggiungimento del risultato pattuito**); per tale motivo, questi è tenuto a realizzare il progetto dal punto di vista tecnico, ma anche a segnalare gli eventuali errori nell'ambito delle istruzioni impartite dal committente. Dunque, la eventuale clausola di **discrezionalità tecnica** inserita nel contratto, porterà alla esenzione dalla responsabilità dell'appaltatore solo nei casi in cui le eventuali irregolarità insite negli ordini impartiti dal committente non siano riconoscibili con la ordinaria diligenza e perizia; così come andrà esente da responsabilità l'appaltatore che abbia informato il committente che le indicazioni fornite da quest'ultimo porteranno alla realizzazione di un risultato tecnico non in linea con le regole della conformità al progetto. In tutti gli altri casi, la responsabilità ricade sempre sull'azienda appaltatrice, la quale potrà essere chiamata a rispondere dinanzi al giudice a causa del non esatto adempimento dell'appalto, della risoluzione del medesimo contratto ed al risarcimento del danno cagionato al committente.

Parliamo della disciplina specifica di settore.

Nella materia di cui ci stiamo occupando, il legislatore ha previsto un corpo normativo che fa capo alla legge n. 81 del 2008, meglio conosciuta come il **testo unico sulla sicurezza (TUS)**; a questa si affianca il decreto ministeriale n. 37 del 2008 che fissa standard minimi di sicurezza nella installazione impiantistica.

Andando per ordine, il **testo sulla sicurezza** è di natura strettamente tecnica, nel senso che la legge im-

pone agli installatori di attenersi scrupolosamente alle norme sulla salute delle persone coinvolte ed a quelle circa la sicurezza del lavoro; inoltre, l'installatore deve conformare ai requisiti di sicurezza imposti dalla legge tutti i materiali adoperati, i macchinari usati, le installazioni realizzate, gli impianti elettrici ed elettronici; tutto deve corrispondere alle norme tecniche previste nel testo unico. Solo in tal modo, seguendo le regole d'arte, l'installatore potrà andare esente da qualsivoglia responsabilità contrattuale ed extracontrattuale. Ecco spiegato il motivo per il quale le imprese di rilevanti dimensioni e capacità preferiscono costituire al loro interno un ufficio tecnico dedicato.

Il DM 37/2008 rappresenta un fulcro centrale dell'applicazione delle normative in materia impiantistica giacché impone **criteri minimi di sicurezza** per tutte quelle imprese che si occupano di installazione di impianti in ambito domestico ed industriale, a partire dalla impiantistica di videosorveglianza. In primo luogo, la legge prescrive un titolo abilitativo dell'impresa appaltatrice degli impianti (art. 3), richiedendo che l'imprenditore individuale o il legale rappresentante ovvero il responsabile tecnico da essi preposto con atto formale, sia in possesso dei requisiti professionali (di cui si dirà più avanti). Non solo, ma stabilisce altresì che la figura del responsabile tecnico è incompatibile con ogni altra attività continuativa.

Nella stessa normativa (art. 4) sono previsti alcuni **requisiti tecnico-professionali**: innanzitutto è necessario possedere un diploma di laurea in materia tecnica specifica conseguito presso una università statale o legalmente riconosciuta, ovvero un diploma o qualifica conseguita al termine di scuola secondaria del secondo ciclo con specializzazione relativa al settore delle attività oggetto del decreto; oppure un titolo o attestato conseguito ai sensi della legislazione vigente in materia di formazione professionale, previo un periodo di inserimento di almeno quattro anni consecutivi, alle dirette dipendenze di una impresa del settore. Ancora, rappresenta titolo abilitativo anche lo svolgimento di prestazione lavorativa svolta, alle dirette dipendenze di una impresa abilitata nel ramo di attività cui si riferisce la prestazione dell'operaio installatore per un periodo non inferiore a tre anni, escluso quello computato ai fini dell'apprendistato e quello svolto come operaio qualificato, in qualità di operaio installatore con qualifica di specializzato nelle attività di installazione, di trasformazione, di ampliamento e di manutenzione degli impianti oggetto del decreto.

Per quanto concerne la fase progettuale ?

Certamente anche il momento della progettazione tecnica dell'impianto che si va a realizzare deve essere sviluppato seguendo le **regole dell'arte**; con tale locuzione il legislatore vuole significare una serie tipologica di interventi che vanno dalla predisposizione dei disegni planimetrici, dagli schemi di impianto, dalle relazioni tecniche circa consistenza e tipologia dell'installazione; senza dimenticare che, a conclusione dei lavori, l'impresa appaltatrice deve rilasciare la **dichiarazione di conformità dell'intero impianto.** Tale dichiarazione si sostanzia in un documento che include il progetto, una relazione sui materiali adoperati, la dichiarazione di congruità dei materiali rispetto al contesto ambientale in cui si è operato, l'indicazione sulle caratteristiche degli apparecchi usati nella installazione.

Esiste anche una normativa di carattere penale ?

Premesso che nel nostro ordinamento giuridico **la responsabilità penale è personale**, se, ad esempio, il lavoratore assunto commette una rapina ai danni di un utente presso il quale l'impresa aveva in precedenza realizzato un impianto allarme intrusione, il legale rappresentante dell'impresa installatrice non risponderà del reato di rapina commesso dal proprio dipendente. Il problema che qui si presenta è di altra natura, e cioè se l'impresa di installazione che assume personale qualificato ha la possibilità di verificare a monte l'idoneità del proprio dipendente a lavorare in un settore delicato come quello della sicurezza; in tali casi, però, l'impresa potrebbe essere chiamata a rispondere per la responsabilità civile, nella fattispecie per avere omesso di vigilare sull'operato dei propri dipendenti. Ma il discorso è piuttosto lungo e dovremmo richiamare lo statuto dei lavoratori che fa divieto all'imprenditore di assumere informazioni sul lavoratore (la c.d. indagine preassuntiva) finalizzata all'assunzione dello stesso.

Esiste poi un'altra norma generale nell'ordinamento penale italiano che stabilisce un fondamentale principio, secondo il quale (art. 40 cod. pen.) *non impedire un evento che si ha l'obbligo giuridico di impedire, equivale a cagionarlo.* Questa norma è di fondamentale importanza per un duplice ordine di motivi: in primo luogo, pone sullo stesso piano **azione ed omissione**

Le Sucre™

Le Sucre™: soluzione di sicurezza gestita autonomamente dall'utente finale

Sviluppato in risposta alle esigenze degli utenti finali, Le Sucre™ è un sistema di sicurezza senza fili che si inserisce con discrezione in qualunque punto della casa. Installato da professionisti esperti e insieme ai servizi Honeywell Cloud Services, Le Sucre™ offre agli utenti finali un sistema di monitoraggio autonomo basato sulla medesima tecnologia e qualità delle installazioni connesse agli istituti di vigilanza. L'utente finale sarà facilmente in grado di sapere se il sistema è attivo o disattivato e di apportare le eventuali modifiche necessarie.

Offri il pieno controllo ai tuoi clienti con Honeywell Cloud Services!

Honeywell

Per ulteriori informazioni visitare il sito **www.honeywell.com/security/it**

nel senso che chi è responsabile di una determinata situazione rilevante per l'ordinamento (ad es. l'appaltatore che è responsabile dell'opera commissionata) viene investito di una posizione di garanzia rispetto agli eventi dannosi che dovessero verificarsi nel corso dell'esecuzione, stabilendo che è necessario approntare tutti gli strumenti tecnici per impedire che l'evento si verifichi; questo è il secondo punto centrale della norma, quella cioè di evidenziare una responsabilità penalmente rilevante in capo ad un soggetto qualificato che assume su di se l'obbligo di impedire che si verifichino situazioni pericolose per altri soggetti.

Per concludere, appare palese che esistono una serie di impegni legali che ricadono sull'attività professionale dell'azienda di installazione

Le normative tecniche nonché quella sulla sicurezza sono sicuramente molto stringenti e ricche di complessità, e vanno seguite pedissequamente se non si vuole incorrere nelle sanzioni previste dalla legge; per evitare ciò è possibile procedere ad una **attenta analisi** azienda per azienda per verificare il rispetto delle regole e, se del caso, porvi rimedio prima di incorrere nelle violazioni.

In conclusione, esistono le c.d. buone pratiche in campo tecnico, come il regolamento del Comitato elettrotecnico italiano 79-3, dedicata ai sistemi di allarme e a norme particolari per gli impianti di allarmi intrusione; basti ricordare l'allegato K di questa norma Cei, nel quale vengono stabilite le competenze ed i requisiti richiesti per quei soggetti che operano a vario titolo nell'ambito della fornitura di servizi per impianti di allarme intrusione e rapina. Tuttavia, è di auspicio che il legislatore si faccia carico, al più presto, di intervenire a regolamentare in maniera più esaustiva ed idonea la materia, soprattutto offrendo ai professionisti del settore safety and security modelli di maggiore tutela di pubblica sicurezza.

BETAFENCE
Il nome della Recinzione

Visita www.betafence.it

Securifor®

un sistema completo che abbina design e massima sicurezza

La ridottissima dimensione e la robustezza delle maglie
impediscono lo scavalcamento della barriera e rendono il sistema **anti-taglio**
e **anti-finger**, garantendo contemporaneamente **grande visibilità anche laterale.**

Scansiona il QR-CODE con il tuo smartphone per approfondire Securifor® e la gamma Alta Sicurezza Betafence.

Betafence Italia SpA C.da Salinello, 59 - 64018 Tortoreto (Te) Italy -Tel. +39.0861.7801 - Fax +39.0861.780650 - info.italy@betafence.com

“Drive the change”: il messaggio lanciato nell’incontro HESA 2015

a cura della Redazione

All’edizione 2015 del Meeting Nazionale dei Concessionari e Installatori Autorizzati HESA, che si è tenuta anche quest’anno nell’incantevole baia di Biodola all’Isola d’Elba, la parola chiave è stata “Cambiamento”. Un cambiamento nella sostanza dei fatti, percepibile nel contenuto dei messaggi lanciati, nelle novità presentate, nella presenza di alcuni dei principali produttori distribuiti da HESA e nello stesso coinvolgimento partecipativo dei clienti fidelizzati. Segnali che attestano l’evoluzione in corso a livello globale ma, soprattutto, testimoniano l’impegno profuso da HESA, indiscusso protagonista storico del settore, per rimanere al passo con i tempi e confermarsi come punto di riferimento per tutti gli attori della sicurezza: produttori, progettisti, installatori, clienti finali.

Carlo Hruby, amministratore delegato di HESA S.p.A, ha lanciato un messaggio molto incisivo sulla necessità di “governare il cambiamento” da parte degli installatori: “*La consapevolezza di aver scelto la strada dell’evoluzione, unica alternativa all’estinzione dell’installatore di sicurezza professionale che, come era stato visto nella scorsa edizione svoltasi ad Arese nel maggio 2014, è sempre più schiacciato sia dalla fascia alta del mercato, rappresentata dai main contractor e dai system integrator, che dalla fascia bassa degli elettricisti e degli impiantisti. Il ruolo di HESA come alleato strategico rende possibile l’attuazione di questa evoluzione, offrendo alla rete dei propri partner Concessionari e Installatori Autorizzati le migliori tecnologie oggi presenti sul mercato affiancate dalla più completa gamma di servizi esclusivi. Per poter sfruttare al meglio gli importanti strumenti che HESA offre è necessario però che le aziende di installazione mettano a punto a loro volta una strategia che sappia valorizzarli.*”

Carlo Hruby ha quindi dedicato particolare attenzione all’analisi del contesto, passaggio essenziale per individuare le nuove tendenze del mercato e poter adeguare di conseguenza le proprie strategie: “*In un momento storico come quello attuale, che vede in Italia i furti*

eldes

IL PRODOTTO PIÙ INNOVATIVO PER LA SICUREZZA

ESPANDIBILE FINO A 16 DISPOSITIVI SENZA FILI

EPIR3

Tutto in uno

www.dias.it

dias
Sicurezza quotidiana.

in abitazione più che raddoppiati negli ultimi 10 anni - come hanno recentemente rivelato il Censis e Transcrime in due differenti ricerche - e una crescita del nostro settore riscontrata sia a livello mondiale sia a livello nazionale, si confermano per il nostro mercato delle interessanti opportunità, soprattutto nei segmenti residenziale e commerciale dove, secondo una ricerca condotta da ***IHS Research****, entro la fine del 2015 si avrà una crescita a livello mondiale rispettivamente del 9,4% e del 5,9%, pur in un contesto economico ancora incerto. In questo scenario pare andare bene anche l'Italia dove, stando alle anticipazioni di* ***Anie Sicurezza,*** *nel 2014 il nostro settore avrebbe fatto registrare una crescita del 5%, pari a circa la metà del tasso di crescita a livello mondiale, ma certamente migliore dello 0,9% di incremento dell'anno passato.*"

"*In questo contesto, ancora pochi professionisti della sicurezza si rendono però conto che, per trarre vantaggio dalle opportunità che si profilano all'orizzonte, occorre porre al centro della propria strategia il cambiamento, che deve essere costante e continuo* – ha quindi concluso Hruby - *Per un'azienda di installazione che voglia continuare ad essere competitiva, questo significa adattare la propria struttura e modificare i propri piani velocemente, in base alle evoluzioni del mercato, saper cogliere rapidamente le opportunità commerciali e saper utilizzare al meglio gli strumenti tecnici e commerciali di cui dispone. Per questo motivo, il Meeting dei Concessionari e Installatori Autorizzati HESA – che da sempre si configura sia come momento indispensabile per fare un bilancio dell'attività sia come vetrina dove i più qualificati professionisti della sicurezza possono conoscere in anteprima le ultime novità di prodotto - assume quest'anno una rilevanza ancora maggiore. Pone infatti al centro dell'attenzione una profonda riflessione sulle strategie da adottare affinché i più qualificati operatori del settore possano trasformare i problemi in opportunità ed essere i veri protagonisti del cambiamento*."

Con una premessa di questo genere, le novità tecnologiche presentate al Meeting hanno assunto un particolare rilievo, configurandosi come "strumenti" individuati da HESA e messi a disposizione dei propri clienti per aiutarli a governare il cambiamento. In particolare, le novità introdotte per la **Centrale Serie Quaranta** che, a un anno dalla presentazione, ha riscosso il consenso unanime degli installatori. Le centrali Serie Quaranta sono la punta di diamante della proposta HESA riservata ai professionisti della sicurezza che aderiscono alla rete dei Concessionari e degli Installatori Autorizzati. Sviluppate con le più avanzate tecnologie oggi disponibili a livello mondiale, rappresentano lo stato dell'arte e l'eccellenza nella protezione antintrusione e sono state progettate in esclusiva per HESA con l'obiettivo di rispondere con la massima affidabilità e flessibilità alle particolari esigenze di sicurezza del mercato italiano.

FLIR, OPTEX e SAMSUNG TECHWIN sono i produttori che hanno partecipato per la prima volta al Meeting, presentando ognuno le ultime novità introdotte sul mercato italiano.

Tra le novità annunciate da HESA all'Isola d'Elba, si segnalano le telecamere termiche FLIR Serie T41, un range essenziale, composto da due telecamere Bullet di medie dimensioni, da due Mini Bullet e da una telecamera di tipo Dome brandeggiabile.

Nell'ambito della protezione per esterno, la gamma OPTEX è la più completa oggi presente sul mercato italiano. Da sempre particolarmente apprezzata per la grande affidabilità, comprende i rivelatori Redwall SIP, da oggi anche IP. Dotati di doppio PIR, rappresentano la soluzione ideale per una protezione di aree esterne anche di dimensioni molto estese.

Qualità, integrazione e semplicità di utilizzo sono alla base della nuova gamma di telecamere WiseNetLite IP Full HD di SAMSUNG TECHWIN, disponibili ora tra i prodotti per la videosorveglianza del catalogo HESA. Si tratta di una linea composta da 10 nuove telecamere, Bullet IR, Minidome da interno e MiniDome antivandalo da esterno, con risoluzione 2 Megapixel Full HD o 1,3 Megapixel HD.

iseo.com

ISEO®

LA MIA CHIAVE È SMART.

Argo
Iseo App

Apri, controlla e gestisci gli accessi.
Basta lo smartphone e Argo App di ISEO.

Con Argo e il cilindro elettronico Libra Smart, apri la porta con il tuo smartphone. Puoi anche consentire l'accesso a locali riservati, a persone selezionate e per periodi prestabiliti, verificando orari, giorni di ingresso e... molto altro ancora.

>> INFO.ISEOZERO1@ISEO.COM

Numero Verde
800 101971

Da Verizon i 20 termini per la protezione dei sistemi IT in azienda

a cura della Redazione

Il rischio che un'azienda possa subire attacchi informatici è sempre più elevato: il problema non è più il **se**, ma il **quando** e - nell'eventualità - essere consapevoli del genere di minaccia che si deve affrontare, fondamentale per poter predisporre le misure adeguate.

Un tema di estrema attualità anche per il mondo della sicurezza fisica: se l'avvento delle tecnologie over IP a metà degli anni '90, aveva aperto una prima breccia nel "muro" che la divideva da quella logica, l'Internet of Things (IoT) lo sta abbattendo del tutto. Si sta delineando di conseguenza uno scenario nuovo, al quale dedicheremo in permanenza nella piattaforma **essecome/securindex.com** ampio spazio con informazioni "trasversali" ai due ambiti, per fornire un contributo di conoscenza agli operatori di entrambi i settori.

Iniziamo con un glossario realizzato da **Verizon** dei 20 termini più comuni legati alla cybersecurity che si devono conoscere per poter proteggere il proprio business dagli hacker. Una volta riconosciuta la minaccia, il **Verizon Data Breach Investigations Report (DBIR) 2015** vi fornirà la chiave di lettura per affrontarla al meglio.

- ***Detection deficit*** – il deficit di rilevamento è il tempo che intercorre tra una violazione e la sua scoperta
- ***Malware*** – termine generico che indica diverse forme di software malevoli progettati per danneggiare intenzionalmente un sistema o accedervi senza che amministratori o proprietari ne siano consapevoli
- ***Crimeware*** – malware che punta al controllo dei sistemi per condurre attività illegali
- ***RAM-scraping malware*** – Memory-scraping malware utilizzato dagli hacker per accedere a dati sensibili non raggiungibili con altre metodologie di attacco
- ***Keylogger malware*** – questo malware si installa da browser nel corso di una navigazione in rete o quando si scarica un software. Una volta attivo il software registra quanto digitato dall'utente, come login o indirizzi email, e trasmette a un remote service le informazioni raccolte
- ***Exploit kit*** – si tratta di un attacco informatico pre-packaged, utilizzabile anche da chi ha poca esperienza nel cybercrime. Varia in complessità e nel genere di vulnerabilità che attacca, ma la caratteristica che lo contraddistingue è la facilità di implementazione. Hacker alle prime armi in

genere adottano questo tipo di minaccia grazie a interfacce user-friendly che rendono più facile indirizzare l'attacco e gestirlo.

- ***CVE*** – acronimo per *Common Vulnerabilities and Exposure*, è un dizionario di informazioni note al pubblico che raccoglie le vulnerabilità e i rischi più comuni in rete
- ***CVSS*** – acronimo per *Common Vulnerability Scoring System*, è un metodo aperto e standardizzato per la classificazione delle vulnerabilità in ambito IT
- ***JBOH*** – acronimo per *Java-Script-Binding-Over-HTTP*, è un programma che permette agli hacker di eseguire codici da remoto su dispositivi Android in cui sono installate App infette
- ***IDS or IPS*** – acronimo per *Intrusion Detection Systems or Intrusion Prevention Systems*, può essere un software o un dispositivo fisico e serve a monitorare un sistema o una rete per individuare eventuali attività malevole in corso
- ***VERIS*** – acronimo per *Vocabulary for Event Recording and Incident Sharing*, rappresenta una serie di metriche sviluppate per fornire un linguaggio comune utile a definire gli incidenti di sicurezza in maniera strutturata e replicabile
- ***Intrusioni POS*** – si definiscono intrusioni nei sistemi *Point-of-Sale* quegli attacchi che avvengono sui dispositivi utilizzati come terminali di pagamento. Il dispositivo può essere uno dei vari registratori di cassa digitali utilizzati in diversi settori
- ***Skimmer per carte di pagamento*** – lettori di carte malevoli inseriti dagli hacker nei terminali utilizzati per i pagamenti, quali sportelli ATM o altri dispositivi attraverso cui si effettuano transazioni con carte di pagamento, per copiare i dati dalla banda magnetica
- ***Attacchi a Web app*** – attacchi web-based che possono assumere forme diverse, ma comunemente definiti dall'utilizzo dei protocolli *https* o *http*. L'attacco generalmente ha come obiettivo la sicurezza di un sito internet o il traffico dati ad esso collegato e, in alcuni casi, può arrivare a oscurare o interrompere completamente l'attività di un sito
- ***Attacchi DDoS*** – le minacce *Distributed Denial of Service* hanno come obiettivo di impedire agli utenti di utilizzare le risorse online, sovraccaricando la rete con traffico malevolo generato arbitrariamente

- ***Phishing*** – tentativo fraudolento di ottenere dati sensibili e riservati spacciandosi per un'azienda legittima (in genere organizzazioni finanziarie come istituti di credito) e richiedendo tali dettagli via email.
- ***Cyberespionage*** – l'atto di sottrarre informazioni sensibili registrate in formato digitale e archiviate in computer o reti appartenenti a società o a organizzazioni governative.
- ***Botnet*** – serie di computer compromessi da malware e collegati tra loro in un network controllato da remoto. Il gestore del botnet può impartire ordini ai computer infetti facendo loro compiere qualunque azione, tipicamente attacchi DDOS o invii di email spam.
- ***Ransomware*** – malware sviluppati con l'obbiettivo specifico di bloccare l'accesso a sistemi o informazioni fino a quando non sarà pagato un riscatto.
- ***Clickfraud*** – l'azione di registrare in maniera artificiale i click associati a una campagna di pubblicità online basata sul pay-per-click (PPC), simulando così la visita da parte degli utenti. I click sono tipicamente realizzati attraverso una persona o con un programma specifico.

http://news.verizonenterprise.com/2015/05/cyber-security-definitions-enterprise-data-breach/

Uno sguardo dal ponte: da Londra segnali chiari sul futuro della sicurezza

di Raffaello Juvara

Il rito dell'incontro primaverile degli operatori della sicurezza in terra d'Albione si è celebrato quest'anno all'insegna di un'apprezzabile concretezza. Quasi scomparsi gli stand faraonici che in passato avevano sottolineato e, in qualche modo, determinato l'unicità planetaria dell'evento inglese, la maggior parte degli espositori affezionati ha scelto allestimenti semplificati, quasi a sottolineare che IFSEC è diventata oggi una delle tappe del roadshow continuo che sono tenuti a fare per incontrare i clienti nel loro bacino di residenza e presentare soluzioni rispondenti alle esigenze dei rispettivi mercati. Una formula che gli operatori della sicurezza del Regno Unito dimostrano di apprezzare, affollando a ondate gli stretti corridoi di ExCel.

Quanto ai contenuti, da questa edizione di IFSEC sono emersi segnali piuttosto chiari sullo scenario in divenire della sicurezza, in relazione sia all'evoluzione tecnologica complessiva che agli assetti strategici del mercato globale.

L'evoluzione delle tecnologie

Sul piano delle tecnologie, protagonisti assoluti sono stati gli spettacolari sviluppi nella definizione delle immagini video e delle consequenziali applicazioni in ambito security e intelligence. La diffusione dello standard H265 ha appena aperto la strada al video ultra HD 4K, ormai presente anche nei box del China Pavillion con i produttori di Shenzen, e già la canadese **Avigilon** ha presentato la telecamera 7K HD

Pro con sensore a 30 Mp: una risoluzione di 7.360 pixel in orizzontale e 4.128 in verticale, che consente una definizione dei dettagli finora inimmaginabile. È stato spiegato in conferenza stampa che *Sharper* & *Smarter*, gli attributi di comunicazione assegnati alla tecnologia 7K, ne sintetizzano gli effetti pratici, 'il potere di vedere quello che una volta non si vedeva; la possibilità di utilizzare immediatamente le immagini per agire prima, non per reagire'.

Del resto, il numero sempre maggiore di informazioni messe a disposizione dalle immagini è elaborabile a piacimento, in funzione delle esigenze di utilizzo: dalla business intelligence all'anti terrorismo, dal controllo del traffico alla telemedicina, alla prevenzione incendi: la telecamera diventa un sensore multi-funzione sulla scena, con una conseguente dominanza gerarchica della parte video nel sistema complessivo di sicurezza. **Richard Lewis** di **Canon Europe** ci ha confermato la focalizzazione del leader mondiale nell'*imagine* sul tema della business intelligence, e le linee strategiche annunciate l'anno scorso in occasione dell'acquisizione di **Milestone Systems**, il leader mondiale nelle piattaforme aperte di gestione video (VMS). La crescita a due cifre della videosorveglianza a consuntivo e in previsione hanno convinto in gruppo giapponese a concentrarsi sul segmento, attraverso l'acquisizione di aziende leader nei rispettivi comparti (Milestone nel 2014 e AXIS nel 2015).

Stuart Rawling di **ONVIF** ci ha spiegato che il ruolo del più importante standard mondiale nella videosorveglianza IP è oggi quello di facilitare il processo di integrazione tra i sistemi video e gli altri sistemi di sicurezza, essendo questa l'esigenza espressa dai costruttori che, a loro volta, rispondono agli stimoli provenienti dal mercato. Va in questa direzione anche il recente rilascio di un Client Test Tool per la verifica

IL 100% DEI DIPENDENTI ITALIANI DI SIEMENS SP È PASSATO IN VANDERBILT

Rientra a pieno titolo nell'assestamento globale del mercato della sicurezza il perfezionamento dell'acquisto di **Siemens Security Products** da parte di **Vanderbilt**, il nuovo global player americano della sicurezza e del controllo accessi fondato e condotto da **Joe Grillo**. L'abbiamo incontrato assieme a **Valerio Vittone,** Country Head Security Products di Vanderbilt, e ci ha spiegato innanzitutto che l'acquisizione è diventata completamente operativa dal 1° giugno, con il trasferimento del 98% dell'organico complessivo di Siemens SP ma del 100% di quello italiano:" *Ho voluto confermare tutto il gruppo di lavoro perché, soprattutto in Italia, la sicurezza è un mercato di relazione, dove contano molto le conoscenze personali. I clienti hanno dimostrato di apprezzare questo*".

Parlando dei prodotti, il ceo di Vanderbilt ha sottolineato: "*Partiamo da una gamma completa, a livelli di eccellenza assoluta. Con i sistemi antintrusione SPC, i più venduti nel centro e sud Europa, il controllo accessi Aliro, pensato anche per le PMI e la linea di NVR Vectis iX, nessun altro produttore ha un catalogo come il nostro, e adesso sono in arrivo altre novità, a ulteriore completamento di una gamma totalmente interoperabile".*

"*Vanderbilt si rivolge ai grandi clienti direttamente e attraverso Siemens Building Technologies"* continua Grillo: *Tramite la rete di distributori, andiamo verso tutti i più importanti mercati verticali: pubbliche amministrazioni, oil & gas, industrie, scuole, PMI, banche, retail. Vanderbilt sarà uno dei protagonisti del mercato della sicurezza anche in Italia."*

della conformità dei prodotti ai Profili S, G e C.
Il video cresce e si espande: a IFSEC 2015 **Dahua Technology,** secondo produttore cinese di sistemi di videosorveglianza, ha presentato una gamma completa di sistemi di controllo accessi, antintrusione e video-citofonia, con il dichiarato obiettivo di proporsi sul mercato globale come fornitore unico nei confronti dell'installatore di sicurezza. Tutto fa presagire che altri top vendor di video seguiranno questo percorso che, del resto, **AXIS Communications** aveva iniziato già nel 2013 con il sistema di controllo accessi A1001.
Del tutto coerente con questo scenario è lo sviluppo delle applicazioni di analisi video, che a IFSEC spaziavano negli ambiti più estesi. Particolarmente significativa è stata la conferenza di **Richard Berkeley,** responsabile delle indagini forensi di **Scotland Yard,** che ha spiegato come sia stato possibile arrivare a identificare e processare centinaia di persone responsabili di atti vandalici durante i disordini avvenuti in Inghilterra nell'estate del 2011, grazie all'utilizzo massiccio delle prove video, ottenute mediante un approccio scientifico utilizzato per la prima volta dalla polizia. Un passaggio che ha cambiato per sempre le modalità di raccolta e di analisi delle immagini raccolte dai sistemi di videosorveglianza.

I nuovi equilibri nel mercato globale
Girando per gli stand a IFSEC 2015, è venuto spontaneo domandarsi quanti fossero i global player europei in grado di competere a livello mondiale nel mercato della sicurezza, a prescindere dalla loro presenza o meno in fiera. La risposta è stata che nella produzione di tecnologie sono rimaste solamente PMI, magari a livello di assoluta eccellenza, ma non in condizioni di reggere la concorrenza con i giganti dell'area del Pacifico. Negli USA si è creata una specializzazione nel controllo accessi e se Vanderbilt è entrata nella sicurezza comperando la BU di Siemens SP (vedi box), il 1° luglio Allegion ha comprato SimonsVoss, una PMI tedesca da 50 milioni di euro di fatturato specializzata in sistemi di chiusura digitalizzati.
Nel settore video, ben si sa, è in corso una furibonda battaglia tutta orientale (Cina, Corea e Giappone), con il resto del mondo a guardare (e comprare telecamere…). C'è solo da sperare che le eccellenze europee e nord-americane del comparto mantengano l'autonomia delle rispettive sedi, gestendo in proprio quei rapporti "ad personam" con i clienti che nella sicurezza fanno ancora la differenza.

E l'Italia? Si potrebbe dire che la situazione sia stata "plasticamente" rappresentata dalle presenze a IFSEC: di anno in anno diminuiscono le aziende con la voglia (o la possibilità) di sostenere i costi di partecipazione a quella che una volta era la vetrina mondiale della sicurezza, oggi un affaccio al mercato britannico.

milestone

The Open Platform Company

Presentate a MPOP 2015 le prime soluzioni sui Metadata dei partner Milestone

Prima parte

a cura della Redazione

L'edizione 2015 di **MPOP** (Bologna, 22-23 aprile), l'incontro annuale di **Milestone Systems** con i partner e i clienti, è stata l'occasione scelta dai manager della multinazionale danese, entrata a far parte del gruppo **CANON** nel 2014, per fare il punto della situazione sulle possibilità di utilizzo dei *metadata,* un tema di valenza essenziale per lo sviluppo dell'analisi video.
Milestone aveva avviato nel 2012 un progetto triennale di ricerca assieme all'Università Tecnica di Danimarca (DTU)**,** all'Università di Aalborg, al gruppo svedese Securitas AG e alla statunitense Nabto inc, finanziato con 15 milioni di corone danesi dalla Fondazione Nazionale Danese, "per sviluppare l'interpretazione del materiale videoregistrato in modo che il contenuto possa venire descritto automaticamente".
(www.securindex.com 1/8/2014).

Jorgen Skovgaard, vice presidente di R&D di Milestone Systems, presentando alla stampa internazionale il progetto lo scorso anno, aveva dichiarato: "*Siamo ancora nella prima fase di questo progetto e ci aspettiamo di presentare al mercato diverse soluzioni innovative per la ricerca sull'uso dei metadata, il cui framework è già stato rilasciato con Xprotect 2014.*
Nelle prossime fasi, punteremo la ricerca, fra l'altro, sulle possibilità che il software possa distinguere nelle immagini video le situazioni normali da quelle anomale. Questo significherebbe che la videosorveglianza può generare proattivamente un allarme prima che avvenga un incidente e consentirne ulteriori utilizzi come strumento di lavoro in molteplici scenari operativi".
Skovgaard aveva poi concluso: "*Le possibilità sono praticamente infinite, con lo sviluppo costante della tecnologia del nostro software video. Possiamo immaginare che ci sarà una marea di nuove soluzioni sviluppate dai nostri partner, costruite sulla piattaforma aperta di videosorveglianza di Milestone*".
Alla scadenza del triennio, vengono puntualmente annunciate le prime soluzioni sviluppate dai partner italiani di Milestone, che **essecome/securindex.com** presenterà in un approfondito servizio a puntate, per introdurre un argomento che avrà un grande rilievo nell'evoluzione della sicurezza nel prossimo futuro.

Il servizio inizia con un'intervista a **Ivan Piergallini,** Channel Business Manager, Central & Southern Italy.

La progressione dei sistemi in rete, con l'integrazione sempre più avanzata tra video, controllo accessi, antintrusione e sistemi eterogenei (energia, clima, fire ecc) sta facendo evolvere anche funzione e ruolo dei VMS. Ci può descrivere lo scenario attuale e futuro che Milestone ha delineato?
La convergenza dei servizi di sicurezza fisica nelle infrastrutture "IP" della rete informatica sta rivoluzionando il modo di progettare, realizzare e manutenere i nuovi sistemi di videosorveglianza e di sicurezza in generale. Tale rivoluzione diventa ogni giorno più endemica offrendo integrazioni software e hardware di ogni genere, creando interessanti applicazioni nei diversi mercati verticali e nuove opportunità di business in settori dove prima la videosorveglianza non sarebbe stata facilmente associata o i sistemi di sicurezza sarebbero stati gestiti in modo chiuso ed indipendente. Grazie alla sua piattaforma aperta con interfacce di programmazione dell'applicazione (API) pubblicate, disponibili e documentate nel dettaglio, attraverso il Software Development Kit Milestone offre agli utenti di integrare applicazioni e sistemi di terze parti dell'area sicurezza, automazione, controllo ed altro che si intende monitorare, o interfacciare per lo scambio di informazioni. La Strategia è nulla senza la Cultura. Milestone ha le sue radici nella cultura dell'Open Platform, dell'integrazione, della scalabilità, della flessibilità e facilità di utilizzo da parte dell'operatore, ed è pronta già per il futuro.

Ci può parlare delle soluzioni sviluppate da Milestone e dai suoi partner per i principali mercati verticali (retail, banche, infrastrutture critiche ecc) che danno la possibilità di gestire anche funzionalità diverse da quelle di sicurezza come, ad esempio, la business intelligence?
La cultura, la ricerca e l'esperienza nei principali mercati di riferimento di Milestone offrono al partner la possibilità cambiare prospettiva, di vedere le necessità dal lato del cliente al fine di vedere le opportunità e poter offrire delle soluzioni, non dei prodotti. Nell'ambito Retail in particolare le integrazioni dei Partner Milestone, come il conteggio delle persone, il monitoraggio dei POS/ATM, i software di analisi video per la mappatura zone calde, il mascheramento, il riconoscimento facciale, l'identificazione dell'età e del genere, possono offrire soluzioni di sicurezza ma allo stesso tempo il beneficio al cliente di analisi e gestione dei dati di un negozio, utili per poter gestire al meglio lo staff nei vari punti vendita o di decidere come disporre una particolare tipologia di merce.

A MPOP 2015 si è parlato di metadati, un capitolo fondamentale nell'evoluzione dei software di analisi degli eventi. Come si propone Milestone nei confronti di questo tema?
Le nuove tecnologie hardware, con telecamere sempre più potenti e capaci di trasformarsi oggi da semplice occhio che osserva a intelligenza che interagisce con eventi, situazioni, oggetti, e tecnologie software avanzate stanno favorendo la conoscenza e l'utilizzo dei *metadati*, intesi come lo strumento in grado di decifrare migliaia di terabyte di dati in informazioni utili, correlate tra loro con criteri scelti, ovvero la capacità di trovare velocemente le informazioni cercate in un mondo ormai troppo ricco di informazioni digitali. Milestone dispone già di un framework standard Onvif in grado di immagazzinare tutti i metadati in modo "leggibile" ed "interrogabile", di una piattaforma standard ed aperta in grado di rendere disponibili tutte le informazioni di contesto ricercate collegate in modo "intelligente" alle immagini. La piattaforma di gestione diventa il vero centro intelligente del sistema di videosorveglianza con Milestone, offrendo oggi con la struttura dei metadati la possibilità di una ricerca centinaia di volte più veloce degli eventi ed immagini di interesse e domani la capacità del rilevamento automatico di attività o situazioni "anomale", rendendo il sistema di videosorveglianza pro-attivo allertando l'operatore prima che si verifichi un problema.

milestone

The Open Platform Company

Cosa sono i Metadata: la parola all'esperto

contributo di Frediano Di Carlo, Consulente per la sicurezza e le tecnologie

Introduzione

Il mercato della videosorveglianza continua inarrestabile la propria crescita e le telecamere aumentano nelle nostre città di giorno in giorno e, con esse, l'ingente mole di dati dai quali estrarre informazioni d'interesse pubblico e privato.

Di recente, abbiamo assistito, tramite i mezzi d'informazione, a incoraggianti risultati investigativi delle FF.OO., anche per mezzo della videosorveglianza.

Si pensi al caso di **Yara Gambirasio,** nel quale una prova importante è costituita dalle riprese di più passaggi del furgone dell'inquisito nelle zone d'interesse delle indagini; o al caso del piccolo **Loris Stival,** nel quale una prova determinante a carico della madre, presunta assassina, è data dalla ricostruzione degli spostamenti effettuati la mattina della scomparsa del piccolo, grazie all'analisi di diversi filmati di telecamere della zona.

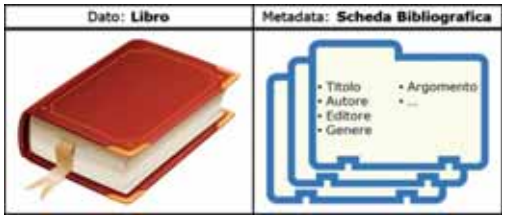
Eppure, ci sono voluti giorni per raggiungere tali risultati, tempi di certo inadeguati in caso d'indagini dove il fattore tempo è determinante. D'altra parte, a pensarci bene, non potrebbe essere altrimenti: ancora oggi, per la ricerca d'informazioni dalla videosorveglianza si utilizza la stessa fonte degli esordi di tali sistemi, la registrazione video. Ultimamente, è corredata da alcuni strumenti per velocizzare le ricerche, ma sempre legati a eventi predeterminati d'interesse e non, come negli esempi precedenti, a eventi che fuori dello specifico contesto rappresentano la semplice normalità.

Questa situazione è destinata purtroppo a peggiorare, al crescere del numero di telecamere e della complessità degli eventi da ricercare.

Per venire incontro a tali inconvenienti e arricchire il contenuto informativo delle scene riprese, alcuni mesi fa ONVIF ha rilasciato delle specifiche sulla gestione del Metadata. Il presente articolo ne descrive i contenuti, l'utilizzo e, soprattutto, le potenzialità destinate a mutare profondamente il concetto di Ricerca degli Eventi.

Etimologia

Il termine **Metadata** deriva in parte dal Greco **meta** (μετα), che significa *con*, *oltre*, *dopo*, e dal Latino **data** (plurale di datum), che significa *dati*, *informazioni*. Il significato è dunque "con le informazioni", "oltre le informazioni"; una definizione adatta allo scopo è **Ulteriori Informazioni *(sui Dati)***.



Un esempio per chiarire: se il nostro dato è rappresentato da un Libro, possibili altre informazioni sullo stesso, ossia un set di metadata, sono rappresentate dalla Scheda Bibliografica.
Sovente si utilizza anche il termine TAG, ma si tratta di un'espressione impropria, essendo esso uno degli elementi costituenti i metadata, per completare l'esempio precedente:

Attività di Standardizzazione

Non è del tutto corretto parlare di **standard** per i metadata, essendo tali informazioni le più disparate possibile e ciascuna con propria specificità.
Se, comunque, si esegue una ricerca in Rete utilizzando i termini *metadata* e *standard*, emergono preponderanti risultati legati allo standard ISO 19115, definito "Geographic Information – Metadata"; non meraviglia scoprire che la maggior parte delle attività degli enti normatori sono rivolte alla standardizzazione delle informazioni di geolocalizzazione, visto il ruolo primario ricoperto dalle stesse nell'attuale vita quotidiana.
Per trovare informazioni specifiche su attività di standardizzazione d'informazioni legate ai filmati ovvero, più generalmente ai contenuti multimediali, è necessario risalire agli anni a cavallo tra la fine del secolo scorso e l'inizio dell'attuale, quando fu costituito il gruppo **MPEG** (Motion Picture Expert Group), il cui leader riconosciuto è il nostro **Leonardo Chiariglione** (http://www.chiariglione.org/), tuttora parecchio attivo nello specifico settore.
Il gruppo mise a punto i seguenti standard, pesantemente entrati nella nostra vita quotidiana:

MPEG-1: ISO/IEC 11172 (1993) – «Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s»

- come supporto per la nuova codifica video fu introdotto il "**Video CD**";
- la nuova codifica audio prese il nome di **mp3**, contrazione di "MPEG1 Layer 3", derivante dal fatto che la stessa era specificata dal terzo documento (layer) dello standard.

MPEG-2: ISO/IEC 13818 (1994) – «Generic coding of moving pictures and associated audio information»

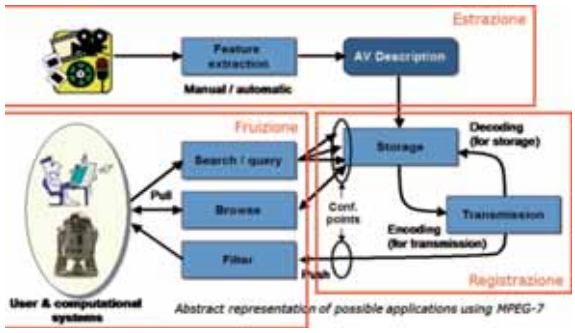
- come supporto per la nuova codifica video fu introdotto il "**DVD**", *Digital Versatile Disk* o *Digital Video Disk*;
- fu introdotta una nuova codifica audio che prese il nome di **aac**, *Advanced Audio Codec*.

MPEG-4[1]: ISO/IEC 14496 (1999) – «Coding of audio-visual objects»

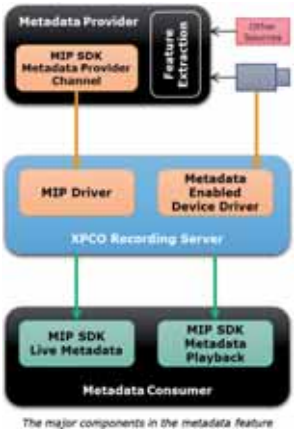
- come supporto per la nuova codifica video fu introdotto il "**Blue Ray Disk**";
- la codifica audio rimase la precedente **aac**;
- nel 2003 fu introdotta, con il Layer 10, una nuova codifica video nota con il termine **H.264** (frutto del lavoro del Gruppo Misto costituito da MPEG e ITU-T, *International Telecommunication Union*);
- sempre nel 2003 il Layer 14 introdusse il formato file **mp4**.

Nel 2002 fu promulgato lo standard **MPEG-7** (ISO/IEC 15938) «Multimedia Content Description Interface», che rappresenta lo standard di Metadatazione dei contenuti Multimediali applicabile ai precedenti MPEG-4, 2, 1[2].

La figura a lato, tratta dalla documentazione dello standard, illustra schematicamente il meccanismo di estrazione, salvataggio e successivo utilizzo, dei metadata.



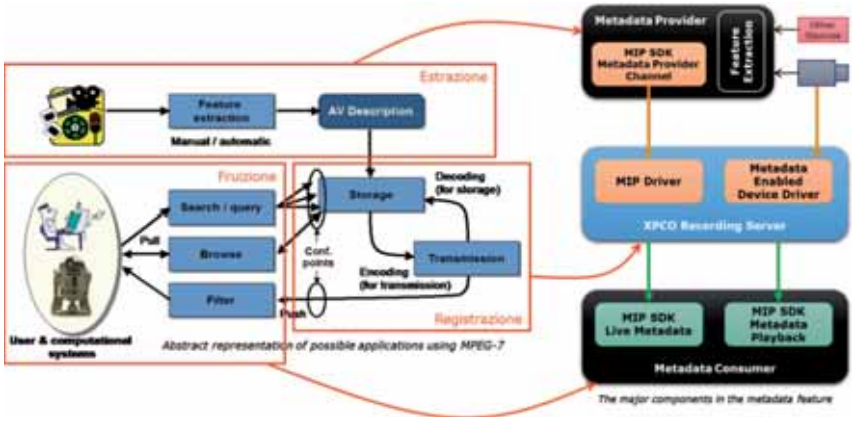
1. Nota storica: la sigla MPEG-3 non fu utilizzata per evitare possibili confusioni con mp3.
2. Nota storica: la sigla MPEG-7 fu derivata proprio dall'applicabilità di tale standard a tutti i 3 precedenti (4+2+1 = 7).



The major components in the metadata feature

Uno dei produttori che per primo ha implementato sulla propria piattaforma le funzionalità dei metadata, così come specificate da ONVIF, è stato **Milestone** che le ha rese disponibili lo scorso anno con il SDK 2014; nella documentazione è stata utilizzata l'immagine a sinistra per illustrarne i principi di funzionamento.

Da questa ulteriore immagine è facile dedurre che i due schemi in linea di principio coincidano perfettamente:

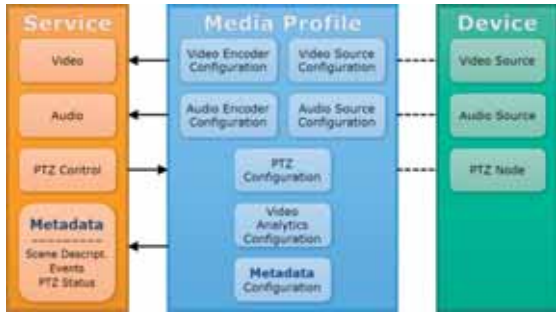


The major components in the metadata feature

ONVIF

Le entità coinvolte nella gestione dei metadata per **ONVIF** sono le seguenti.

Le specifiche dei componenti sono descritte nel documento **Analytics Service Specification,** attualmente rev. 2.5, mentre quelle del WEB Service nel documento "Analytics Service WSDL" (*Web Service Description Language*), attualmente rev. 2.2.



Il paragrafo 5.1 delle Specifiche, intitolato **Scene Description Interface**, elenca gli elementi normati da ONVIF che, alla revisione attuale sono:

Data/Ora (*timestamp*) dell'evento

Posizione (all'interno della scena)

Elementi della Scena, costituiti da:

- **Oggetti**
- **Alberi di Oggetti** (Object Tree), utilizzati per descrivere Oggetti multipli, es. quando due oggetti si avvicinano tanto da non essere più tracciati singolarmente
- **Descrittori delle Sagome** (*Shape Descriptor*), insiemi di elementi geometrici che descrivono il contorno degli oggetti. Al minimo, un descrittore deve contenere il rettangolo che circonda l'oggetto (*Bounding Box*) e il Centro di Gravità (punto che descrive la traiettoria dell'oggetto)
- **Colore**
- **Descrittori delle Celle di Rilevamento degli Oggetti** (*Motion In Cells Descriptor*), la zona della scena dove avviene il rilevamento dell'oggetto
- **Descrittori della Classe degli Oggetti**, che possono essere: **Animali · Volti · Persone · Veicoli · Targhe · Gruppi · Altro.**

È doveroso sottolineare come tali elementi costituiscano il solo insieme di base: è infatti possibile, grazie all'uso del XML (*eXtensible Markup Language*) per la descrizione della scena, aggiungere ulteriori elementi (*tag extension*), oltre a quelli previsti, tramite il costruttore "**Extension**".

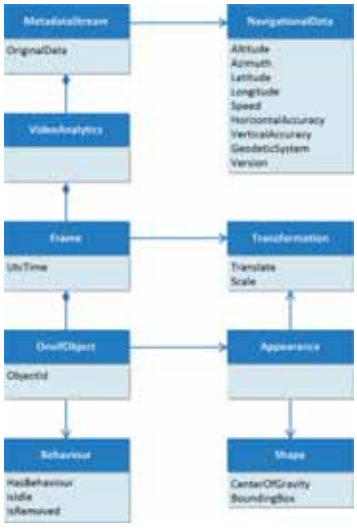
La stessa Milestone ha introdotto la prima estensione nel proprio SDK, rendendo disponibile una prima versione (1.0) dei dati di geolocalizzazione, definiti di "Dati di Navigazione", la cui struttura XML è la seguente.

Le definizioni degli campi costituenti il blocco dell'estensione sono quelle riportate in tabella.

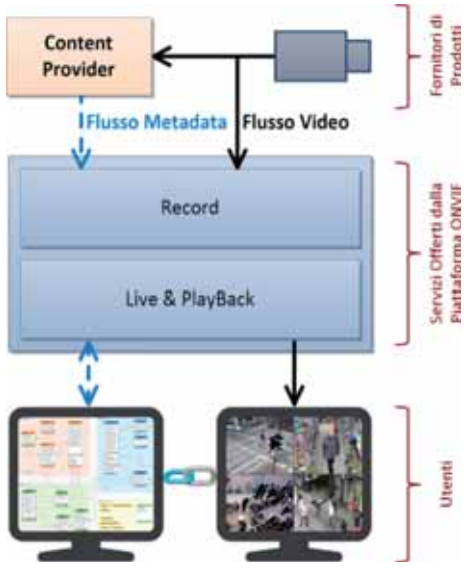
Table 1: Definition of fields in Milestone navigation data format

Field	Description
NavigationalData	This is the container tag for all the navigational data. It is located directly inside the MetadataStream node.
Latitude	In degrees. A double from -90 to +90
Longitude	In degrees. A double from -180 to +180
Altitude	Measured in meters. A double
Azimuth	Aka bearing or course, this is the device angle to true North. Measured in degrees with a double from -180 to +180
HorizontalAccuracy	Horizontal accuracy measured in meters. A positive double
VerticalAccuracy	Vertical accuracy measured in meters. A positive double
Speed	The speed of the device. A non-negative double.
GeodeticSystem	Defines how to interpret the coordinates and altitude. If not present, a value of WGS84 is assumed.

Infine di seguito lo schema delle (principali) classi utilizzate.



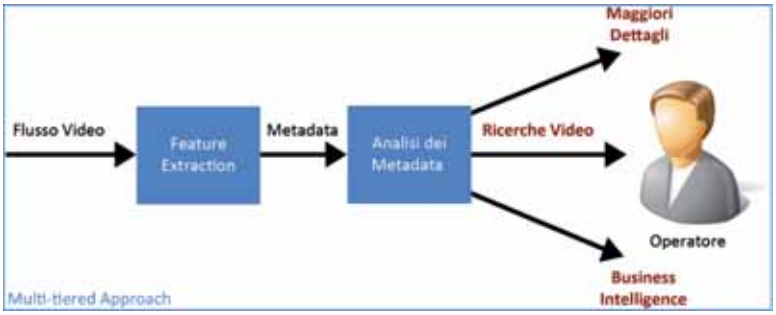
È facile immaginare, per esempio, che ai Veicoli possano essere associati altri dati quali la Classe (moto, auto, autocarro, ecc.), il Colore, la Velocità ecc., così come ai Volti il Sesso, la Classe d'Età (giovane, adulto), le Caratteristiche Morfologiche, le Espressioni, ecc. In pratica le informazioni supplementari (Metadata) che possono essere abbinate a un filmato, sono virtualmente infinite. L'immagine a destra illustra il flusso operativo, dalla generazione delle immagini fino alla fruizione dei filmati e relativi metadata, con l'indicazione degli attori in gioco.



Potenzialità dei Metadata

In una recente scheda informativa, **Agent Vi** (www.agentvi.com) utilizza i seguenti schemi per differenziare l'ap-

proccio tradizionale della Video Content Analysis, che definisce Monolitico, da quello innovativo con l'uso dei Metadata, che definisce Multilivello.



E correda tali immagini con la seguente tabella.

	APPROCCIO MULTILIVELLO	APPROCCIO MONOLITICO
Flessibilità	Alto	Basso
	Metadata molto dettagliati forniscono le basi per una varietà di applicazioni	Gli algoritmi dedicati sono ottimizzati per uno scopo specifico. Ulteriori funzionalità richiedono nuovi algoritmi
Esecuzione simultanea di più applicazioni	Facile	Difficile
	I Metadata sono creati una sola volta e utilizzati per varie applicazioni, con il minimo overhead aggiuntivo per ogni ulteriore applicazione	Ogni nuova funzionalità richiede uno specifico algoritmo che incrementa in modo significativo i requisiti di CPU e di memoria
Mix tra real-time e off-line	Facile	Difficile
	La creazione dei Metadata avviene in tempo reale, l'analisi degli stessi può essere intrapresa sia in tempo reale, sia in tempi successivi non in linea	L'intero algoritmo viene eseguito ogni volta sul flusso video, sia esso dal vivo, sia registrato

In sintesi è possibile affermare che l'utilizzo dei Metadata consente di ottenere le seguenti funzionalità aggiuntive:

- Disporre di maggiori **Dettagli degli Eventi** rilevati dal Sistema
- Velocizzare le **Ricerche** Video (degli Eventi) ed effettuare **Correlazioni** tra gli stessi
- Disporre di dati sui quali operare con algoritmi di **Business Intelligence**

Alcuni Possibili Esempi

Dettagli degli Eventi

Supponiamo di disporre di un filtro di analisi che rileva "Accesso Vietato in Zona a Senso Unico", all'accadere dell'evento avremo:

- con sistemi di Video-Analisi tradizionali:
  - notifica dell'evento e relativa osservazione visiva, in alcuni casi distinguendo tra persone e automezzi
- con sistemi corredati da Metadata:
  - notifica dell'evento e relativa osservazione visiva …
  - Tipo: Veicolo
  - Classe: Autocarro
  - Colore: Rosso
  - Targa: ED126YT
  - Velocità: 45 Km/h

Ricerche e Correlazioni

Supponiamo di dover verificare se un furgoncino rosso ha attraversato la precedente zona a senso unico:
con sistemi di Video-Analisi tradizionali:

- selezione di tutti gli eventi di attraversamento della zona e successiva osservazione visiva degli stessi alla ricerca del furgoncino rosso

con sistemi corredati da Metadata:

- selezione degli eventi di attraversamento zona con **Tipo = Veicolo**, **Classe = Autocarro** e **Colore = Rosso** e successiva eventuale osservazione visiva dei risultati

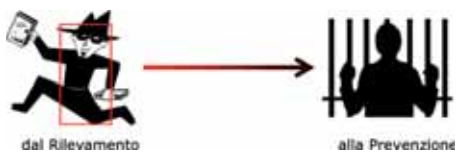
Supponendo che la nostra zona a senso unico sia nei pressi di una banca che ha subito un furto, grazie ai dati di cui disponiamo è facile verificare se la presenza del solito furgoncino rosso sia avvenuta, o si sia intensificata nel periodo del furto. Analogamente sarà possibile effettuare ricerche incrociate al fine di verificare se in concomitanza di diversi furti è presente la ricorrenza di una stessa vettura (stessa targa).

Business Intelligence

Supponiamo di avere una o più telecamere all'interno di un negozio, in corrispondenza di una vetrina, corredate da un sistema di analisi che rileva i volti dei passanti quando entrano nella scena e quando ne escono. L'algoritmo di "Face Detection" è regolato per il rilevamento di volti frontali di una data dimensione minima, per fare in modo che siano esclusi quelli lontani; è plausibile supporre che le riprese siano effettuate su passanti che osservano la vetrina:

- con sistemi di Video-Analisi tradizionali:
  - *è improbabile che, al momento, esistano sistemi di face detection, se non dedicati, che notificano l'uscita di scena*
  - con sistemi corredati da Metadata:
- con i dati a disposizione è possibile ricavare il **Tempo Medio di Osservazione**, per esempio, per **Classe d'Età** (Giovane, Adulto) e **Sesso**, fornendo informazioni su una sorta di "Indice di Gradimento" dell'allestimento della vetrina in funzione di tali categorie
- ma è anche possibile, con algoritmi appena un po' più sofisticati, raccogliere informazioni statistiche sulle **Emozioni** suscitate dalla vista della vetrina, disponendo in tal modo di dati utilizzabili per rendere più attraenti (*emozionanti*) i successivi allestimenti.

In sintesi, è possibile affermare che, tramite specifiche implementazioni SW che utilizzano i Metadata accumulati in un DB, sia possibile impiegarli a un livello superiore a quello della singola Scena, rilevando informazioni più articolate, con maggiore precisione e tempi decisamente inferiori, rispetto a quanto sia possibile fare con le tecniche tradizionali. Sofisticati algoritmi statistici possono consentire l'identificazione di modelli di comportamento dei fenomeni osservati, e fornirne accurate stime quantitative. L'utilizzo di tecniche di **Business Intelligence** sul tali analisi comportamentali permette di stimarne gli "Indicatori", la cui costante osservazione degli scostamenti consente di predire l'occorrenza degli eventi controllati; in pratica…



milestone

The Open Platform Company

Audio e video, l'annotazione automatica di A.I. Tech mediante metadata

contributo di Gennaro Percannella, Sales Manager, Pasquale Foggia, Chief Software Architect, A.I. Tech srl

Metadati e videosorveglianza?

Per rispondere a questa domanda proviamo a pensare al seguente scenario: centinaia di telecameraedi sorveglianza installate in un aeroporto. Qual è la probabilità che un operatore nella control room sia in grado di notare tempestivamente una persona che entra in un'area interdetta, o individuare un bagaglio abbandonato, o un comportamento sospetto di una persona? Studi scientifici dimostrano che dopo 20 minuti di osservazione continua un normale operatore non noterà oltre il 90% di eventi rilevanti. Si consideri inoltre il caso in cui, ore o giorni dopo che sia avvenuto un evento criminoso, si renda necessario ricercare all'interno di ore e ore di sequenze video catturate da decine di telecamere una persona vestita con colori specifici che passa attraverso una porta. Per ritrovare gli eventi d'interesse nelle sequenze non annotate l'operatore dovrebbe visualizzare tutti i video con l'elevato rischio già dopo pochi minuti di lavoro di perdere delle sequenze rilevanti. La video content analysis (anche detta analisi video intelligente o più brevemente analisi video) costituisce un insieme di tecniche alla frontiera con la ricerca scientifica nei campi della Intelligenza Artificiale e della Computer Vision che consentono ad un calcolatore di analizzare un flusso video allo scopo di comprenderne il contenuto e di annotarlo automaticamente (i metadati) senza l'intervento umano. I sistemi di analisi video possono richiamare l'attenzione dell'operatore quando avviene qualche evento specifico nella scena inquadrata dalla telecamera o consentono di ridurre di diversi ordini di grandezza i tempi della ricerca consentendo all'operatore di trovare solo quelle sequenze video che soddisfano alcuni criteri specificati dall'operatore.

I metadati nella piattaforma di analisi audio e video di A.I. Tech

In questo articolo cercheremo di dare una risposta alle seguenti domande: quali sono i tipi di metadati estratti automaticamente dalla piattaforma di analisi audio e video di A.I. Tech? Come sono rappresentati ed inviati ai sistemi deputati alla fruizione (Video Management Systems, piattaforme di business intelligence)?

La piattaforma di A.I. Tech incorpora un motore di analisi video basato su algoritmi avanzati di object detection e tracking e di filtraggio del rumore che consente di rilevare con accuratezza diverse tipologie di eventi (conteggio persone, heat-map, superamento di linea, rilevamento di intrusioni, riconoscimento di comportamento sospetti, segnalazione di oggetti rimossi/incustoditi, rilevamento di fumo e fiamme) anche in condizioni ambientali complesse sia indoor che outdoor.

A.I. Tech (www.aitech.vision) è una società fondata nel 2010 che produce soluzioni avanzate di analisi audio e video per i mercati verticali del retail e della sicurezza. A.I. Tech è stata fondata da ricercatori universitari attivi da oltre 25 anni nella realizzazione di sistemi intelligenti basati sulla elaborazione di segnali audio e video.

La piattaforma di analisi è disponibile sia come applicazione lato server (si veda Fig. 1 per uno screenshot della piattaforma di analisi integrata con Milestone XProtect), o come una applicazione in modalità “edge” in grado di poter essere eseguita a bordo di telecamere Axis, Hikvision e Samsung che supportano l’elaborazione embedded. La piattaforma di A.I. Tech è ingegnerizzata in modo da consumare poche risorse di calcolo, consentendo di elaborare un elevato numero di flussi video contemporaneamente su server di fascia alta, o di elaborare a pieno frame rate un singolo flusso video a bordo della telecamera. Inoltre, è anche disponibile per dispositivi di calcolo a basse prestazioni e basso consumo energetico (quali Raspberry Pi o altre piattaforme embedded basate su Linux) consentendo di portare alla periferia (“to the edge”) l’elaborazione anche laddove non siano disponibili telecamere che supportano l’esecuzione embedded.

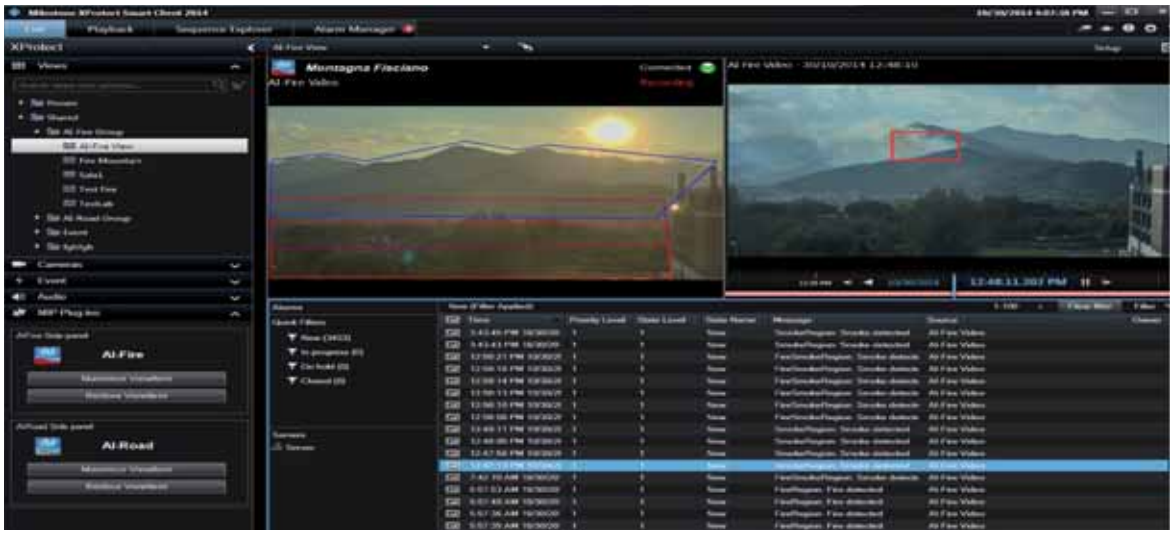


Fig. 1· Funzioni di analisi video per il rilevamento fumo e fiamme integrate in Milestone XProtect

Inoltre, l’offerta di A.I. Tech si arricchisce con la disponibilità di prodotti per l’analisi audio che consentono la rilevazione ed il riconoscimento di eventi audio (quali urla, rottura di vetri, esplosioni) sia in ambienti affollati che sterili, fornendo così metadati aggiuntivi a quelli già forniti dalla analisi video (si veda la Fig. 2 per la schermata principale della applicazione di analisi audio di A.I. Tech).

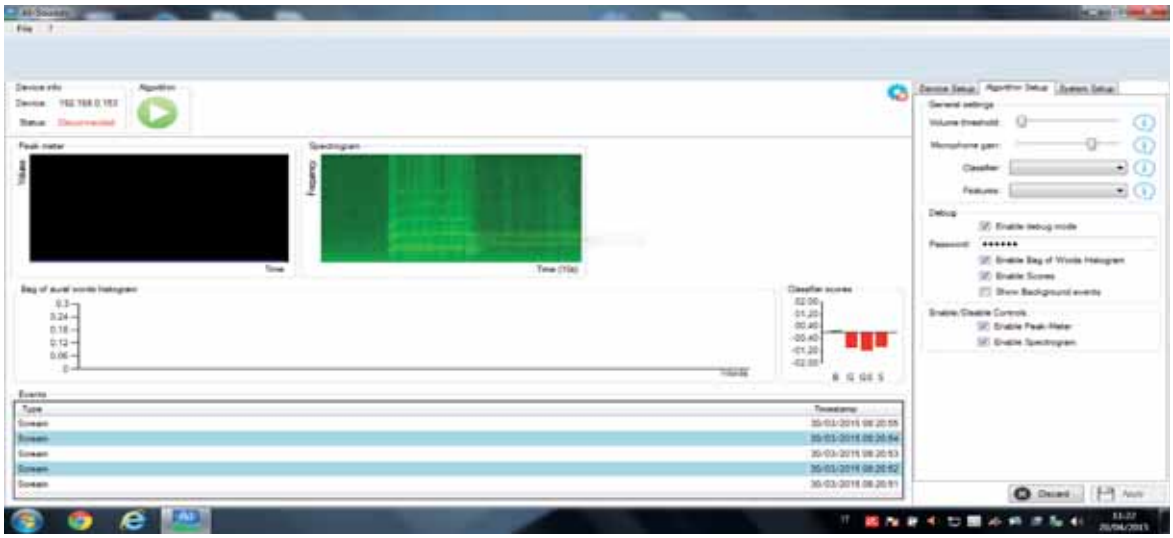


Fig 2 · Schermata principale della applicazione di analisi audio di A.I. Tech

L'informazione fornita attraverso i metadati dipende dalla specifica funzione di analisi: in generale, essa include l'evento individuato dall'applicazione, con il riferimento temporale utile per associarli alla porzione rilevante del flusso video, insieme con informazioni riguardanti gli oggetti o le entità coinvolti. Ad esempio, il bounding box degli oggetti (si veda in Fig. 3 per alcuni esempi), l'età stimata, il sesso e la razza della persona per eventi legati alla individuazione di volti.

Fig. 3 · Esempi di bounding box di oggetti rilevati mediante la piattaforma di analisi video di A.I. Tech.

Inoltre, ove appropriato, il sistema è in grado di fornire un'indicazione quantitativa del grado di confidenza della rilevazione, in modo da consentire all'applicazione che usa i metadati di filtrare ed elaborare e/o riportare all'utente solo quelli che siano ritenuti sufficientemente affidabili.
Nella Tabella 1 sono riassunti i metadati forniti dalla piattaforma di A.I. Tech per ogni specifico tipo di funzione di analisi audio/video.

METADATI	**TIPO DI EVENTO**
Timestamp	Tutti gli eventi audio/video
Bounding box dell'oggetto	Superamento linea Intrusione Oggetto abbandonato/rimosso Comportamento sospetto Fumo Fiamme Analisi volto
Traiettoria dell'oggetto	Intrusione Comportamento sospetto
Colore medio dell'oggetto Classe dell'oggetto (persona, veicolo, altro) Dimensioni dell'oggetto (altezza, larghezza) in cm Distanza dell'oggetto dalla telecamera Velocità dell'oggetto	Superamento linea Intrusione Oggetto abbandonato/rimosso Comportamento sospetto
Direzione dell'attraversamento linea	Superamento linea
Ingresso/uscita dall'area virtuale	Intrusione
Sesso (maschio/femmina) + confidenza Età (bambino, adolescente, adulto, anziano) + confidenza Razza (Bianco, Nero, Asiatico) + confidenza	Analisi volto
Classe audio (sparo, urlo, rottura vetro, altro) + confidenza	Analisi audio

Tab. 1· Lista dei metadati correntemente supportati dalla piattaforma di analisi audio e video di A.I. Tech.

Sistema di notifica dei metadati nella piattaforma di A.I. Tech

L'architettura del sistema di notifica dei metadati della piattaforma di analisi di A.I. Tech è realizzata sfruttando un approccio modulare basato su plug-in, come rappresentato nella Fig. 4.

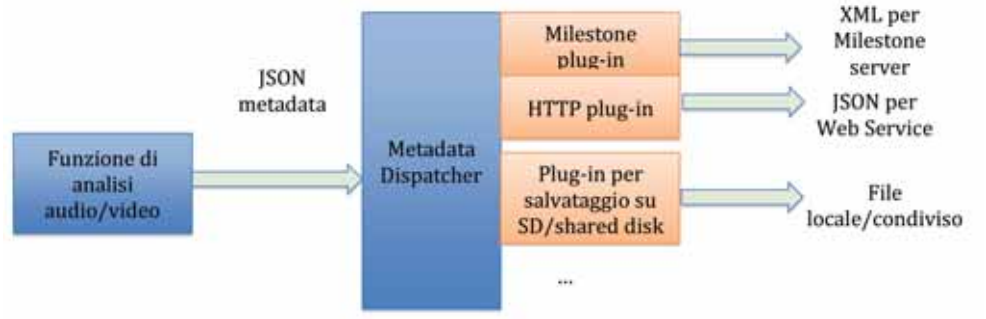


Fig. 4 · Architettura del sistema di notifica dei metadati nella piattaforma di A.I. Tech.

Tale architettura è stata progettata con lo scopo di garantire i seguenti vantaggi:

- Semplicità d'integrazione con Milestone XProtect, con supporto per il formato di eventi e metadati di Milestone.
- Semplicità d'integrazione con qualsiasi altra applicazione basata sul paradigma dei web service, mediante RESTful web services di semplice realizzazione.
- Possibilità di sviluppare in futuro altri plug-in per supportare altre piattaforme (ad esempio per business intelligence).
- Possibilità di immagazzinare i metadati localmente per uso off-line.
- Alta configurabilità, grazie alla possibilità di stabilire al momento della configurazione quali plug-in devono essere abilitati e quindi verso quali sistemi deve essere indirizzato il flusso di metadati.

La funzione di analisi audio/video della piattaforma di A.I. Tech genera i metadati in un formato interno basato sullo standard JSON (JavaScript Object Notation, standard ECMA-404), leggero e flessibile, in grado di rappresentare anche strutture dati complesse. JSON è solitamente utilizzato in applicazioni web e per RESTful web services, in quanto è più compatto e semplice da analizzare rispetto all'XML. Il formato JSON è anche popolare nei database NOSQL; ad esempio il database document-oriented MongoDB, usato spesso nel contesto della gestione di Big Data, salva i dati in formato JSON.

I metadati generati sono poi passati al Metadata Dispatcher, il componente della piattaforma di A.I. Tech, che si occupa della bufferizzazione dei metadati e del loro inoltro ad un insieme di plug-in, ognuno dei quali può essere attivato e configurato tramite l'applicazione di configurazione di A.I. Tech. I plug-in sono responsabili per l'adattamento dei metadati a diversi formati ove richiesto e per il loro inoltro ad applicazioni remote di fruizione. Ad esempio, il plug-in Milestone converte il formato JSON in XML, usando lo schema XML definito da Milestone per la sua linea di prodotti XProtect, ed invia le informazioni al Milestone XProtect Event Server in modo tale che l'informazione sia poi utilizzabile per operazioni di ricerca e filtraggio degli eventi.

Il plug-in HTTP invia i dati in formato JSON mediante una richiesta HTTP POST ad un indirizzo specificato in fase di configurazione; questo può essere semplicemente associato ad un web service basato sul paradigma REST allo scopo di consentirne la fruizione attraverso una applicazione utente. Questa rappresenta una soluzione molto conveniente per inviare i metadati ad applicazioni di terze parti basate su service oriented architecture(SOA).

Il plug-in di salvataggio aggiunge i metadati ad un file che può risiedere su un dispositivo di salvataggio locale (ad esempio una scheda SD nel caso in cui l'applicazione risieda sulla telecamera) or su un dispositivo di storage condiviso (ad esempio un server o un NAS). La prima opzione è estremamente utile quando la telecamera potrebbe non essere sempre collegata alla rete, rendendo possibile la raccolta differita dei metadati per un uso off-line. La seconda opzione può essere applicata quando non è possibile, o desiderabile, avere l'applicazione che deve consumare i metadati che gira su un server; in questo caso l'applicazione può verificare periodicamente i file da leggere e processare i metadati.

milestone

The Open Platform Company

Il meraviglioso mondo dei Metadata secondo Bosch Security Systems

Contributo di Jan Noten, System Integration Architect e Stefano Riboli, Marketing Video Systems Bosch Security Systems

Introduzione

In una soluzione di videosorveglianza convenzionale, gran parte delle riprese video provenienti dalla telecamere di sicurezza sono trasmesse centralmente ad una sala controllo per una supervisione centrale del sistema o dei sistemi connessi.
Questo significa che le immagini in tempo reale provenienti dalle telecamere sono guardate da uno o più operatori, mentre la gran parte delle telecamere è registrata in simultanea. Il numero di telecamere che l'operatore può visionare è spesso limitato dall'hardware del sistema e dalla capacità dell'operatore di poter visionare su più monitor in simultanea le telecamere, mantenendo un livello di attenzione ai dettagli per un elevato periodo di tempo. Gli eventi come allarmi, guasti e sabotaggi come l'oscuramento ed il riposizionamento delle telecamere sono presi in carico dall'operatore.
Le moderne funzioni di intelligenza come l'Intelligent Video Analysis (IVA), presenti nelle telecamere ed encoder di Bosch, riducono il carico e lo stress agli operatori permettendogli, tramite una valutazione a priori basata su algoritmi e regole di allarme nella telecamera, di poter analizzare solo gli eventi salienti del sito.
L'Intelligent Video Analysis può aumentare in maniera significativa il numero delle telecamere in gestione all'operatore, riducendone il carico e aumentando il livello di attenzione sull'evento, rendendo disponibile la telecamera di interesse al software di management e, quindi, all'operatore.
Immaginando un'applicazione con ben 500 telecamere, come potrebbe un gruppo di operatori tener sotto controllo tutte le informazioni?
La soluzione c'è: l'Intelligent Video Analysis (IVA) e l'elaborazione dei Metadata!

Cos'è Metadata?

Metadata è un flusso di informazioni (data) nel tempo sincronizzato, che rappresenta il contenuto del flusso video (video stream) in ogni momento. I Metadata possono tuttavia essere trasmessi in modo indipendente dal flusso video compresso ed essere collegati al video tramite RTP timestamps. I principali obiettivi del formato Metadata Bosch sono la semplicità, l'efficienza dell'occupazione di banda, la scalabilità e l'espandibilità. Il formato Bosch del Metadata è descritto in un documento chiamato VCD (Video Context Description).
Per esempio, le informazioni contenute nel Matadata possono essere:

- Informazioni relative all'Intelligent Video Analysis (IVA) come: nuovi oggetti, la posizione degli oggetti, il movimento dei pixel, gli allarmi e molto altro ancora
- Opzionali:
  - la posizione del motore di Pan, Tilt o Zoom della telecamera
  - testo inviato sulla porta seriale della telecamera, come POS (Point of Sales) o ATM (Automated Teller Machine) associati al testo video

I Metadata di Bosch Security Systems possono essere resi disponibili nel flusso video in diretta (Live) ed in riproduzione (Playback). I video registrati, che includono i Metadata, forniscono una grandiosa modalità per richiamare lo storico e le informazioni di qualsiasi momento. Riprodurre il video sui Metadata permette di simulare e lavorare il video esattamente come un video reale sospeso nel tempo. Dietro al video, il flusso Metadata contiene tutta l'intelligenza della singola immagine video, la quale è usata come motore di ricerca intelligente. In questo modo, attraverso una ricerca adeguata del contenuto del Metadata, l'operatore può indirizzare direttamente quanto accaduto durante l'evento. Questo processo produce non solamente un video dettagliato ed accurato, ma permette anche di agire in tempi estremamente rapidi. Il processo di ricerca del Metadata è inteso come ricerca forense. Al fine di permettere alla telecamera di produrre il flusso Metadata per la sessione video in diretta ed in riproduzione, lo stream deve essere invocato. Una volta che il flusso Metadata è attivo, cioè abilitato nella telecamera, il contenuto sarà automaticamente registrato nei dispositivi BVIP (Bosch Video IP) come, per esempio, nella memoria della telecamera "Edge Recording", cioè come nelle memorie SD e CF o tramite una registrazione iSCSI generata direttamente dalla telecamera o, in ultimo, mediante Video Recording Manager (VRM).

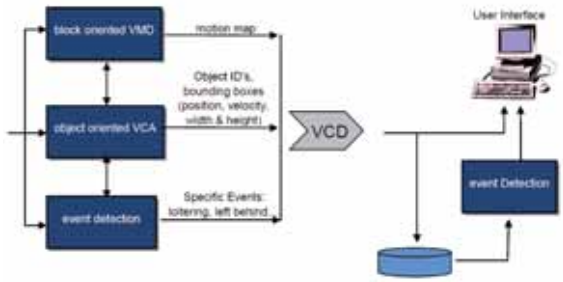


Fig. 1 · Rappresenta il flusso Metadata (VCD) generato dalla telecamera per il Live ed il Playback

Come invocare un flusso Metadata dalla telecamere Bosch (dettaglio tecnico)

Il flusso Metadata della telecamera Bosch può essere inizializzato in varie modalità come:

1. Real Time Streaming Protocol (RTSP)
2. ONVIF
3. Remote Control Protocol Plus (RCP+)

1. Ricevere il Metadata via RTSP:

Ogni telecamera Bosch è in grado di riconoscere le richieste provenienti da un flusso RTSP, tuttavia il protocollo RTSP è ricco di alcune caratteristiche opzionali, quali la semplice richiesta diretta alla telecamera del flusso Metadata: **RTSP://<ip camera>/?vcd=1**

Il flusso che sarà ricevuto conterrà semplicemente tutti gli elementi descritti nel documento Bosch Metadata e, tramite un semplice parser, cioè un'**analisi sintattica,** che analizza il flusso continuo di dati in ingresso in modo da determinarne la struttura, sarà possibile restituire i dati grezzi (RAW) intelligenti all'applicazione software.

2. Ricevere il Metadata via ONVIF:

Il flusso Metadata via ONVIF è una recente novità delle telecamere Bosch con firmware 6.10 o superiore, cioè su tutti gli hardware con Common Product Platform (CPP) di quarta e di sesta generazione (CPP4 e CPP6). La CPP Bosch permette l'impiego di un unico firmware su tutte le telecamere IP. Per maggiori informazioni http://downloadstore.boschsecurity.com/

Aggiornando le telecamere Bosch all'ultimo firmware, è possibile ricevere il Metadata in formato ONVIF. Il Metadata ONVIF contiene le coordinate del Bounding Boxes dell'oggetto, cioè il quadrilatero che delimita del suo baricentro e l'Object ID, cioè la chiara identificazione dello stesso rispetto ad altri oggetti nella scena.

Nota: il Metadata ONVIF (MetadataConfig1) deve essere aggiunto manualmente al profilo ONVIF della telecamera.

Quante aziende italiane conosci che da oltre 80 anni portano innovazione e tecnologia in tutto il mondo?

Sofitel Bali Nusa Dua Beach Resort
Bali - 2014

Impianto di videosorveglianza con oltre 200 telecamere ad alta definizione, focale fissa, variabile e speed dome.

Fracarro è un'azienda italiana che opera in tutto il mondo da prima che tu nascessi. Ha portato la TV nella casa dei tuoi nonni e negli anni '80 ha scelto di mettere a frutto le sue competenze tecnologiche anche nel settore Sicurezza. Così anche oggi puoi contare su soluzioni per la protezione antintrusione e videosorveglianza sempre all'avanguardia.

Impianto filare o wireless? Da oggi Defender Hybrid.

La nuova centrale Defender Hybrid rivoluziona il modo di progettare i sistemi antintrusione perché consente la totale libertà nella scelta di utilizzare, nello stesso impianto, dispositivi filari e wireless, rendendo semplice anche la protezione di zone difficilmente raggiungibili con la tradizionale cablatura.

- 40 zone wireless e 8 filari
- 16 telecomandi e 4 sirene wireless
- Espansioni opzionali su BUS fino a 64 zone wireless o filari
- Combinatori telefonici PSTN e GSM con sintesi vocale integrata
- Completamente gestibile da web

YouTube fracarro.com

FRACARRO
shaping the future

Esempio ONVIF per la richiesta delle coordinate dell'oggetto all'interno della scena:
Inoltre i messaggi di evento sono anche parte del Metadata. Il formato ONVIF del messaggio dell'evento contiene informazioni basate sulle regole del motore IVA della telecamera.

Fig. 2: rappresenta il contenuto del Metadata Stream ONVIF

Informazioni aggiuntive relative alle regole IVA:
Le telecamere IVA Bosch supportano anche 8 regole di IVA. La configurazione delle regole deve avvenire attraverso la pagina web del dispositivo e mediante apposito tool software. Le tipologie di rilevazioni IVA che possono essere trovate all'interno del Metadata sono elencate di seguito.

Elenco degli eventi IVA nel Metadata:
a) Oggetto nel campo
b) Superamento linea
c) Bighellonare
d) Cambio di condizione
e) Percorso
f) Oggetto rimosso
g) Oggetto abbandonato
h) Ingresso nel campo
i) Uscita dal campo
j) Similarità
k) Affollamento
l) Contatore

Un messaggio di evento ONVIF contiene la **sorgente video,** il **tipo di evento** ed il **nome regola IVA**.
Tutti gli eventi sono parte della richiesta ONVIF "***GetEventProperties",*** e supportano la creazione dinamica delle regole IVA. Nel caso in cui una regola IVA è creata lato telecamera, il client software ONVIF deve invocare nuovamente la richiesta "***GetEventProperties".*** Per esempio, se la telecamera attiva differenti configurazioni di analisi video su fascia oraria, grazie ad una programmazione interna, è sufficiente inviare nuovamente la richiesta ONVIF. I cambiamenti creati nelle regole come, per esempio, aver spostato le linee virtuali di attraversamento non richiedono alcun aggiornamento del "***GetEventProperties".***
Nota: per essere retro compatibili tutti gli eventi IVA sono trasmessi come eventi di "**Motion Alarm".** Esistono alcuni tool freeware in commercio che permettono di ottenere un test tool software ONVIF.

3. Ricevere il Metadata via RCP+:
Bosch offer ai partner del programma IPP (Integration Partner Program) il documento riguardante il protocollo **Remote Control Protocol Plus** (RCP+). Il documento descrive i comandi nativi della struttura per comunicare con un dispositivo Bosch BVIP. Per ricevere il flusso Metadata nell'applicazione software non Bosch può essere usato il comando RCP "CONNECT_PRIMITIVE". Questo comando facilita le varie opzioni di connessione. Per iniziare la connessione con il flusso Metadata, devono essere impostati di conseguenza i 2 byte per "Coding" nella parte di payload del MediaDescriptor (bit5=1).
Conclusione: Fornire l'accesso al flusso Metadata è un grande beneficio per coloro che si occupano della realizzazione di applicazioni software per ambienti che richiedono specifiche di funzionamento non standard come, per esempio, riconoscere un colore, una direzione, una dimensione, una velocità ed una proporzione dell'oggetto in movimento senza la necessità di sviluppare ed utilizzare enormi risorse hardware. Il Metadata contiene l'intelligenza del flusso video fornito dalla telecamera, "Intelligence at the edge". Il vantaggio del Metadata è che permette di essere veloci e accurati, garantendo un accesso intelligente ai contenuti video in grandi sistemi; infine, riduce il carico sugli operatori della sala controllo attraverso l'applicazioni dei corretti filtri sugli eventi e sulla ricerca. Per esempio, immaginate di dover usare qualsiasi criterio di ricerca in relazione ad una persona o ad un oggetto senza averlo predeterminato. Tramite una ricerca forense nel flusso Metadata, sareste in grado di cercare un veicolo di colore rosso che ha percorso un determinato tratto stradale, il tutto in pochi secondi di ricerca all'interno del file di testo relativo al Metadata.

Dorma + Kaba, nasce un leader nella sicurezza e nel controllo accessi

a cura della Redazione

Kaba Holding AG (SIX: KABN), con headquarter a Rümlang (Svizzera), ed il Gruppo Dorma Holding GmbH + Co. KGaA, con sede a Ennepetal (Germania), annunciamo la creazione del gruppo dorma+kaba group. L'accordo transattivo è stato firmato il giorno 30 aprile 2015.

- dorma+kaba diventeranno una delle prime 3 aziende leader internazionali nel mercato delle soluzioni di sicurezza e di controllo accessi, con vendite pro-forma superiori a 2 miliardi di CHF (1,9 miliardi di euro)
- leader di prodotti e servizi offerti da un'unica fonte grazie a un portafogli di prodotti complementari, value chain potenziata e una presenza geografica in tutti i mercati chiave
- opportunità di crescita eccellenti e una notevole potenziale sinergia per creare un maggiore valore aggiunto per gli azionisti Kaba; previsto dividendo straordinario di CHF 50 per azione
- Il gruppo Dorma aumenta il proprio impegno imprenditoriale con l'acquisizione del 9,1% del capitale di Kaba
- Kaba deterrà il 52,5% delle azioni della nuova dorma+kaba Holding mentre il Gruppo Dorma manterrà il 47,5% del business Dorma e Kaba combinato
- L' Assemblea Straordinaria per l'approvazione della fusione è avvenuta in data 22 maggio 2015; il completamento della transazione è previsto per il terzo trimestre 2015

Dorma è un fornitore di soluzioni per l'accesso e servizi correlati, è leader mondiale nel settore dei chiudiporta, porte automatiche e accessori per vetro. Kaba è un leader globale per il controllo accessi, la raccolta di dati di impresa e sistemi di chiusura. Ulrich Graf, presidente di Kaba dichiara: "La combinazione di due marchi forti quali Dorma e Kaba porterà alla creazione di una società leader nel nostro settore. Gli azionisti di riferimento assicureranno un orientamento a lungo termine, che rappresenta un altro vero vantaggio competitivo nel nostro dinamico settore ". Con un fatturato pro-forma di oltre 2 miliardi di franchi, circa 16.000 dipendenti e sedi in 53 paesi, il gruppo dorma+kaba diventerà una delle tre maggiori company internazionali nel mercato altamente frammentato delle soluzioni di sicurezza e di controllo accessi. Dr. Hans Gummert, presidente di Dorma dichiara: "Con la fusione delle nostre due società, rafforzeremo in maniera significativa la nostra posi-

zione sul mercato. Non solo condividiamo più di cento anni di tradizione imprenditoriale e gli stessi valori, ma anche in gran parte le nostre strategie".

Kaba e Dorma – un'unione eccellente

La competenza tecnologica di Kaba e Dorma, i prodotti ed i canali di distribuzione si completano a vicenda in maniera eccellente. La reti di servizi di distribuzione condivisa, il cross selling e il posizionamento come un one-stop-shop per le soluzioni di sicurezza e di accesso aprono un significativo potenziale di crescita aggiuntivo per la nuova holding. "Insieme a Kaba , stiamo facendo un grande passo in avanti " dichiara Thomas P. Wagner , CEO di Dorma, "Noi amplieremo la nostra offerta, rafforzeremo la nostra presenza internazionale e aumenteremo la nostra capacità di innovazione. Questo ci permetterà di cogliere meglio e più rapidamente un vantaggio dalle opportunità che si presentano attraverso megatrend quali l'urbanizzazione e la digitalizzazione". dorma+kaba avrà stabilimenti produttivi in tutti i mercati chiave del settore e accelererà l'espansione globale attraverso la sua presenza rafforzata in particolare in Europa, America e Asia-Pacifico.

Sostanziale valorizzazione attraverso un notevole potenziale di crescita e sinergie

Su base pro-forma, il nuovo gruppo ha generato un fatturato di 2.242 milioni CHF per l'esercizio 2013/2014 (ex 30 giugno 2014) e un EBITDA pari a CHF 303 milioni. Il margine EBITDA pro-forma è stato del 13,5 %. Riet Cadonau, CEO di Kaba dichiara : " Dorma e Kaba sono partner ideali a tutti gli effetti. Il progetto di fusione creerà ulteriori opportunità per una crescita sostenibile e redditizia fornendo così un valore aggiunto per i nostri clienti, partner, dipendenti e azionisti".

Key figures per l'anno finanziario 2013/2014 (al 30 giugno 2014)

	Kaba[1] In CHF million	Dorma[1] In EUR million	**dorma+kaba pro-forma[1] In CHF million[2]**
Sales	1,003.5	1,010.3	**2,241.7**
Gross profit	446.8	436.2	**981.4**
Gross margin	44.5%	43.2%	**43.8%**
EBITDA	155.3	120.2	**302.6**
EBITDA margin	15.5%	11.9%	**13.5%**
EBIT	123.6	89.3	**233.0**
EBIT margin	12.3%	8.8%	**10.4%**
Net profit	84.6	71.6	**172.4** [3]
Equity ratio	62.8%	52.1%	**57.2%**

1) Reference figures based on IFRS
2) Average CHF/EUR exchange rate for the 2013/2014 financial year: 1.225608
3) Whereof 52.5% attributable to dorma+kaba Holding shareholders

Con i suoi prodotti, soluzioni e servizi innovativi, il gruppo internazionale Kaba è un fornitore leader di soluzioni di alta qualità per il controllo degli accessi, chiavi, cilindri di sicurezza, sistemi di controllo accessi fisici, di raccolta dati e rilevazione presenze, e sistemi di accesso per hotel. Il gruppo è anche un leader globale di mercato per i sistemi di chiusura di alta sicurezza, chiavi grezze, chiavi transponder e per le macchine di produzione chiavi. Il gruppo quotato in borsa ha un fatturato di circa un miliardo di franchi e impiega circa 9.000 persone in oltre 60 paesi. Per più di 150 anni, Kaba ha dettato le tendenze nel mercato della sicurezza in termini di funzionalità, praticità e design, mantenendo il focus sulle esigenze dei clienti. **Per maggiori dettagli consultate il sito www.kaba.com**

Dorma è il partner di fiducia e servizi di alto livello, che Con oltre 100 anni di tradizione alle spalle, Dorma, azienda di proprietà familiare, si è sviluppata come leader del mercato mondiale negli strumenti di controllo delle porte, sistemi ed accessori per vetro. Anche nel settore delle automazioni, l'azienda fa parte dell'élite mondiale. Dorma è inoltre fornitore di sistemi di porte scorrevoli. Il Gruppo con sede a Ennepetal, Germania, è presente in più di 50 Paesi ed impiega circa 7200 persone in tutto il mondo. **Per maggiori informazioni visitate il sito www.dorma.com**

ekey biometric systems, le soluzioni biometriche per la casa intelligente

a cura della Redazione

ekey biometric systems, società austriaca con sedi anche in Italia, Germania e attiva in tutto il mondo, collega in rete le sue soluzioni biometriche per l'accesso, le prepara per la "casa intelligente" e le rende amministrabili tramite un'app. Nel 2004, quando ekey commercializzava il suo primo sensore fingerprint, la biometria era ancora una parola largamente sconosciuta. Da quando anche gli smartphone sono stati muniti di sistemi per la scansione biometrica, il profilo della biometria e in particolare dell'impronta digitale in termini di visibilità da parte del grande pubblico è molto cambiato. La biometria sta acquistando un certo peso nella sicurezza e, in particolare, nel controllo accessi perché offre alcuni indiscutibili vantaggi:

- **Sicurezza**: i sistemi biometrici sono progettati per proteggere le strutture da accessi non autorizzati e utenti illegittimi in modo solitamente più efficace e affidabile rispetto ai sistemi tradizionali.
- **Integrazione**: le tecnologie biometriche possono essere facilmente integrate in altri sistemi di allarme e videosorveglianza attraverso i network IP.
- **Accuratezza**: soprattutto negli anni più recenti, l'impiego di sistemi biometrici sta rendendo il processo di identificazione molto più sicuro e accurato.

- **Comodità**: La chiave è sempre a portata di mano.
- **Semplicità**: il problema delle password o delle chiavi che possono essere copiate, dimenticate o smarrite, viene eliminato.
- **Convenienza:** l'impiego delle tecnologie biometriche permette di ridurre i costi.
- **Stabilità**: i dati biometrici di una persona, salvo casi eccezionali, rimangono invariati nel tempo. E non possono essere smarriti.

Produttore leader nel suo campo

ekey è uno dei precursori internazionali per quanto riguarda i sistemi biometrici per il controllo degli accessi, e un vero e proprio "Campione Nascosto" focalizzato su obiettivi ambiziosi, in particolare sulla leadership di mercato. Il gruppo con sede centrale in Austria si è specializzato nella scansione dell'impronta digitale e produce sistemi per l'accesso ad impronta digitale per porte, aree d'ingresso e impianti d'allarme, persino degli scanner che permettono di autorizzare i pagamenti online. ekey opera in 3 ambiti principali: la ricerca di base, lo sviluppo di soluzioni OEM e la produzione di una gamma standard di sistemi biometrici per il controllo degli accessi.

Nel campo delle vendite, le attività si concentrano su due priorità, i produttori di porte e il settore elettrico. In merito al settore elettrico, ekey coopera con produttori di impianti d'allarme e citofonici. Non esiste alcun marchio che non è adatto all'integrazione del lettore ekey. La maggiore crescita ci si aspetta dalla cooperazione con i costruttori di porte. ekey non solo coopera con tutti i costruttori di porte austriaci, ma collabora con i principali produttori in Germania, Italia, Slovenia e Repubblica Ceca.

1,5 milioni di porte all'anno

Le potenzialità sono grandi. Considerando solo Germania e Italia, la produzione annua di porte si aggira intorno ai 1,5 milioni in ognuno dei due Paesi. Più della metà sono porte in legno o alluminio, adatte per l'integrazione di un lettore d'impronte. In Italia, le porte d'ingresso si suddividono in ca. 400.000 porte per nuovi edifici e ca. 250.000 porte in edifici esistenti. Inoltre, il lettore impronte è adatto per porte blindate, portoni per il garage, cancelli, porte per l'industria. Il lettore ekey arte (nella foto) è stato creato per essere integrato nelle maniglie.

Accanto ai sistemi ekey home e ekey multi è disponibile la più ampia variante ekey net. Qui si tratta di una soluzione che viene adottata principalmente da imprese o associazioni. In Austria, la Croce Rossa utilizza i sistemi ekey, inoltre anche in Italia numerose brigate di Vigili del Fuoco hanno optato per le soluzioni ekey, grazie alle quali la gestione diventa molto più facile. ekey conta tra i suoi clienti molti rinomati enti e aziende p.es. l'ente europeo Eumetsat, l'aeroporto di Trento, grandi imprese tedesche o svizzere anche in settori di sicurezza (assicurazioni, centri informatici, società farmaceutiche).

NFC non ci fa concorrenza

Attualmente NFC non viene considerata una tecnologia concorrente. Una serratura NFC richiede sempre di avere con se il proprio smartphone. Inoltre la batteria non deve mai essere scarica. Ma ci portiamo a presso sempre lo smartphone? Il proprio dito sicuramente si.

C´è un'altra considerazione da fare: con le porte NFC sarebbe necessario che anche i bambini venissero muniti di uno smartphone. Questo ha poco senso. Ciò che invece è più sensato è di integrare nel lettore d'impronte un lettore di schede, per permettere anche a portatori di handicap oppure persone sofferenti di malattie alle dita (gotta) di aprire

porte. Di conseguenza è disponibile una soluzione ekey munita di un lettore di schede integrato.

Collaborazioni con università

L'azienda investe in media il 17 percento del fatturato annuo nella ricerca e nello sviluppo di nuovi prodotti. Il totale degli investimenti in R&S negli anni 2002-2014 ammonta a circa 10 milioni di euro. In questo campo ekey collabora con l'Università di Linz e l'Istituto tecnico superiore di Hagenberg.

Il futuro

Il futuro è quello di collegare il fingerprint con la casa intelligente. L'impronta digitale è perfettamente adatta per identificare gli abitanti in una casa intelligente. La casa sa chi entra, e in base a questa informazione vengono attivate oppure bloccate certi eventi. In tal modo, si può non solo programmare p.es. l'impianto musicale o creare un'atmosfera dove sentirsi a proprio agio, ma è possibile bloccare la TV per i bambini oppure il forno per persone affette da demenza. ekey è compatibile con tutti i sistemi.

La biometria nel mondo delle app

ekey è presente anche nel mondo delle app. Grazie all'app per ekey home (Android e iOS), i sistemi ad impronta digitale possono essere amministrati anche con lo smartphone. Tramite l'app è possibile ad es. registrare nel sistema nuove impronte oppure cancellarle in caso di bisogno.

La filiale italiana dell'azienda è disponibile per ogni tipo di informazioni all'indirizzo: italia@ekey.net.

Centrali Serie Quaranta, l'eccellenza nella protezione antintrusione

a cura della Redazione

Le centrali Serie Quaranta sono la punta di diamante della proposta HESA riservata ai professionisti della sicurezza che aderiscono alla rete dei Concessionari e degli Installatori Autorizzati. Sviluppate con le più avanzate tecnologie oggi disponibili a livello mondiale, rappresentano infatti lo stato dell'arte e l'eccellenza nella protezione antintrusione e sono state progettate in esclusiva per HESA con l'obiettivo di rispondere con la massima affidabilità e flessibilità alle particolari esigenze di sicurezza del mercato italiano.

Dotate di 5 zone e 5 aree espandibili fino a 100 zone e 15 aree con un innovativo modulo a 5 ingressi/uscite - grazie al quale ogni terminale può essere programmato liberamente come ingresso zona o uscita logica programmabile - le centrali Serie Quaranta sono abbinate a una linea completa di tastiere, rivelatori e contatti dal design moderno ed elegante e sono progettate in maniera da rendere l'installazione, l'espansione e la gestione del sistema semplici e veloci.

Tra le varie tastiere della Serie Quaranta - di tipo touchscreen, LCD e a sfioramento – si distinguono

per l'eleganza del design le tastiere touchscreen Q-TOUCH, dotate di ampi schermi ad alta risoluzione da 4,3 e 7 pollici e utilizzabili anche come eleganti cornici digitali. Grazie all'interfaccia chiara, al microfono e all'altoparlante integrati che guidano l'utente nelle fasi di inserimento e disinserimento del sistema, queste tastiere offrono la massima semplicità per la gestione del sistema. L'interfaccia grafica semplice e intuitiva delle tastiere Q-TOUCH è la stessa utilizzata anche nell'applicazione per sistemi iOS e Android sviluppata per la Serie Quaranta. Scaricabile da Apple Store e da Google Play, permette di rispondere alle più svariate esigenze di comfort e di sicurezza, consentendo agli utenti di controllare e gestire da remoto il proprio sistema di sicurezza e vari dispositivi di automazione domestica, comodamente tramite smartphone e tablet.

Per comunicare ogni tipo di allarme, la Serie Quaranta dispone di moduli vocali e di comunicazione GSM e GSM-GPRS che offrono elevate prestazioni. Tra essi, il modulo Q-GSM su linea seriale può essere installato anche distante dalla centrale e permette di inviare SMS fino a 15 numeri telefonici e di gestire la centrale tramite SMS. In caso di mancanza di comunicazione con la centrale, è in grado di funzionare in modo autonomo.

Tra i vari componenti del sistema si distinguono un software intuitivo e dal design moderno per la programmazione locale e remota, e il lettore di prossimità a incasso Q-PROX-I che, grazie alla particolare forma, è compatibile con qualsiasi serie di frutti elettrici. I contatti magnetici della Serie Quaranta sono dotati di due terminali singolarmente programmabili come ingresso o uscita, dove gli ingressi gestiscono direttamente i rivelatori tapparella e vibrazione. Si ricorda, inoltre, che tutta la parte senza fili 868MHz è completamente bidirezionale. HESA ha reso disponibili, in abbinamento alle centrali Serie Quaranta, diversi sensori scelti tra i migliori oggi presenti sul mercato già assemblati con i trasmettitori.

A garanzia della massima qualità e affidabilità, i componenti della Serie Quaranta sono conformi alle normative CEI 79-2, EN50131-3 ed EN131-6.

In occasione del Meeting dei Concessionari e Installatori Autorizzati HESA 2015 che si è svolto all'Isola d'Elba il 14 e 15 maggio scorsi, HESA ha presentato in anteprima alla rete dei propri partner un'importante vetrina di novità che si inseriranno in questa gamma di sistemi.

Una di queste è la sirena Serie Stile collegata su bus della centrale Quaranta. Questa sirena riunisce in sé tecnologia all'avanguardia, prestazioni avanzate e un design moderno declinato in una vasta gamma di tonalità. La sirena Stile si adatta armoniosamente ad ogni ambiente, assicurando la massima affidabilità anche nelle condizioni ambientali più critiche e rap-

presenta il completamento ideale di ogni sistema di sicurezza. La nuova versione progettata per la centrale Serie Quaranta è dotata inoltre di due led aggiuntivi di segnalazione dello stato della centrale.
Altra novità della centrale Serie Quaranta è la scheda di uscita di rete Q-ESP/DAC , che permette di controllare i carichi elettrici domestici e utenze quali luci e prese. Per queste utenze consente la regolazione dell'intensità, offrendo la possibilità di gestire scenari domotici dove spesso l'intensità dell'illuminazione è determinante. La scheda permette anche il controllo dello sfasamento tra corrente e tensione di ogni singola uscita, così da controllare eventuali inefficienze del sistema elettrico. La gestione simultanea di più uscite di Q-ESP/DAC può inoltre consentire la regolazione del colore dell'illuminazione.
Alla famiglia Serie Quaranta si aggiunge inoltre il nuovo rivelatore Q-200DT senza fili a effetto tenda per interni a doppia tecnologia. Grazie a due sensori e all'analisi digitale dei segnali, Q-200DT rileva con precisione i corpi in movimento e può fornire anche la segnalazione della direzione del movimento. Oltre all'elevata sensibilità, la doppia tecnologia garantisce un'alta immunità ai falsi allarmi, mentre la compensazione della temperatura consente di adattare il rivelatore ad ogni condizione ambientale. Il rivelatore è munito di sensore inerziale che lo protegge da tentativi di rimozione o apertura, mentre l'antimascheramento vanifica la copertura del rivelatore.

Altri due nuovi componenti del sistema sono rappresentati dal rivelatore PIR senza fili Q-PIR200 e dal rivelatore a doppia tecnologia senza fili Q-PIR200DT. La tecnologia del rivelatore Q-PIR200 è basata sull'analisi digitale dei segnali tramite un elemento piroelettrico duale che rileva la radiazione infrarossa e un innovativo filtraggio del segnale. È in grado di rilevare con precisione l'intrusione di un corpo in movimento nell'area protetta. Il conteggio degli impulsi programmabile assicura un'alta immunità ai falsi allarmi. La compensazione della temperatura consente di adattare il rivelatore alle condizioni specifiche dell'ambiente in cui è inserito, mentre il sensore inerziale lo protegge da vibrazioni e inclinazioni dovute a tentativi di sabotaggio. La versione a doppia tecnologia Q-PIR200DT offre la funzione di antimascheramento tramite sensore a microonde. Il rivelatore ha un'alta immunità ai falsi allarmi grazie alla doppia tecnologia e al conteggio degli impulsi programmabile. Anche questa versione è dotata di compensazione della temperatura e di sensore inerziale.
Oltre alle novità di prodotto, nella stessa occasione HESA ha annunciato in anteprima la versione di firmware 2.0 della centrale Serie Quaranta. Questo aggiornamento apporta numerose e importanti novità, con l'introduzione di nuovi dispositivi senza fili. Permetterà ad esempio di visualizzare sulle tastiere touchscreen Q-TOUCH le mappe grafiche e un calendario per la gestione eventi e di integrare sull'interfaccia Q-IPW telecamere ONVIF per la videosorveglianza, con visualizzazione delle immagini tramite app Quaranta per Ios e Android.

CONTATTI

HESA SPA
(+39) 02 380361
www.hesa.com

H265, il cilindro del Mago per Videotrend e Dahua Technologies

a cura della Redazione

Il mercato della videosorveglianza professionale è spinto da una sempre più crescente domanda di alta definizione e con essa cresce anche lo sviluppo di elaborazione delle immagini. Si sente sempre più spesso parlare di 4K, che inizia a giocare un ruolo oramai vitale nella video sorveglianza, soprattutto in applicazioni come sicurezza urbana, parcheggi, porti, piazze e dove in generale giocano un ruolo importante la definizione dei dettagli delle immagini, la decodifica e lo spazio richiesto per la trasmissione e la registrazione di un numero sempre crescente di Bytes. Una buona notizia, a questo riguardo, è rappresentata dal nuovo codec **H265**, che offre livelli di compressione del segnale ancora più spinti, a parità di qualità, migliorando anche l'efficienza della trasmissione dei segnali video.

Vantaggi del codec H265.

High Efficiency Video Coding (HEVC), noto anche come H265, è un nuovo standard di compressione video recentemente presentato come successore dell'H264/MPEG-4 AVC (Advanced Video Coding) e, al momento, in via di sviluppo congiunto da parte del ISO/IEC Moving Picture Expert Group (MPEG) e del ITU-T (Video Coding Expert Group).

Se comparato allo standard AVC H264, il nuovo H265 dovrebbe essere in grado di ridurre di un ulteriore 50% il bit rate richiesto per codificare uno stream video di alta qualità. Il bit rate a 1080p si dice sia circa il 40-50% inferiore, sempre con immagini di ottima qualità.

In definitiva il nuovo H265 può ridurre le dimensioni del video compresso in modo significativo permettendo anche con una bassa banda una visione fluida

e favorendo così la domanda del mercato per apparecchiature 4K/Ultra HD. Inoltre, con il rapido sviluppo delle tecnologie mobili e 4G, la integrazione fra queste due industrie aprirà nuovi meravigliosi possibili scenari.

Dahua: l'offerta di prodotti 4K.

Nonostante i notevoli benefici, la nuova tecnologia non è ancora stata adottata dall'industria della videosorveglianza, in quanto questa compressione rappresenta ancora una novità. Ci vorrà pertanto ancora del tempo prima che abbia una più vasta applicazione. **Dahua Technology,** azienda tradizionalmente leader ed innovativa, riconosce le qualità e il grande impatto di questa nuova tecnologia e ha pertanto voluto adottare H265 nella sua gamma di nuovi prodotti quali telecamere,

NVR, apparati di trasmissione e sistemi di Video-wall. Dahua ha recentemente rilasciato una nuova telecamera IP da 5 megapixel della serie Ultra Smart che utilizza ambedue i codec H264 e H265 permettendo di ridurre la banda di circa il 40% con una qualità di immagine ineguagliabile. Inoltre, grazie alle altre funzioni quali Ultra Defog, RoI e alle rilevazioni intelligenti, questa telecamera può rendere la sorveglianza più chiara, più intelligente e più fluida. Sulla scia di questo prodotto noi possiamo pertanto aspettarci di vedere a breve sempre più telecamere H265 in modelli con diverse risoluzioni.

Per quanto riguarda i videoregistratori, Dahua è stata la prima azienda del settore a introdurre una gamma completa di NVR 4K con H265 per coprire ogni fascia di utilizzo, dalla medio-bassa alle applicazioni di grande scala. Questi NVR hanno capacità di decodifica fino a 12 Megapixel, con 60 fps @1080p con preview e playback H265, e con live e playback in real time di 4 canali a 4K. Inoltre hanno anche delle funzioni intelligenti di analisi video, di rilevamento facciale e altre.

Un'attenzione particolare viene anche dedicata da parte del team R&D al contenimento dei consumi delle apparecchiature.

Anche nel settore dei suoi prodotti per Video-wall, Dahua ha adottato la tecnologia H265 nella nuova piattaforma M70 capace di decodificare simultaneamente canali multipli in H265. In virtù del suo progetto modulare la M70 può gestire e decodificare in uscita fino a 40 canali UHD (Ultra High Definition) H265.

Questi canali HD possono anche combinarsi per generare una immagine integrata sul video-wall.

H265 offre nuove possibilità.

"*H265 è uno dei maggiori standard di compressione che ci permette di implementare soluzioni UHD come 4K o anche 8K, e che rappresentano, in definitiva, il trend della videosorveglianza*" commenta **James Wang,** Product Director di Dahua Technology.

"*I vantaggi portati da H265 non si limitano a quanto appena detto" ha aggiunto Wang, "proprio come dal cappello di un prestigiatore, ci aspettiamo che escano parecchie altre cose, il nostro team di R&D sta lavorando a nuove possibilità quali il controllo del bit rate, il bilanciamento della qualità dell'immagine, e anche video analisi e tracking intelligenti*".

"*Sono sempre elettrizzato dalle novità e dalle nuove tecnologie, poiché hanno la possibilità di far evolvere e migliorare i prodotti, l'industria e perfino la società*" ha continuato Wang. "*H265 rappresenta proprio questo. Possiamo sfruttare con fiducia tutti i potenziali di questo nuovo standard e utilizzarli al meglio. Il mio consiglio è di rimanere con noi, rimanere con i trend più innovativi e vedere cosa saremo capaci di far uscire dal cilindro del mago*"

Dahua Technology è distribuita, in Italia, da VIDEOTREND Srl

Videotrend S.r.l.
Distributore ufficiale Dahua
Tel. 0362 1791300
www.videotrend.net / info@videotrend.net

CONTATTI

VIDEOTREND SRL
(+39) 0362 1791300
www.videotrend.net
e.minotti@videotrend.net

Comunicazione IP e Cloud: cosa dice Pyronix

a cura della Redazione

L'era digitale in cui viviamo ci permette di fare cose nuove e sorprendenti con oggetti di uso quotidiano. Da anni l'uso delle tecnologie digitali è in aumento e, considerando le vendite mondiali di smartphone, ormai raddoppiate rispetto a quelle di computer fissi e portatili, è evidente che la tendenza verso una maggiore mobilità non può essere ignorata. Se, da una parte, è importante accogliere con favore le nuove tecnologie, dall'altra non bisogna dimenticare le caratteristiche fondamentali tipiche dei sistemi di sicurezza e la loro cruciale funzione per proprietari di abitazioni e di attività commerciali. Lo scopo primario è proteggere la vita e gli oggetti di valore da intrusioni esterne. Tuttavia, non dobbiamo essere insensibili ai progressi della tecnologia e alle richieste degli utenti per i loro sistemi di sicurezza.

Come possiamo, quindi, trarre vantaggio dalle tecnologie digitali nel settore della sicurezza, noi produttori e installatori? Poiché oggi i sistemi di sicurezza si orientano verso le comunicazioni via Internet (IP), assistiamo non solo ai vantaggi rappresentati da una riduzione dei costi di manutenzione e da una comunicazione più affidabile, ma anche al proliferare di opzioni potenziate per sistemi antintrusione mai viste prima. Prodotti interconnessi che comunicano tra di loro attraverso Internet permettono una maggiore integrazione, aspetto già messo a frutto da alcuni operatori del mercato.

Detto ciò, sono numerosi i grandi cambiamenti tecnologici spesso ostacolati dall'infrastruttura concepita per ampliare al massimo la disponibilità della soluzione. Sebbene la possibilità di comunicare tramite IP non sia nuova, l'infrastruttura per rendere quest'opzione ampiamente disponibile è stata accettata e utilizzata nel mercato italiano dei sistemi antintrusione solo recentemente. Il mercato è ora maturo per accettare la tecnologia e favorirne la diffusione, rendendo la soluzione più praticabile per molti installatori, ma anche per molti proprietari di abitazioni e di attività commerciali.

Il cambiamento tecnologico rivoluzionario reso possibile dall'IP nel rilevamento di intrusioni consente di controllare in sicurezza la propria abitazione da dispositivi smart, via app e Internet. L'attuale diffusione di smartphone rende il controllo dello spazio domestico attraverso le app una necessità per i produttori di sistemi di allarme antintrusione sul mercato. Accanto ad una rivoluzione dei prodotti assistiamo anche ad una rivoluzione delle aspettative di utenti e installatori nei confronti dei sistemi di sicurezza: le loro necessità e richieste sono cambiate e questa nuova tecnologia è considerata un requisito minimo.

L'integrazione più semplice di altri prodotti nel sistema di sicurezza è un'altra delle opzioni messe a disposizione dalla tecnologia cloud, che permette ai produttori di sistemi di sviluppare prodotti nuovi e più allettanti per il mercato. L'integrazione di telecamere IP e dispositivi di automazione domestica, tutti collegati attraverso Internet, attribuisce un aspetto completamente nuovo all'idea di sistema di sicurezza. Se le telecamere IP in rete non sono una novità, il pas-

so successivo è inserirle all'interno dell'intero sistema antintrusione. Applicato alla possibilità di tenere sotto controllo il sistema antintrusione attraverso un dispositivo smart e telecamere in rete nel proprio sistema, questo è un grande vantaggio messo a disposizione degli utenti da Internet e dagli smartphone.

Il raggio di integrazione si è ampliato con una maggiore interconnettività tramite IP. Soluzioni interamente integrate, precedentemente riservate ai segmenti più alti del mercato, diventano oggi una possibilità praticabile. Integrare l'automazione domestica con i sistemi antintrusione è un'attività tipicamente dispendiosa e lunga che prevede la posa di cavi e l'attivazione di terminali dal pannello di controllo. Il futuro dell'automazione domestica all'interno dei sistemi antintrusione prevede l'integrazione tramite IP, utilizzando la tecnologia cloud. In questo modo i sistemi possono comunicare tra di loro in maniera più efficace e più intelligente, facendo diventare smart le abitazioni e migliorando notevolmente l'esperienza dell'utente.

Questo cambiamento nella proposta di valore comporta per i produttori la necessità di adattare le loro strategie in modo da accogliere i prodotti di questa nuova era, visto che non si tratta più di vendere singoli sistemi di sicurezza fisici. Oggi le aziende possono sfruttare la rivoluzione rappresentata dagli smartphone, creando app perfettamente integrate con i loro prodotti attraverso l'infrastruttura cloud. L'ecosistema di connettività tra i sistemi domestici, il cloud e i dispositivi smart dell'utente crea una nuova prospettiva per l'amministrazione del sistema. Ora gli utenti dispongono infatti di un pannello di controllo digitale e una tastiera portatile per gestire il loro sistema domestico. Questa tecnologia eleva il sistema di sicurezza dal mondo degli acquisti obbligati al mondo degli acquisti di lifestyle che integrano la vita quotidiana dell'utente.

I vantaggi, però, non sono *solo* per l'utente finale. Questa nuova tecnologia comporta anche per gli installatori il vantaggio di poter accedere al pannello di controllo attraverso connessioni IP, in modo più sicuro e più rapido rispetto ai metodi tradizionali. L'infrastruttura cloud può persino permettere agli installatori di gestire più sistemi allo stesso tempo, con la possibilità di trasferire la gestione cloud agli utenti o includerla nei servizi offerti. Se al momento molti produttori si concentrano principalmente sull'esperienza per l'utente unendo le tecnologie, il cloud porterà con

sé un cambiamento generale nel modo in cui gli installatori gestiscono e curano i loro sistemi in futuro.
Utilizzando l'infrastruttura cloud, il monitoraggio dei sistemi di allarme diventa più semplice e più sicuro, comportando un vantaggio per i centri di ricezione allarme che utilizzano le comunicazioni IP. Poiché IP significa costi minori e interrogazione più frequente del sistema d'allarme, i centri di ricezione allarme saranno in grado di fornire un sistema più affidabile e sicura ai clienti.
Come accade per molti mercati dipendenti dalle tecnologie, il settore dei sistemi antintrusione dovrà rimanere vigile rispetto ai cambiamenti nelle nuove tecnologie, in particolare a quelli potenzialmente utilizzabili in maniera più innovativa. Solitamente, più delle tecnologie stesse è la loro applicazione che permette alle aziende di sfruttare le opportunità presentate. Le modalità con cui le organizzazioni utilizzano e sfruttano in maniera innovativa tali opportunità, integrando le ultime novità nella loro offerta di prodotti sul mercato, permetteranno ulteriori progressi al settore nel suo complesso.
Non dimentichiamo che l'assorbimento dinamico e la penetrazione delle nuove tecnologie nel mercato europeo è aspramente contrastata da rigidi standard quali WDS, EN50131, INSERT e NF2P. Questi standard sono stati concepiti per fornire quadri di riferimento chiari per l'installazione e l'uso di prodotti, tuttavia, poiché la definizione degli standard è un processo prolungato nel tempo, finora questi non si sono dimostrati in grado di tenere il passo con i progressi delle nuove tecnologie e dei nuovi sviluppi come cloud e IP.
Solo recentemente è stato approvato uno standard di trasmissione IP a livello europeo per le segnalazioni ai centri di ricezione allarme . Questi regolamenti sono un disincentivo per gli operatori del mercato all'adozione più massiccia di nuove tecnologie come cloud e app.
Detto ciò, il tasso di adozione di nuove tecnologie nel mercato italiano ha superato ampiamente gli standard e ciò rappresenta una serie di sfide per produttori e installatori. La sfida è introdurre flessibilità nell'offerta di prodotti e servizi, ampiamente influenza dal cliente (utente), senza compromettere la sicurezza e senza infrangere le regole.
È chiaro che, in ogni caso, restare competitivi nell'era digitale significa per le aziende cogliere le opportunità presentate dalle nuove tecnologie ed elaborarle all'interno della loro proposta di valore centrale.

L'ecosistema Centrax

I fornitori di Sistemi gestionali centralizzati complementari per il ticketing, anagrafiche aziendali, data mining; le soluzioni e i protocolli pubblici per il monitoraggio di impianti tecnici e per il risparmio energetico. Sesta e ultima parte

La cinque parti già pubblicate riguardavano la comunità degli utenti, quelle dei fornitori complementari di apparati e sistemi di videosorveglianza, di dispositivi di teleallarme, di centrali di allarme intrusione e incendio,di sistemi di erogazione del contante, di meccatronica, di gestione bussole e aree self-banking,di caricamento del contante

a cura di Bruno Fazzini, Citel spa

Sistemi centralizzati di sicurezza/safety/ticketing

Note legali

Fatti salvi quelli di Citel e dei suoi prodotti, tutti i marchi citati nel seguito di questo documento sono utilizzati unicamente a scopo illustrativo per una fruibilità immediata da parte del lettore. Ciò detto, Citel dichiara espressamente di non avere su di essi nessuno dei diritti che appartengono esclusivamente ai legittimi proprietari.

L'interesse del mercato e la richiesta

Soprattutto nelle installazioni di dimensioni consistenti o in organizzazioni complesse emerge la richiesta di interagire con altri sistemi informatici per uno scambio dati in ingresso e/o in uscita rispetto alle applicazioni di Centrax, dando luogo quasi sempre ad applicazioni interattive Server-Server come nei casi seguenti, alcuni occasionali altri di tipo organico e ripetitivo:

- trasmissione automatica al sistema di ticketing del manutentore di richieste di intervento contenenti la diagnostica di guasti in campo trattati da Centrax
- raccordo con sistemi informatici gestionali dell'utente o di suoi fornitori, come nel caso di GUP di Poste e Binka di Selex, utilizzati per ottenere, caricare e aggiornare dati anagrafici di referenti o impianti negli uffici periferici
- di sistemi specializzati di comunicazione satellitare come nel caso di Explor di Telespazio
- di moduli, su progetto, di analisi dei dati storici a fini predittivi

La disponibilità e la collaborazione delle terze parti
Nessun problema di disponibilità a fronte delle richieste di grandi utenti.

Le innovazioni introdotte con l'integrazione
L'innovazione di tipo generale risiede nel fatto che si tratta di casi, sempre più comuni, di interazione tra sistemi informatici dove la gestione della sicurezza fisica è, essa stessa, un sistema informatico gestionale dipartimentale, a conferma di quanto Citel ha sempre postulato.
Nel particolare – soprattutto nel caso dell'interazione con sistemi di ticketing – si tratta di innovazioni che finalmente convergono con la tendenza generale dei processi gestionali di produrre informazioni che passano dall'uomo solo per eccezione mentre di norma diventano dati che alimentano direttamente altri processi informatici a valle.

Il livello raggiunto dalle applicazioni
Nei casi citati si trovano esempi di come le applicazioni di sicurezza tendono ad essere riprogettate e affinate puntando anche sulla fluidità gestionale, sulla riduzione intelligente dei costi sfruttando strumenti – oltre a metodi e approcci – già largamente diffusi nei settori produttivi e amministrativi delle aziende.
Anche se il bilancio costi / benefici può essere controverso, per utilizzatori con una periferia da gestire numerosa, eterogenea e indisciplinata, il data mining & analysis può rivelarsi utile per isolare ricorrenze anomale o indesiderate e procedere di conseguenza a interventi correttivi o migliorativi di tipo impiantistico o comportamentale in determinate categorie di impianti nell'ambito della massa gestita. Oppure – teoricamente – per gestire in maniera selettiva – su basi predittive – determinati eventi decidendo in definitiva di risparmiare risorse correndo un (maggior) rischio calcolato.

Monitoraggio impianti e risparmio energetico

l'interesse del mercato e la richiesta
Citel riceve una spinta crescente dall'utenza ad allargare le funzionalità di telegestione anche in direzione degli eventi di natura tecnica e strumentistica, e per verificarlo basterebbe il prospetto soprastante, comprendente sia marchi con protocollo proprio che protocolli pubblici del settore industriale.
La spinta primaria è attualmente quella di chi ha adottato Centrax per applicazioni di sicurezza e vede la possibilità di estenderne l'utilizzo ottenendo progressivamente funzioni di building automation partendo dal controllo dei consumi di energia. Si tratta di una progressione agli inizi, ma destinata ad estendersi al pari del settore della sicurezza fisica, in passato dominato dai sistemi chiusi mono-fornitore e oggi in fase di progressiva conversione all'apertura multifornitore.
Il Centrax è un sistema di tele-gestione proceduralizzata di eventi e situazioni. E gli eventi e le situazioni vanno

gestiti secondo criteri di efficienza e di conformità alle norme e alle buone pratiche. Che gli eventi siano generati da impianti tecnici per la sicurezza fisica piuttosto che da impianti tecnici per la vivibilità dell'edificio non fa differenza sul piano concettuale mentre viene messa a fattor comune la sistemistica informatica che permette la gestione delle relazioni tra apparati e o sottosistemi, anche indipendentemente dal fatto che siano di produttori differenti.

L'utilizzo di Centrax in senso multifunzionale, in alternativa a più sistemi specializzati e separati, porta vantaggi gestionali ed economici per l'utente facilmente intuibili, ma la sua credibilità in settori esterni alla sicurezza ha origine nelle competenze specialistiche del laboratorio di progettazione di Citel che comprende anche specialisti di controllo di processi industriali. Non a caso tra le prime applicazioni di Centrax c'è stata la gestione dell'allarmistica tecnica in caselli e gallerie di una concessionaria autostradale.

La disponibilità e la collaborazione delle terze parti

Il settore del building automation, quindi quello della climatizzazione e degli impianti tecnici, ha fornitori in prevalenza multinazionali con una notevole propensione per i sistemi multifunzionali – sicurezza fisica compresa – ma di tipo protetto. Questa politica, basata su protocolli chiusi e di solito non disponibili, è però sempre meno accettata dal mercato e si suppone che sarà sempre meno praticata dai fornitori, e lo dimostrano casi già verificatisi di forzatura dell'apertura ad opera di grandi clienti. Quando non si tratta di sistemi di Building Automation ma di singoli sottosistemi, da interfacciare a fini di telecontrollo, è possibile che non vi siano preclusioni purché a chiederlo siano grandi utenti.

le innovazioni introdotte con l'integrazione

Le innovazioni che hanno sollevato già interesse tra gli utilizzatori Centrax sono quelle per il telecontrollo di apparati o sottosistemi di controllo dei consumi di energia. L'innovazione emergente va a toccare invece il settore del Building Automation per affermare progressivamente l'interoperabilità e il governo complessivo dei sottosistemi specializzati di gestione, includendo anche la climatizzazione, ad opera di un supervisore in regola con i requisiti PSIM. L'integrazione in ambito Centrax del monitoraggio impianti permette appunto l'interazione in architettura aperta e condivisa con le applicazioni della sicurezza e della safety passando da una rete dati e ottenendo:

- l'immediatezza della segnalazione, il monitoraggio della rete, l'affidabilità della trasmissione dei dati, grazie alle prestazioni e alle garanzie delle connessioni basate sulle norme CEI 79/5-6
- il trattamento corretto, proceduralizzato, tracciato, auditabile dell'allarme tecnico e dell'intervento, la possibilità di aprire ticket in automatico, ecc.

Più in generale, il committente e il progettista possono già pensare in termini di "automazione e controllo di edifici in *Open Architecture*", *dove convivono sottosistemi di sicurezza, safety, automazione scelti singolarmente in base a valutazioni di prestazioni/prezzo ma interoperanti tra di loro e controllati da un supervisore unico. Senza considerare che la sistemistica aperta di Centrax permette di gestire non solo un grande edificio o comprensorio, ma anche – sotto una regia unica – un insieme di edifici dell'organizzazione in un ambito corporate o dei clienti di una società di servizi.*

il livello raggiunto dalle applicazioni

Il caso di più immediata applicazione è stato lo sfruttamento delle prestazioni e dell'affidabilità delle connessioni CEI 79/5-6 over-IP per la connessione di apparati tecnici per la segnalazione di anomalie, superamenti di soglia ecc. Si pensi, solo per fare un esempio, al monitoraggio della catena del freddo nella GDO con la segnalazione garantita degli allarmi (o delle misure) provenienti dai dispositivi di monitoraggio dei surgelatori, ottenuta a costo zero o quasi se innestata nella sistemistica per la sicurezza, e con una qualità tecnica e gestionale di un altro ordine di grandezza rispetto alle formule correnti nel settore dei teleallarmi. In fase di propagazione è il controllo dei consumi di energia come applicazione aggiuntiva al Centrax esistente; in questo caso non conta tanto la sicurezza della trasmissione quanto il fatto che sia gratuita e comunque assicurata. Il catalogo dei moduli Centrax prevede ora una famiglia di moduli di integrazione ma anche di misurazione, di interazione via protocollo con sistemi di condizionamento, di generazione, di continuità, ecc.

Kaba exos 9300 4.0: sicurezza globale ed organizzazione efficiente

a cura della Redazione

La sicurezza e l'organizzazione sono due asset importanti per le aziende. Oltre a migliorare la sicurezza, le soluzioni Kaba sono sinonimo di processi operativi ed organizzativi più trasparenti, sicuri ed efficienti, come dimostra la nuova release del sistema Kaba exos 9300 4.0.

Kaba, da sempre attenta alle esigenze di sicurezza ed organizzazione delle aziende, presenta la nuova release del sistema di controllo accessi Kaba exos 9300, potenziato con una serie di nuove applicazioni altamente innovative.

Gestione visitatori

Il modulo di gestione visitatori della versione 4.0 di Kaba exos 9300, una vera maior release, è caratterizzato da una nuova interfaccia web semplice ed intuitiva. Il personale di reception è guidato passo dopo passo nel processo di registrazione del visitatore, l'apposito media di identificazione (tessera/badge) viene rilasciato in modo più rapido e semplice. I visitatori possono essere pre-registrati attraverso il web, prima della loro visita, ricevono una conferma via mail in formato .pdf della registrazione. Grazie al QR code stampato sulla conferma, i visitatori potranno essere identificati più velocemente ed il servizio di accoglienza alla reception ne beneficerà. Il sistema inoltre registra in modo dettagliato tutti i processi e garantisce sempre la tracciabilità nel rispetto delle linee guida interne e delle disposizioni di legge.

Mobile Access con NFC

La soluzione Kaba exos 9300 da oggi supporta completamente la tecnologia NFC. Con il modulo Kaba Mobile Access è possibile utilizzare uno smartphone con tecnologia NFC come supporto di accesso. L'assegnazione dei diritti viene eseguita a livello centrale nel sistema Kaba exos mentre la trasmissione al telefono avviene in modo sicuro attraverso un Trusted Service Manager. Allo stesso modo vengono comunicati al sistema centrale i transiti e lo status dei componenti di chiusura off line. Con il modulo Mobile Access e grazie alla distribuzione Over The Air, le funzioni ed i processi per la distribuzione di media d'identificazione e le autorizzazioni di accesso sono estremamente veloci e performanti; l'acceso è immediato sia per varchi controllati on line, sia per quelli controllati off line (CardLinkl) attraverso l'utilizzo dello smartphone come un badge.

Integrazione dei nuovi componenti wireless

Nella release 4.0 di Kaba exos 9300 è possibile integrare anche la nuova gamma di prodotti wireless, maniglie e cilindri digitali e meccatronici. Così, ai già affermati componenti stand alone (meccatronici, digitali e meccanici) e on line (lettori e controller), si aggiungono i nuovi dispositivi on line wireless. Questi componenti risultano ideali soprattutto per tutti quegli ambienti in cui il cablaggio non è possibile ma dove resta necessario il controllo on line del varco. Chiaramente, sui varchi controllati da questi dispositivi wireless, i processi di modifica\verifica delle autorizzazioni di acceso e di controllo degli allarmi diventano in tutto omogenei a quanto accade sui varchi on line cablati. Infine non occorre alcuna configurazione on-site in quanto la programmazione resta centralizzata come già oggi avviene su tutti gli altri dispositivi Kaba exos, sia per quelli predisposti per varchi on line che stand alone (CardLink).

CONTATTI

KABA SRL
(+39) 051 4178311
www.kaba.it

Video IP per il Comune di Arezzo da Videotrend e Dahua Technology

a cura della Redazione

Siamo ad Arezzo, una gemma incastonata nelle dolci colline toscane: città di origine antichissima, importante centro etrusco e poi romano.
Nel Medioevo divenne un potente libero Comune guidato dai vescovi, Conti del Sacro Romano Impero, sempre in lotta con Siena e con Firenze, che la assoggettò nel 1384.
Il centro storico conserva ancora tutto il fascino del passato e suoi tanti monumenti sono arricchiti dalle opere di grandi artisti rinascimentali, come Cimabue, Piero della Francesca, Andrea della Robbia e Giorgio Vasari ed è anche la città dove è nato il grande poeta Francesco Petrarca.
In anni più recenti ha ospitato il set cinematografico per registrare tante scene del famoso film di Roberto Benigni "La vita è bella", vincitore nel 1999 di ben 3 premi Oscar.

Città d'arte del passato e del presente, con una forte vocazione turistica, offre ancora oggi gli antichi sapori della cucina toscana mentre nelle sue vie si scopre un artigianato di qualità e, soprattutto, una esperienza orafa che l'ha resa famosa in tutto il mondo.

L'esigenza

Costituisce, infatti, uno dei più importanti poli produttivi italiani per la lavorazione dell'oro ed in particolare ospita, in Località Pratacci, alcune delle aziende più affermate del settore. Nell'ambito della riqualificazione degli impianti di illuminazione stradale, l'amministrazione comunale si è posta l'obiettivo di fornire a questa zona della città, un'efficace sistema di monitoraggio e controllo video per garantire un elevato sistema di sicurezza. Le varie possibili tecnologie sono state attentamente valutate da parte degli uffici tecnici del Comune, anche grazie al supporto del personale qualificato Videotrend, importatore ufficiale dei sistemi professionali di videosorveglianza Dahua Technology in Italia, sino ad arrivare al progetto di un sistema estremamente innovativo, affidabile e dalle performance di assoluto livello.

La soluzione

L'impianto che ne è scaturito, cablato interamente mediante fibre ottiche, è basato sull'impiego di una macchina di registrazione NVR VKD4128 che provvede a registrare 62 flussi IP corrispondenti ad altrettante telecamere con risoluzione nativa Full HD (1920x1080) di tipo VKD-ME250.

Gruppi di 4 telecamere IP confluiscono ad apparati switch industriali con terminazioni in fibra multimodale ad attacco SC, per connessione a due armadi stradali che fungono da centro-stella. Infine due dorsali monomodali portano i flussi ad uno shelter che ospita gli apparati di registrazione, peraltro dotati di RAID da 16 dischi da 3,5" per il massimo della sicurezza ed affidabilità nella protezione dei dati.

Sono state inoltre previste 5 telecamere per lettura targhe VKD-CPR200 in corrispondenza di altrettanti varchi di accesso all'area. Mediante un sistema hw/sw denominato CENTER e sviluppato interamente da R&D Videotrend, vengono registrate e classificate le informazioni di screenshot per una rapida fruizione finalizzata al rilevamento dei transiti. Le telecamere dispongono di OCR a bordo rendendo il sistema veloce ed estremamente efficace.

I vantaggi

Il complessivo risultato portato a collaudo è stato ritenuto ineccepibile, anche grazie ad una corretta e sapiente posa in opera da parte di società specializzate, che hanno concorso alla perfetta realizzazione di tutte le connessioni sotto la supervisione diretta di personale tecnico Videotrend.

La tecnologia Dahua ha permesso di ottenere un sistema di videosorveglianza professionale di altissimo livello che, sotto il profilo del rapporto prestazioni/costi, non ha rivali.

Dahua Technology è distribuita, in Italia, da VIDEOTREND Srl

Recinzioni, l'innovazione firmata BETAFENCE

a colloquio con Alfredina Gloria, Innovation Manager Betafence Italia
a cura della Redazione

L'innovazione è nel Dna di **Betafence Italia,** che ha istituito presso la propria sede un centro specializzato, punto di riferimento per l'intero Gruppo.
L'ufficializzazione dell'attività del centro, insieme alla presenza di uno stabilimento con un'elevata capacità produttiva, hanno consentito alla sede italiana di rivestire all'interno del Gruppo Betafence un ruolo d'importanza strategica.
Innovare costantemente, brevettando prodotti unici nel mercato, ha portato Betafence a divenire un'azienda di riferimento internazionale nel settore delle recinzioni, consolidando giorno dopo giorno la propria posizione.
L'ingegner **Alfredina Gloria**, **Innovation Manager Betafence Italia**, è da qualche anno la responsabile del centro innovazione della filiale italiana del Gruppo a Tortoreto (TE), e racconta come Betafence interpreti il concetto d'innovazione.

Innovare per crescere

In settori competitivi come quello della sicurezza, una cultura aziendale volta alla continua ricerca di innovazione è fondamentale, perché rimanere fermi vuol dire perdere potenzialmente quote di mercato. Innovare per Betafence vuol dire anticipare i competitors, sia per quanto riguarda i materiali e le tecnologie, che per il design e l'ideazione di nuovi prodotti. Per questo, Betafence rinnova ogni anno le proprie gamme di prodotti, migliorando quelli già esistenti e proponendo nuove idee, materiali innovativi, soluzioni più adatte a soddisfare le necessità e il gusto dei propri clienti. Sperimentiamo nuovi materiali, lavoriamo ad esempio a nuove verniciature, lavoriamo con metalli innovativo come Corten e alluminio negli accessori. Investiamo inoltre sul design e ultimamente stiamo operando per l'integrazione dell'acciaio con altri materiali (con legno, pietra, vetro); un palo contenente corpi illuminanti off grid che diviene un vero e proprio elemento di arredo e design con nuove funzionalità.
In Betafence infatti l'estetica non rinuncia mai alla funzionalità: se da un lato curiamo nel dettaglio ogni prodotto al fine di proporre prodotti di alto valore estetico, dall'altro, quando li progettiamo partiamo sempre dalle loro qualità intrinseche che devono essere l'utilità fun-

zionale, la praticità nell'uso, la semplicità d'installazione e la durata nel tempo.
Dal punto di vista tecnologico,abbiamo raggiunto traguardi importanti nell'ambito della ricerca sul coating dei fili di acciaio, ambito in cui lo stabilimento italiano è uno stabilimento pilota.
Impieghiamo leghe di alluminio e zinco, materiali performanti ma lavoriamo anche su nuove leghe. Teniamo a sottolineare che, per rispettare il nostro impegno verso l'ambiente, scegliamo solo materie prime certificate, prive di sostanze tossiche o nocive, in accordo con le normative REACH e operiamo per individuare materiali e soluzioni sempre più eco-compatibili. Anche a livello di processi produttivi, puntiamo alla riduzione dell'impatto ambientale.

I punti di forza del centro innovazione Betafence
Il capitale più importante per Betafence sono le persone che ogni giorno operano per produrre sicurezza offrendo soluzioni industriali capaci di assicurare la protezione adatta a ogni livello di necessità. La nostra forza è prima di tutto nella nostra squadra, un gruppo dinamico sempre pronto a recepire ed anticipare le esigenze del mercato. La sinergia tra ingegneri, tecnici di cantiere, esperti di settore e funzionari tecnico-commerciali di consolidata esperienza, in un'attività coordinata in tutte le fasi consente di proporre soluzioni capaci di rispondere alle esigenze reali del mercato, apportando un contributo di miglioramento funzionale delle soluzioni già esistenti o soluzioni alternative nuove destinate a diversi settori: dalle infrastrutture all'alta sicurezza dall'impiantistica sportiva fino al residenziale. Una delle chiavi di successo dei nuovi prodotti proposti al mercato è nella forte sinergia con la produzione. Nell'intero progetto che dall'ideazione porta allo sviluppo dei nostri prodotti, è affidato un ruolo importante e imprescindibile alla produzione, attraverso alcune figure di riferimento qualificate e selezionate per una costante ottimizzazione delle proposte.

SECURIFOR® 4D: maggior rigidità contro le intrusioni

a cura della Redazione

Nuovo sistema di recinzione alta sicurezza

La gamma Betafence destinata al settore dell'alta sicurezza è in costante ampliamento. Lo testimonia il recente ingresso di **Securifor® 4D**, un sistema di recinzione con tutte le caratteristiche delle soluzioni Securifor, ma **ancora più rigido**.

Come gli altri modelli in gamma, Securifor 4D presenta una **maglia molto stretta** (12,7 x 76,2 mm), fili robusti, ravvicinati tra loro e di diametro elevato; la particolarità è data dai **fili orizzontali che si susseguono in alternanza dal fronte al retro del pannello.** Questo dettaglio costruttivo fa sì che il sistema sia **ancor più resistente al taglio e molto difficile da scavalcare**, rappresentando un'efficace **soluzione di rallentamento**.

Secondo prove effettuate presso uffici di polizia specializzata, le maglie Securifor vantano un indice di resistenza fino a 40 volte superiore ad altre tipologie di recinzione. Severi test sulle prestazioni dimostrano che Securifor 4D **ha una rigidità fino a 10 volte maggiore rispetto agli altri pannelli della gamma Securifor.**

Ecco perché **Securifor 4D è la recinzione ideale** per ostacolare gli accessi non autorizzati a **caserme, basi militari, ferrovie, siti industriali e commerciali, carceri e centri di detenzione**. Con il suo design pulito ed essenziale, ha un **impatto visivo discreto**, integrandosi con facilità nel contesto ambientale ed architettonico di utilizzo.

Nonostante la struttura a maglia stretta, Securifor garantisce **un'elevata trasparenza** offrendo un'**ottima visibilità**, anche laterale.

Il sistema è abbinato a tutti i sistemi di fissaggio standard (Bekafix® Super, Pali rettangolari); prevede inoltre l'utilizzo del palo Bekasecure®: oltre alla propria funzione strutturale, Bekasecure permette il cablaggio di **sistemi attivi**, con il passaggio al suo interno di cavi energia, cavi dati e cavi a fibra ottica. Permette inoltre l'installazione facilitata di dispositivi di illuminazione e video controllo sulla sommità del palo stesso. La recinzione diviene così **sistema di difesa integrato con gli impianti di illuminazione, videosorveglianza e comunicazione.**

La gamma Securifor è disponibile anche nelle configurazioni 2D, 3D, Double Skin e Flat per rispondere a specifiche esigenze e livelli di sicurezza.

CONTATTI

BETAFENCE ITALIA SPA
(+39) 0861 7801
www.betafence.it

Security for Retail

GLI EVENTI DI ESSECOME

SECURITY FOR RETAIL SHOW

Milano
3-5 novembre 2015

Fiera Milano - Rho

SICUREZZA

Le presentazioni a Security for Retail Forum 2015

SafePay™ Gunnebo per la sicurezza del contante

Il sistema **SafePay ™ di Gunnebo** rende a un tempo più veloci e più sicure le operazioni di cash-in-transit. Il ciclo del contante dalla cassa al trasporto valori è completamente chiuso e sicuro, e il flusso del denaro non è mai stato così scorrevole. I retailer che hano provato **SafePay ™** sanno di potersi aspettare ottimi risultati in tempi rapidi. **SafePay ™** rende automatiche le procedure di quadratura e controllo del contante, unifica il processo di gestione del contante per tutte le aree del checkout compreso il self service, e fornisce i rendiconti on line. Anche il personale è subito in grado di apprezzarne i vantaggi: **SafePay ™** azzera il problema dei resti, riconosce i falsi con un'affidabilità certificata dalla BCE, elimina i compiti ripetitivi e la manipolazione di monete e banconote. Con **SafePay™** aumenta naturalmente anche la sicurezza del punto vendita: senza contanti in circolazione, per eventuali rapinatori avvicinarsi al punto vendita diventa una perdita di tempo, a tutto vantaggio della tranquillità del personale e dei clienti, che vedono anche ridursi il tempo di attesa alle casse. I sistemi **SafePay™,** come tutte le soluzioni **Gunnebo**, sono personalizzabili in base alle esigenze del cliente per garantire un'integrazione ottimale nel contesto architettonico e lavorativo. Un'altra caratteristica di **SafePay ™** che permette a chi sceglie questo sistema una completa tranquillità, è la rivoluzionaria procedura di manutenzione. **SafePay™** è in realtà affidabile e robusto e di rado richiede interventi di assistenza ma, nel caso in cui questa necessità si presenti, il sistema è totalmente controllabile da remoto: l'operatore può prendere contatto con l'**Help Desk SafePay™** di **Gunnebo** e procedere a una rapida risoluzione del problema. Gli operatori dell'**Help-Desk SafePay™** conoscono a fondo il sistema e sono in grado di guidare l'operatore, un semplice passo alla volta, per eliminare piccoli guasti (un oggetto incastrato nel contamonete, ad esempio) senza il fermo macchina e con costi di manutenzione praticamente azzerati. L'efficienza dell'**Help-Desk SafePay™,** la semplicità del funzionamento e la chiarezza delle istruzioni fornite sono tali che tutti gli operatori possono risolvere gli eventuali piccoli inconvenienti senza alcuna difficoltà. **Gunnebo** opera sempre in stretto contatto con ciascun cliente, proponendo sistemi perfettamente idonei per le specifiche esigenze di ogni punto vendita. L'esperienza di **Gunnebo** ha infatti dimostrato che ottimizzando la gestione del punto cassa e il servizio di assistenza, nell'ambito di un rapporto di partnership con il retailer, si ottiene un importante risultato in termini di fidelizzazione del cliente finale, l'acquirente. La chiave del successo degli interventi **Gunnebo** è la capacità di porsi a fianco del cliente come un partner più che come un fornitore, studiando e comprendendo le esigenze e immedesimandosi in chi concretamente lavora o acquista nel negozio, utilizzando le soluzioni nel quotidiano, sempre con l'obiettivo di ottenere il miglior risultato possibile per tutte le persone coinvolte.

GUNNEBO
For a safer world

Ideale:
efficiente, remunerativo, innovativo.

Perfetto:
personalizzabile, curato in ogni dettaglio, accessibile anche da disabili.

Gradito:
discreto e sempre disponibile, anche oltre gli orari di apertura.

...e il Servizio?
Rapido, affidabile, attuabile anche da remoto.

In una parola:
SafeStoreAuto

il Sistema di Cassette di sicurezza self-service

Soluzioni che creano valore

- CONTROLLO ACCESSI
- TRATTAMENTO DENARO
- SICUREZZA FISICA
- SICUREZZA ELETTRONICA

www.gunnebo.it

GUNNEBO
For a safer world®

AXIS COMMUNICATIONS

Qual è il modo migliore per gestire luce e ombra?

Simultaneamente.

Questo perché le telecamere di rete Axis con tecnologia ad ampio intervallo dinamico (Wide Dynamic Range, WDR) possono gestire luci forti e ombre scure nella stessa immagine. Inoltre sta a significare che è più facile individuare e identificare persone, veicoli e incidenti, non importa quanto siano difficili le condizioni di illuminazione. Sono il responsabile per la sicurezza in una centrale elettrica e WDR mi ha semplificato notevolmente la vita.

Per maggiori informazioni su WDR, l'utilizzo delle immagini e la soluzione di sorveglianza migliore per le proprie necessità, vedere la guida interattiva Axis all'indirizzo www.axis.com/imageusability

I racconti della Sicurezza - 1

a cura di Raffaello Juvara

Iniziamo con questo numero di **essecome** una nuova idea editoriale, fuori dagli schemi consueti della comunicazione tecnica specializzata rivolta alla sicurezza: una collana di racconti dedicati proprio a lei, alla Signora Sicurezza, scritti da autrici e autori che, vivendo e lavorando con lei, la conoscono benissimo. Sarà dunque una raccolta di testimonianze di persone che, avendo "respirato" la sua stessa aria, la possono raccontare, con fantasia e leggerezza, senso dell'umorismo o anche dell'horror e del pulp, in funzione delle proprie conoscenze e delle proprie ispirazioni letterarie…

È un nostro piccolo contributo per allargare la sfera della conoscenza di una Signora tanto affascinante quanto poco conosciuta, al di là dei luoghi comuni, da parte di coloro che non hanno il privilegio di vivere nella sua corte. Iniziamo la collana con "**Il Caravaggio rubato**", un breve racconto di **Simona Nistri,** responsabile relazioni istituzionali e esterne della Fondazione Enzo Hruby, tratto dalla rivista trimestrale "EHF-Sicurezza per la cultura", organo ufficiale della Fondazione Enzo Hruby, anno XXII - n. 2 giugno 2013, che ringraziamo per la cortese disponibilità.

Invitiamo tutti i nostri lettori a inviarci i loro racconti, novelle, fiabe, poesie: sarà un nostro piacere pubblicarle nelle nostre pagine.

Il Caravaggio rubato
Uno dei furti d'arte più clamorosi nella storia, visto con gli occhi della tela

di Simona Nistri

Sono arrivata nell'Oratorio di San Lorenzo, a Palermo, nel 1609 e lì rimasta fino a quella fatidica notte tra il 17 e il 18 ottobre del 1969, quando venni letteralmente strappata da quella che fu la mia casa per oltre 300 anni. Io, chiamata la *Natività*, un olio su tela di 298 per 197 centimetri, realizzata da uno degli artisti più autorevoli del mio tempo, Michelangelo Merisi, conosciuto anche come il Caravaggio, un nome che farà la storia dell'arte, arrotolata come un misero tappeto, caricata su una motoape e portata via da qualche balordo.
"Incredibile", "unica", "preziosa", questi gli aggettivi usati per descrivermi… eppure pochi minuti sono bastati, e di me non è rimasto più nulla.
Ricordo perfettamente quella notte: come ogni sera il parroco della chiesa mi ricopriva con una tenda vetusta, unica protezione per la mia incolumità, e chiudeva quella porta che ormai da tempo non costituiva più alcun ostacolo per i malintenzionati.
A proteggermi, dunque, solo le statue del sommo Giacomo Serpotta che ornavano la nicchia in cui ero stata incastonata, ma che nulla poterono davanti allo scempio al quale stavano per assistere.
All'improvviso uno squarcio.
Cosa succede? Fate piano!…. Una lametta inizia a tagliarmi lentamente, sento che sto perdendo aderenza dall'imponente cornice che per tre secoli mi ha cullata all'interno della nicchia a me destinata, brucia e sento il sangue iniziare a colare sui bordi.
Fate piano…non sono una tela fatta di sacco, sono preziosa insomma!
Ma nulla, nessuno mi sente.
La lama del taglierino continua a ferire, o meglio, a strappare i miei bordi, malamente, frettolosamente. Forse i balordi non hanno tempo e, a giudicare dal modo maldestro e poco preciso con cui stanno operando, direi che non hanno idea di cosa stiano compiendo e soprattutto contro cosa… contro una delle opere più significative del Maestro Caravaggio.

Mi strappano, mi scorticano viva dalla cornice e, in men che non si dica, mi ritrovo arrotolata su me stessa come se fossi un qualsiasi disegno su cartoncino. Sento ora solo il freddo della notte, non so dove mi stiano portando,non so chi abbia voluto tutto questo e nemmeno perché.
Poi il silenzio, lo stesso silenzio che avvolge me e la mia scomparsa da oltre quarant'anni. Nessuno sa dove sono, nessuno ha la volontà di far sapere dove sono, ma so che mi stanno cercando e chissà, forse un domani riuscirò a riprendere il mio posto in quella nicchia di San Lorenzo, circondata dalle statue del Serpotta contente di rivedermi, magari protetta da qualcosa di più efficace e all'avanguardia di una semplice tenda.

PREMIO H D'ORO

2006 • 2015

DIECIANNI

L'unico Premio che valorizza
la professionalità degli installatori
di sistemi di sicurezza

Vieni a conoscere il Premio H d'oro sul nostro sito
e candida i tuoi migliori impianti

Per informazioni: Segreteria organizzativa Premio H d'oro
tel. 02.38036625 - candidature@accadoro.it - www.accadoro.it

FONDAZIONE ENZO HRUBY

Il gancio BENOIS per la sicurezza in teatro e non solo

a colloquio con Michele Letizia e Loris Zenarola, designer del gancio Benois
a cura della Redazione

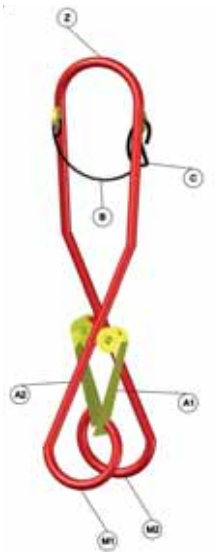
A uno spettatore che assiste a un'opera teatrale spesso sfugge che dietro al sipario e alle quinte c'è un cantiere permanente, per preparare gli allestimenti tra un'opera e l'altra, e cambiare le scene durante gli intervalli. Un cantiere che espone sia i tecnici (macchinisti, elettricisti, attrezzisti, scenografi) che gli stessi artisti al rischio di infortuni di vario genere, in particolare quelli derivanti dalla caduta accidentali di carichi sospesi. In base alle vostre esperienze maturate e visto che tra voi uno dei due funge anche come RLS in uno dei più importanti teatri del mondo, quali misure di prevenzione potrebbero essere adottabili per proteggere l'incolumità delle persone?

Il teatro è come una scatola magica che può sorprendere in qualsiasi momento, anche nei "fuori programma". Parlando del rischio di infortuni di chi lavora al suo interno, la prima osservazione è che tutti, artisti e tecnici, si trovano sotto la "torre scenica", uno spazio che si sviluppa in altezza per alcune decine di metri subito dietro il sipario, dove vengono sospese le scene, le luci e quant'altro è necessario per mettere in scena uno spettacolo. Tutto deve essere pronto per entrare in scena all'alzata del sipario e per effettuare i cambi di scena durante l'esecuzione, in modo veloce, silenzioso e soprattutto sicuro per le persone che si trovano sul palcoscenico. In un certo senso, è uno spettacolo nello spettacolo, che gli spettatori non possono vedere. È evidente che sollevare materiali pesanti come scene, proiettori e fondali, tenendoli in sospensione al di sopra degli artisti e dei tecnici significa doverlo fare secondo le norme anti infortunistica e nessuno permetterebbe il contrario, ma l'imprevisto può essere sempre in agguato, provocando situazioni che devono far riflettere chi ha la responsabilità della sicurezza dei lavoratori. Ad esempio, da un banale contatto tra due stanghe (o barre) che reggono i fondali, si potrebbe verificare una situazione potenzialmente pericolosa, quella di "appoggio" di una delle due stanghe: il movimento opposto, uno di salita e l'altro di discesa, potrebbe creare una collisione tra i fondali oppure l'aggrappo di un cordino o altre criticità che potrebbero degenerare in un batter d'occhio in un incidente per i carichi sospesi. Dall'osservazione di questi fatti è nato "BENOIS", un gancio per assicurare i carichi sospesi ideato proprio per evitare incidenti di questo tipo, tra i più frequenti e pericolosi che possono succedere in un teatro.

Ci può dare qualche dettaglio tecnico del gancio BENOIS?

In sostanza, è un gancio per sospensione o ricovero imbrachi, ideato appositamente per venire utilizzato su stanghe teatrali dedicate alla sospensione di fondali e telette scenografiche. Il gancio è costituito da un alloggio autoportante con sicura antislittamento e, in aggiunta, ha un doppio moschettone a cui fissare le cinghie da imbraco che trattengono in modo auto-assestante il carico ricoverato. La sua particolare conformazione serve per venire alloggiato sulla predetta stanga con un movimento semplice, veloce e sicuro da parte del personale tecnico preposto. Il gancio è ideato per venire costruito in acciaio tramite un processo di calandratura o piegatura, temprato, verniciato e completato con 2 molle di chiusura e cordino d'acciaio con moschettone di sicurezza. Ad aprile 2014è stato rilasciato dal MISE il brevetto per modello di utilità n. 277517 con la descrizione "Gancio polifunzionale ad utilizzo tecnico-teatrale per sospensione o ricoveri imbrachi".

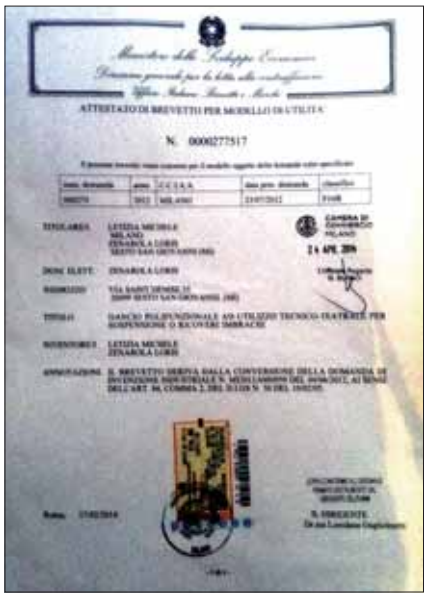
Sono prevedibili impieghi diversi da quelli in ambito teatrale?



Ci sono molte possibilità diverse di utilizzo di BENOIS. Attualmente, nel teatro dove è partita la sperimentazione il gancio viene utilizzato per la sospensione di elementi di illuminotecnica su stanghe teatrali e sembra stia interessando anche altri reparti del teatro stesso. In realtà, BENOIS è un sistema già pronto per evolvere nel campo dell'edilizia, della nautica, dell'agraria, della sicurezza degli operatori formati ai lavori in quota ecc. Ovviamente, per ogni settore il gancio BENOIS presenterà le dovute varianti sul tema, che verranno pubblicate in futuro.

Attualmente BENOIS è prodotto in piccola serie per la sperimentazione. È previsto uno sviluppo industriale per una vendita sul mercato attraverso i normali canali commerciali?

A noi farebbe piacere che il'utilizzo del gancio si consolidasse innanzitutto in ambito teatrale, promuovendolo presso le altre realtà teatrali italiane, fronte sul quale ci siamo già attivati. Inoltre vorremmo farlo conoscere in altri ambienti presentandolo, ad esempio, in occasione di manifestazioni relative alla sicurezza ed altro. I partner futuri potrebbero sicuramente essere delle imprese di servizi legati alla tecnica e alla sicurezza, escludendo al momento la vendita del brevetto. Auspichiamo che i nostri ipotetici clienti possano essere innanzitutto i grandi teatri italiani, ma ben vengano anche i grandi teatri internazionali, assieme agli utilizzatori di tutti gli altri settori!



Denaro Sicuro

Come cambia la sicurezza in banca – 3

a colloquio con Massimo Panizza, Security Risk Manager di Deutsche Bank Italy, che riporta localmente a Jacob Sahakian - Head of Corporate Security and Business Continuity

In questo momento, il sistema bancario italiano sta riorganizzando la rete, riducendo le filiali e riformulandone il lay-out, per adeguarsi alle nuove esigenze operative imposte dall'evoluzione del mercato. Quale impostazione sta seguendo Deutsche Bank per le proprie filiali in Italia, in correlazione con le linee guida globali del Gruppo?
Deutsche Bank rappresenta oggi in Italia uno dei più importanti gruppi bancari internazionali attivi nel Paese, a fianco di privati, famiglie, aziende e istituzioni. Con 650 punti vendita sparsi sul territorio e 5500 professionisti, l'Italia è per il Gruppo Deutsche Bank il suo primo mercato europeo (Germania esclusa). Negli anni, Deutsche Bank è cresciuta in Italia, aprendo nuovi sportelli e ampliando la propria presenza locale. Avvalendosi della propria esperienza internazionale, Deutsche Bank ha saputo anticipare i tempi strutturandosi in maniera adeguata e diversificata. L'attività di space optimisation e la revisione dei lay out dei propri punti vendita (dagli sportelli tradizionali a quelli cashless, dagli uffici dei promotori di Finanza & Futuro a quelli degli agenti di Deutsche Bank Easy) è stata perseguita nel corso degli anni con l'obiettivo di soddisfare al meglio le esigenze locali nel rispetto delle linee guida globali. Di recente, appare significativa la tendenza all'introduzione di sistemi di self banking che se, da un lato, comportano l'introduzione di nuove procedure per la protezione della giacenza e gestione dei flussi in entrata e in uscita, dall'altro consentono al personale di sportello di concentrarsi in attività a più alto contenuto professionale. Per quanto riguarda la security e le dotazioni di sicurezza, nel rispetto degli standards globali, Deutsche Bank fa costantemente riferimento ai protocolli locali e alle indicazioni di ABI Ossif, che rappresentano un importante strumento di analisi del rischio e di individuazione dei correlati interventi di mitigazione.

Dal vostro punto di vista, in che modo vanno adeguate le logiche progettuali della sicurezza fisica delle filali e, di conseguenza, le caratteristiche dei sistemi richiesti ai vostri fornitori?
In un'ottica di prevenzione, rimane fondamentale l'aspetto psicologico per il quale la presenza di sicurezza "percepita" in filiale *è un* elemento di deterrenza che può spostare l'attenzione di un certo tipo di criminalità.

Deutsche Bank ha lavorato molto su questo aspetto puntando sul costante aggiornamento delle misure di sicurezza e sulla loro interconnessione. Nella strategia di difesa rimane centrale la videosorveglianza personalizzata da remoto, integrata e interattiva con il sistema di centralizzazione allarmi. Per quanto riguarda l'antirapina è risultata estremamente positiva l'adozione della Virtual Guard, quale elemento che amplifica l'effetto di deterrenza associato alla presenza della videosorveglianza. Da ultimo stiamo testando, con ottimi risultati, sistemi di face detection che associano un basso impatto operativo ad un elevato impatto psicologico.
Con riguardo all'antifurto e all'antifrode, le strategie di difesa devono essere estremamente flessibili per potersi affinare all'evolversi della tecnologia e trovare risposte adeguate a tipologie di attacco nuove e diversificate. In quest'ambito, diventa fondamentale l'apporto dei nostri providers di sicurezza nella ricerca di soluzioni all'avanguardia e ritagliate "su misura".
Deutsche Bank rimane comunque un osservatorio privilegiato perché ad una struttura relativamente snella può associare un brand a forte identità, universalmente riconosciuto come sinonimo di efficienza e solidità.

Come viene sfruttata nel Gruppo la possibilità offerta dalle tecnologie over IP di utilizzare le infrastrutture e i devices dei sistemi di sicurezza anche per altri impieghi – ad esempio i software di gestione allarmi (PSIM) per funzionalità di domotica, e la videosorveglianza per la business intelligence - a favore di centri di costo diversi dalla sicurezza?
Le tecnologie over IP consentono soluzioni sino a poco tempo fa impensabili. Deutsche Bank, come per tutte le nuove tecnologie, sta effettuando le necessarie valutazioni rischi/opportunità al fine di ottimizzarne l'utilizzo. L'obbiettivo è di massimizzare l'integrazione tra i sistemi e i sottosistemi per migliorare il rendering ed incrementare il livello di controllo complessivo.

Evoluzione della filiale, evoluzione dei sistemi, evoluzione degli utilizzi: come si deve adeguare la funzione del security management della banca moderna per governare questo cambiamento epocale in atto?
La funzione del security risk management si è evoluta enormemente nel corso degli anni parallelamente all'evoluzione normativa ed agli accadimenti storici. Con la globalizzazione è aumentata l'incertezza e la percezione del rischio correlativamente all'aumento delle possibili minacce. È mutata la sensibilità normativa per quanto riguarda la sicurezza e sono mutati i suoi rapporti con la security, entrambe sempre più integrate nella vasta area del risk management. In Deutsche Bank, questo mutamento è stato particolarmente rapido per le sue caratteristiche di banca globale. Travel security, staff protection, building protection, event protection, executive protection, crisis management e business continuity hanno acquisito sempre più rilievo autonomo. Solo pochi anni fa non era nemmeno pensabile l'occupazione di una Filiale a scopi dimostrativi, magari con relativo video in Internet dopo qualche ora. Oggigiorno il rischio è concreto e da valutare per le significative conseguenze che comporta.

E come evolve di conseguenza la figura del security manager, in particolare in un Gruppo internazionale come Deutsche Bank?
La figura del Security Risk Manager è destinata ad assumere un ruolo sempre più centrale in azienda avendo importanti responsabilità strategiche per la protezione dell'azienda, delle sue persone e dei suoi beni. Fondamentale è diventato un approccio sistematico all'analisi del rischio, tenendo in considerazione tutte le tipologie di rischio, inclusi i rischi legali e reputazionali, in condivisione con la funzione di Risk Management. Ne consegue un necessario ampliamento delle competenze, rispetto all'impostazione classica concentrata sulla sicurezza fisica, e un aggiornamento continuo. In Deutsche Bank, allo sforzo di estendere l'analisi del rischio e gli interventi di mitigazione ai diversi aspetti della realtà aziendale, si unisce la necessità di svolgere appropriate attività di reporting a livello globale.


Ideale:
elegante, compatto,
personalizzabile.
Perfetto:
robusto, sicuro,
facile da integrare.
Gradevole:
silenzioso, discreto,
anche per disabili.
...e il Servizio?
Flessibile, rapido,
affidabile.
In una parola:
SpeedStile
il Varco per il controllo
degli accessi
Soluzioni che creano valore
• CONTROLLO ACCESSI
• TRATTAMENTO DENARO
• SICUREZZA FISICA
• SICUREZZA ELETTRONICA
Available on the App Store
GUNNEBO
For a safer world
www.gunnebo.it
Fotografa il QRcode con il tuo Tablet
e collegati direttamente allo Store Apple: potrai scaricare
la nuova applicazione gratuita che permette di visualizzare la foto del
tuo ingresso personalizzato con tutti i modelli di Varchi Gunnebo.
Flessibile, intuitiva, utile per il tuo lavoro!

Aumentano gli attacchi agli ATM: le soluzioni AXIS per le banche

a colloquio con Pietro Tonussi, business developer manager Southern Europe Bank Market
a cura della Redazione

Il denaro contante verrà ancora utilizzato nel 2020? Nonostante ci si trovi in un mondo sempre più tecnologico, in cui le transazioni economiche possono essere effettuate attraverso i nostri smartphone e una semplice connessione internet, oppure utilizzando le tradizionali carte di credito, di debito o altri sistemi elettronici, sentiamo ancora l'esigenza di pagare con il cash.

Le persone continueranno a utilizzare denaro contante per una serie di vantaggi (reali o percepiti), tra cui il fatto di credere di usufruire del sistema di pagamento più sicuro, perché non hanno bisogno di una connessione Internet (pensiamo a tutte le aree del mondo, ma anche dell'Italia, in cui si verifica il cosiddetto "digital divide", la differente possibilità di accesso al Web), perché possono effettuare pagamenti senza un intermediario, non ci sono costi di transazione ed è più facile tenere sotto controllo la propria disponibilità economica, o ancora perché è anonimo e non si corre il rischio di furti di identità. In sintesi, l'utilizzo del denaro contante viene percepito dalle persone come semplice, pratico, efficace, veloce e non costoso, tutti fattori che giustificano questi risultati e le stime sul suo utilizzo fino al 2020.

Questo comporta una serie di conseguenze che devono essere tenute in considerazione con sempre maggiore attenzione da chi si occupa di sicurezza nel settore delle banche e degli istituti finanziari. Innanzitutto la presenza di più sportelli ATM sul territorio, ma anche più luoghi per il loro posizionamento (anche in aree non convenzionali come i centri commerciali, aeroporti e stazioni). Questo significa più cash in circolo e di conseguenza maggior rischio non solo per il denaro stesso, ma anche per i clienti e per tutto quello che concerne il prelievo di contante dai bancomat.

Analizzando in maniera più approfondita questa situazione si evince come anche i criminali, sempre più esperti e senza particolari scrupoli, conoscano questa tendenza generale e si siano organizzati di conseguenza per mettere in atto i loro intenti nei confronti delle banche, delle singole filiali e soprattutto degli ATM, con tecnologie e azioni sempre più evolute che si concretizzano negli attacchi ai bancomat che rappresentano il bersaglio preferito.

Secondi i dati del Rapporto Intersettoriale sulla Criminalità predatoria di ABI-OSSIF, è infatti in crescita l'aumento complessivo dei reati predatori, come dimostra l'alto numero di denunce all'Autorità giudiziaria dei furti e delle rapine, rispettivamente +2,2% e +2,6% nel 2014 rispetto al 2013; l'altro dato importante è che **crescono di anno in anno gli attacchi agli ATM bancari**: solo nei primi 9 mesi del 2014 sono stati registrati 433 episodi rispetto ai 321 del 2013, pari a un **incremento del 34,9 %**. Questi atti criminosi **rappresentano inoltre circa l'80% degli attacchi totali**, a testimonianza di come gli ATM siano diventati il **primo obiettivo in assoluto dei malviventi**, in primis proprio per la loro funzione di erogatori di denaro contante.

Con riferimento alla tipologia di attacchi agli ATM,

questi possono essere divisi in due categorie principali: quelli "fisici", dove i criminali intervengono direttamente sul bancomat e quelli "software", come ad esempio il fishing, ovvero la frode telematica. Gli strumenti più utilizzati negli attacchi fisici sono i gas/esplosivi, le seghe a disco, la dinamite, i martelli e altri arnesi da scasso. Il "cash trapping" risulta il sistema preferito dai malviventi per rubare i soldi dal bancomat, perché è il più semplice da applicare e non richiede particolari conoscenze informatiche. Tra le modalità di attacco fisico più utilizzate ci sono indubbiamente quelli con gas e/o esplosivi, ma è lo skimming quello che spesso ha conseguenze più gravi per il malcapitato soggetto che subisce la truffa. Dobbiamo infine suddividere gli **ATM in due categorie a seconda della loro locazione**: *on-site*, vicino all'agenzia o in area self, normalmente il locale adiacente alla filiale, oppure *off –site*, quelli installati in centri commerciali, aeroporti, stazioni e simili, questi sono quelli chiaramente più soggetti a vandalismi di ogni genere.

"Di fronte a numeri di questo tipo e ai dati sugli attacchi che sono in aumento, bisogna tenere in considerazione anche l'impatto emotivo che viene provocato nel soggetto che subisce, ad esempio, una rapina mentre sta prelevando – aggiunge Pietro **Tonussi, Business Developer Manager Banking Southern Europe di Axis Communications** – *è fondamentale tutelare la sicurezza dell'individuo, rispettando nello stesso momento la sua privacy. Le telecamere quindi vanno viste come oggetti per la sicurezza e la salvaguardia dell'assett aziendale (il bancomat) ma anche e soprattutto di safety, vale a dire per assicurare efficienza e una migliore assistenza ai clienti.*

La videosorveglianza IP come soluzione

Le linee guida per arginare queste tipologie di attacchi sono fondamentalmente tre: l'utilizzo di sistemi di riprese (videosorveglianza), l'uso di controlli biometrici e la geolocalizzazione dei valori, vale a dire la possibilità che il bancomat o il deposito cash possa essere referenziato in modo geografico. Axis Communications, leader di settore della videosorveglianza IP, dispone nella propria gamma prodotti di telecamere di rete adatte ad affrontare questi tipi di attacchi e può essere davvero considerato il partner ideale per

gli istituti bancari nel garantire la sicurezza degli ATM. Tra le telecamere IP che possono apportare un notevole contributo al mondo bancario ci sono sia quelle per il controllo area, che fanno della qualità di immagine e della supervisione a 180° il loro punto di forza, sia quelle che si possono sistemare nei pressi o nel bancomat, come le *pinhole* dalle dimensioni super compatte, e dalle grandi prestazioni con video HDTV. I sistemi video di rete Axis, oltre ad una videosorveglianza di alta qualità, possono migliorare l'assistenza ai clienti (safety) e facilitare le varie attività ottimizzando i costi. Innanzitutto grazie alla sorveglianza di tutta l'area circostante lo sportello, con l'utilizzo di telecamere panoramiche a 360° che consentono di sorvegliare in modo completo e con l'ausilio di una sola telecamera l'area, eliminando gli angoli ciechi. Le telecamere HDTV con obiettivo pinhole, montate all'interno degli sportelli automatici, installate in modo appropriato, possono garantire un elevato dettaglio della scena interna all'ATM con immagini di eccezionale qualità, anche in ambienti con condizioni di illuminazione difficili, come in presenza di grandi finestre o ingressi con porte in vetro e pavimenti lucidi. In definitiva le prime telecamere, utili per il controllo d'area generano overview, mentre le seconde catturano i dettagli, realizzando un break-even ideale tra privacy e safety del cliente. Offrono inoltre il notevole vantaggio di poter essere integrate con sistemi di allarme e di controllo degli accessi, anche da remoto, per una piattaforma di sicurezza completa ed efficiente.

Secondo una survey del 2014 realizzata da **ATMIA**, associazione no-profit che si occupa di analizzare l'universo degli ATM a livello mondiale, risulta che **ci sia una presa di coscienza da parte dei manager responsabili della sicurezza bancaria sull'importanza delle soluzioni tecnologiche**, come la videosorveglianza IP, nell'affrontare il problema degli attacchi agli ATM. Apparentemente, l'inserire ulteriore tecnologia in impianti esistenti potrebbe essere percepito come un costo aggiuntivo, ma teniamo presente che, quando dei criminali attaccano un ATM, la banca affronta dei costi ben superiori che non sono solo quelli del bancomat danneggiato, ma possono essere anche i danni alla struttura del palazzo che la ospita, eventuali feriti tra i passanti o - nella peggio-

re delle ipotesi - delle vittime. "*Inoltre, non possiamo dimenticarci di altri fenomeni che spesso accadono all'atto del prelievo:*– continua **Tonussi di Axis Communications** – *Se un cliente subisce una rapina dopo aver prelevato a uno sportello bancomat, quella filiale non avrà un danno diretto, ma avrà perso un cliente che non si sentirà sicuro ad effettuare questa semplice operazione. L'impatto emotivo sul cliente potrà essere ancora più grave perché andrà ad influire a livello di "customer insatisfaction", elemento che nel futuro una banca dovrà tenere sempre più in considerazione per fornire un servizio all'altezza e per migliorare l'assistenza ai clienti (safety).*

Un altro scenario assai tipico è quello di un utente che si reca in un'area self e vuole prelevare del denaro contante: ci sono due possibili situazioni che possono provocare un danno diretto o indiretto alla banca. Partiamo dalla prima: il cliente può trovare all'interno dell'area self un senzatetto che ha scelto di dormire in questo luogo perché è un posto caldo, in grado di offrire riparo dalle intemperie esterne; il risultato sarà che il cliente non entrerà a prelevare perché non si sentirà al sicuro, creando così un danno indiretto alla banca. Immaginiamo ora che un soggetto entri nell'area self e si senta improvvisamente male, accasciandosi a terra: senza un adeguato sistema di videosorveglianza la banca non è in grado di assicurare la sicurezza del cliente nel modo migliore (danno diretto). Due situazioni diverse, che esemplificano come grazie ad algoritmi intelligenti che rilevano la presenza di un uomo a terra, in grado di riconoscere se un uomo è in posizione orizzontale perché sta dormendo oppure perché sta male, la banca abbia a portata di mano una soluzione utile a garantire la compresenza di safety & security. Una stessa analitica che le banche desiderano per limitare un possibile problema, che può verificarsi anche in altri ambienti oltre a quello delle aree self degli ATM. Le soluzioni Axis, grazie ad allarmi antimanomissione e alla funzionalità di rilevamento di oggetti, nonché ad applicazioni di partner di Axis come quella appena enunciata, permettono di identificare rapidamente anche potenziali attività di skimming e trapping di banconote e carte o altre attività criminose ai danni dei bancomat.

E quando si verificano attacchi con gas esplosivi o con altri attrezzi da scasso? Anche in questo caso la videosorveglianza IP può tornare utile alla banca. Pensiamo innanzitutto a cosa succede in questi casi e a quale sia il comportamento umano dei criminali che effettuano un attacco di questo tipo, per comprendere come la tecnologia possa risolvere questo problema. Sicuramente un criminale che deve far esplodere una cassaforte non avrà un atteggiamento tranquillo come potrebbe essere una persona che deve semplicemente prelevare. Le statistiche su questa tipologia di attacchi evidenziano inoltre che sono ancora due i gas più utilizzati dai malviventi: l'ossigeno e 'acetilene. Innanzitutto perché sono entrambi inodore e non vengono rilevati dai nasi elettronici. L'ossigeno, inoltre, viene scelto perché deflagra senza fuoco, preservando dalle fiamme le banconote, che altrimenti sarebbero inutilizzabili. Le statistiche evidenziano come gli attacchi fisici siano quelli più perpetrati ma, come abbiamo detto, è possibile **realizzare con le telecamere un'analisi comportamentale**, perché c'è sempre una certa concitazione in questi gesti, tipica di questi attacchi: l'analitica è appunto in grado di rilevare tali movimenti, offrendo così la possibilità di attivare delle azioni quasi immediate di fronte a un potenziale gesto criminale o segnalare un potenziale caso sospetto.

Sul piano degli attacchi fisici si dovrebbe in ogni caso ricorrere di più alla **deterrenza a scopi preventivi** che si può ottenere in due modi: con le telecamere sistemate nell'area esterna al bancomat, che possono scoraggiare i criminali nell'attuare determinate azioni, ma soprattutto con telecamere che possono essere utilizzate anche all'interno del bancomat per andare ad analizzare le scene che potrebbero essere sospette, ad esempio relative a persone che hanno effettuato uno o più sopralluoghi nei giorni precedenti all'attacco dell'ATM.

Infine, se analizziamo i dati sugli attacchi agli ATM forniti da OSSIF-ABI e ATMIA e visti i numeri di atti criminali perpetrati a danno delle banche, se ne desume che nonostante cresca la percezione dell'importanza di queste tecnologie nel prevenire e garantire la sicurezza degli ATM e delle filiali in generale, esse non sono ancora così utilizzate in maniera capillare. "Capisco che sia inevitabile dover fare dei confronti tra investimenti e contenimento dei costi, ma un terzo elemento deve essere preso in considerazione quando si prendono decisioni di questo genere, che è la sicurezza del cliente, che ogni giorno usufruisce dei servizi che la banca offre", conclude Tonussi.

Meno rapine in filiale, più furti agli ATM: anche così cambia la banca

a cura di Raffaello Juvara

Presentati da **ABI** a **Banche e Sicurezza 2015** - la due giorni di lavoro sui temi chiave della sicurezza in banca che si tenuta a Roma a Palazzo Altieri il 4 e 5 giugno – i dati su furti e rapine in banca, che attestano una storica inversione di tendenza: gli attacchi agli ATM hanno superato le rapine alle filiali.

Secondo quanto comunicato da **OSSIF**, il Centro di ricerca ABI in materia di sicurezza, nel 2014 sono state tentate **587** rapine a danno delle filiali bancarie, con una ulteriore diminuzione del **37,6%** rispetto all'anno precedente; paragonando il dato con quello del 2007, il calo supera addirittura l'80%. In netto calo anche il cosiddetto "indice di rischio", cioè il numero di rapine ogni 100 sportelli, passato da 3 a 1,9.

Sono questi i principali risultati del rapporto che ha

inoltre evidenziato che, secondo gli ultimi dati del Ministero dell'Interno, le rapine commesse ai danni delle dipendenze bancarie, rispetto al totale di quelle denunciate, sono passate dal **5,5%** del 2004 al **2%** del 2014.
Di converso, si sono registrati **661** attacchi agli ATM, con un aumento del **28,1%**. Il sorpasso nei confronti delle rapine è avvenuto anche a livello di bottino complessivo (**15,2 milioni** dalle rapine contro **16 milioni** dagli ATM) e di bottino medio (**25.855** euro dalle rapine contro **48.080** euro dagli ATM). Le rapine sono state portate a termine nel **74,2%** dei casi, mentre gli attacchi agli ATM sono riusciti al **50,4%**.
Questo, in estrema sintesi, il trend positivo che ha caratterizzato il fenomeno negli ultimi anni, determinato da molteplici fattori, fra i quali il lavoro congiunto di banche e Forze dell'Ordine e i continui investimenti del sistema per la sicurezza delle filiali, attestati da tempo attorno a 700 milioni di euro all'anno.
Il maggior numero di attacchi agli ATM rispetto alle rapine allo sportello è la conferma di una tendenza manifestata da tempo, che trova spiegazioni ben note agli addetti ai lavori: da un lato la diminuzione del contante allo sportello con sistemi di cassa sempre più efficaci; dall'altro, la relativa vulnerabilità fisica degli ATM attrae anche ladri improvvisati, peraltro con risultati negativi una volta su due (49,6%). Da evidenziare anche la diversa rilevanza penale del reato "rapina" rispetto al reato "furto", che esercita un sia pur residuale effetto deterrente.
Nell'ambito delle sessioni dedicate alla sicurezza fisica, **Antonella Trocino** di OSSIF ha descritto il cambiamento in corso nella rete delle filiali, partendo dal ridimensionamento della presenza sul territorio avvenuto dal 2008 al 2014: **3.400** sportelli chiusi, **17.900** dipendenti in meno e **1.909** ATM disinstallati.
Ha evidenziato Trocino: "*Il perimetro del sistema si è ristretto, ma è diventato più complesso. I POS sono aumentati del 25% e gli sportelli stanno cambiando fisionomia, diventando veri e propri "negozi" di merchandising o delle agenzie immobiliari, con esigenze diverse di lay-out e di sicurezza.*"
Il ridimensionamento della rete sul territorio negli ultimi sette anni è dunque stato di uno sportello su dieci, al quale è corrisposta una riduzione del 5% dei dipendenti e circa del 4% degli ATM.

TRASPORTO VALORI: LA RISPOSTA DELLE AZIENDE

Nel corso dell'edizione del 2014 di **Banche e Sicurezza**, l'argomento centrale era la preoccupazione suscitata nelle banche (e non solo) dagli episodi NES e Ipervigile avvenuti alla fine del 2013, che avevano messo in dubbio l'affidabilità del CIT nazionale. Preoccupazioni giustificate, determinate sia dall'entità degli ammanchi (circa 50 milioni di euro) che dagli interrogativi sulla capacita del sistema di evitare il ripetersi di episodi similari e di garantire la *business continuity* in caso di default.
Quest'anno è arrivata la risposta di **Mondialpol Group** e di **BASE – Gruppo Battistolli**, due tra i più importanti operatori italiani che, con modalità diverse, hanno fornito un riscontro concreto sulle misure adottate sia a livello di singola azienda che di sistema, per rassicurare i clienti.
Massimo Gasparotto, amministratore delegato di **Mondialpol Group,** ha sottolineato nel corso del suo intervento la concentrazione in corso tra le aziende, che sta configurando un comparto con pochi gruppi con capacità finanziarie adeguate per effettuare investimenti a livello industriale e garantire la continuità operativa in caso di disastri sistemici. A tale fine, il gruppo ha adottato importanti procedure di auditing e compliance, ed ha messo a punto il **Portale Knox** e il **Mondialpol Cash Service** con l'obiettivo di rendere più efficiente e trasparente per il cliente l'intero ciclo logistico del denaro. **BASE** ha invece affidato la risposta a **Guido Giorgetti** di **Banca MPS** che ha descritto le soluzioni che MPS sta sperimentando con il Gruppo Battistolli per la tracciabilità del contante, al fine di garantirne la reperibilità in ogni passaggio, dalla prelievo in agenzia al rifornimento dell'ATM remoto.

Le previsioni per l'immediato futuro non prevedono cambiamenti di direzione. Come ha commentato durante una pausa dei lavori un rappresentante sindacale che ha chiesto l'anonimato, "*la migliore fotografia di quello sta succedendo alla banche è l'accordo raggiunto tra le parti sociali per ridurre di altri 30.000 posti lavoro gli organici nei prossimi anni. È un accordo indolore per i dipendenti attuali, essendo basato sul pre-pensionamento dei più anziani, ma è devastante per i giovani. Significa che le banche non saranno più attive sul mercato del lavoro in futuro, con tutte le conseguenze sociali connesse".*

Il cambiamento in corso sta ovviamente comportando effetti rilevanti nella filiera dei fornitori di sicurezza del sistema bancario. A parte i dispositivi di sicurezza passiva, direttamente legati all'evoluzione del contante, la diffusione delle tecnologie in rete (videosorveglianza, controllo accessi, antintrusione e sistemi di gestione centralizzata) determina esigenze nuove fra le quali, in primis, l'interazione con la sicurezza logica, più volte richiamata nel corso di questa edizione di **Banche e Sicurezza.**

Come è stato sottolineato da **Claudio Ferioli** di Banca IntesaSanPaolo, a livello globale stanno avvenendo attacchi fisici per violare sistemi informatici e attacchi informatici per violare sistemi fisici. Si deve dunque parlare di evoluzione della sicurezza fisica o di quella logica? Una domanda di estrema rilevanza per l'intera catena di comando della sicurezza in banca, a partire dalle competenze richieste ai security manager.

Sarà certamente questo un tema non marginale, nel quadro complessivo dell'evoluzione del sistema bancario.

L'evoluzione del CIT secondo i protagonisti: la parola a Mondialpol

a colloquio con Massimo Gasparotto, amministratore delegato Mondialpol Group
a cura della Redazione

Il trasporto valori in Italia sta cambiando fisionomia, con una rapida riduzione del numero degli operatori e il contestuale aumento delle dimensioni di quelli rimanenti, che si propongono come partner dell'utenza (banche, Poste, GDO/retail) con caratteristiche strutturali e modalità operative molto diverse rispetto a un passato anche recente. Può descrivere questo cambiamento, dal punto di osservazione di uno dei maggiori operatori italiani?

Il termine cambiamento forse non è perfettamente evocativo di una sorta di "traversata", che peraltro non è certo conclusa. Di certo appropriato se pensiamo alle avvisaglie, risalenti ormai ad una decina di anni fa, che bisognava saper cogliere, senza mai perderne di vista l'evoluzione. Lo é decisamente meno se pensiamo alla frequenza e all'impatto degli eventi degli ultimi due-tre anni: eventi prevedibili, come l'emanazione di corposi dettati di legge, dei quali forse è stata fatta una valutazione riduttiva (quando non del tutto omessa); ma anche veri e propri *fulmini a ciel sereno* che hanno colpito il settore dall'interno, mettendone a dura prova la tenuta … I pilastri hanno retto, ma a caro prezzo.

Oltre all'evoluzione naturale del mercato, quali altri fattori hanno provocato questo cambiamento come, ad esempio, l'intervento delle autorità monetarie?

In un contesto solido, con tutte le parti in causa conscie ciascuna del comune interesse di mantenerlo tale, gli interventi delle autorità monetarie non possono che avere impatti sempre sostenibili, anche perché questi interventi non li ritroviamo serviti dalla sera alla mattina;

intendo dire, come ho un po' anticipato in precedenza, che c'è sempre stato il tempo di approfondire, valutare la portata degli interventi tempo per tempo *in itinere*.
Quindi, tra gli operatori del settore, possiamo sì dire che qualcuno non ha capito, o non ha voluto credere fino all'ultimo che il nostro mondo – un po' abituato a veleggiare senza grandi scossoni – stava invece entrando nella burrasca; ma la maggior parte – occorre rimarcarlo per amore di verità – proprio non ce l'ha fatta, oppure sta ancora soffrendo. Basti pensare alla remunerazione calante dei servizi – anche in termini semplicemente nominali – degli ultimi dieci anni, a fronte invece degli investimenti per la ricerca di innovazioni richieste dal mercato ma, ancor più, per gli aggiornamenti (o com-

plete sostituzioni) delle proprie dotazioni tecniche, necessari proprio per restarci, in quel mercato!

La moneta metallica rappresenta un problema a livello sistemico da quando è entrato in vigore l'euro. Quali soluzioni propone Mondialpol per migliorare l'efficienza del sistema e, dall'altro canto, per rispondere alla richieste dei clienti?
Giusta l'affermazione, e l'impatto è stato rilevante soprattutto sul nostro settore, quale snodo cruciale, punto nevralgico del sistema di circolazione della moneta metallica. Così gli aspetti critici si sono manifestati quasi repentinamente allorché un po' tutti si sono trovati a "fare i conti" – espressione quanto mai appropriata! – con la gestione di grandi quantitativi di moneta, non tanto e non solo in termini di volumi fisici, ma soprattutto di controvalore. Si sono dovute ricercare soluzioni per la clientela, per comprimere i tempi dell'immobilizzo finanziario di elevati stock, innalzando al contempo i controlli e i livelli di sicurezza fisica contro un rischio aumentato in modo più che proporzionale rispetto al diverso valore di un singolo pezzo prima espresso in lire… Banalizzando, "perdere" in qualche modo una moneta da due euro ha portato un danno prossimo allo stesso evento ma per un intero rotolo da cento lire.
Ancorché non immediato rispetto al manifestarsi graduale di queste evidenze critiche, siamo affermare di essere stati comunque solleciti nell'affrontare il problema "moneta" nel suo insieme, mettendo in campo tutte le risorse necessarie – non abbiamo certo lesinato sugli investimenti anche in nuove strutture, attrezzature e apparecchiature – per realizzare un'organizzazione *al top*: efficienza data da processi di lavorazione rispettosi delle regole ma fortemente industrializzati e mirati a lavorazioni di grandi volumi, logistica adeguata a favorire un altrettanto efficiente servizio di raccolta e di redistribuzione della moneta lavorata. Abbiamo quindi una rete capillare che copre ogni necessità della filiera: raccolta-lavorazione-stoccaggio/custodia-redistribuzione, dai quantitativi minimi della clientela *retail* a volumi per i quali possiamo "mettere in strada" i nostri automezzi pesanti adibiti allo scopo. In sintesi, possiamo affermare di poter garantire una vera e propria "logistica della moneta", imperniata su alcuni *hub* di ragguardevoli dimensioni e capacità di lavorazione.

Quali sono le dimensioni del gruppo Mondialpol e quali sono le proposte che fa all'utenza per assicurare la solidità dell'impresa e la business continuity?
La solidità delle aziende del Gruppo è un po' alla luce del sole, in altre parole è testimoniata dagli investimenti e dai bilanci. Per questi ultimi, infatti, c'è un trend positivo qualsiasi "posta" si voglia analizzare; non ultimo, nella seconda metà dello scorso anno sono stati fatti ri-

levanti aumenti di capitale, e non certo per "ricostituzione": la famiglia Mura crede nelle proprie imprese, nelle quali riversa risorse che le rendano quanto più solide possibile. E va sottolineato che ci sono state recenti acquisizioni di altri operatori così come l'insediamento in nuove aree: la clientela del Gruppo è costituita sempre più da *player* che operano in via estesa, fino all'intero territorio nazionale, per questi poter fare riferimento a pochi operatori – o, addirittura, ad uno solo quale può essere il nostro Gruppo – è certamente garanzia di efficienza interna e di economicità.

Ma abbiamo toccato con mano come un'organizzazione ottimale sul piano operativo e sostenuta da "conti in ordine", quale a buon diritto può ritenersi il nostro Gruppo, possa doversi misurare in modo repentino con situazioni critiche, non importa se solo minacciate o già manifeste. Ci siamo resi conto della necessità di incrementare ulteriormente un già oggettivo profilo di professionalità e di affidabilità del Gruppo, e con questo obiettivo, a inizio dello scorso anno, abbiamo intrapreso con il Gruppo Fidelitas un percorso comune, che ha dato come primo risultato la costituzione della Rete d'Impresa Fidelitas – Mondialpol, denominata "Continuità Valori", formula che da sola evoca sufficientemente gli scopi.

Ci può descrivere il portale Knox e quali sono i criteri con i quali viene garantita la sicurezza da attacchi informatici?

Progettato e gestito dalla partecipata Adam, Knox costituisce ormai un riferimento per il sistema; è questa, infatti, la piattaforma attraverso la quale il Gruppo Mondialpol "dialoga" con le controparti – clientela e rete di Istituti di Vigilanza – consentendo di accedere in tempo reale, via WEB, a tutte le informazioni necessarie allo svolgimento e al puntuale controllo dei servizi. Ma Knox non è strumento di mera "amministrazione", ma consente altresì all'utenza di centralizzare e di organizzare tutte le informazioni, usufruendo di strumenti di controllo e di calcolo in modo flessibile e immediato e poter così effettuare analisi dei dati nel breve e nel lungo periodo, fino ad ottimizzare il rapporto immobilizzo del denaro / costo dei trasporti, visualizzando anche in modo grafico gli andamenti di giacenza e proponendo i momenti più opportuni per effettuare prelievi / versamenti in Banca d'Italia. Va da sé che dati e informazioni di questo genere esigono una vera e propria "blindatura", tante e altamente critiche sono le minacce. I presidi e le protezioni di sicurezza informatica sono conseguenti, per tipologia e livello di protezione, e prevedono diversi livelli di accesso, da quelli più semplici alle Strong Autentication con certificati digitali su Web Key Flash-Rom per assegnare i permessi di operatività ed i profili d'accesso. La riservatezza e l'integrità delle comunicazioni client-server è garantita dall'utilizzo di estensioni SSL (Secure Socket Layer) a 128 bit. Ulteriori garanzie sono costituite da sistemi di controllo antihackering, server di base dati e di pubblicazione con back-up a caldo, soluzioni di business continuity e di disaster recovery.

Come evolverà l'offerta del CIT nei prossimi anni, a fronte di una tendenza a livello internazionale di riduzione del contante in circolo?

È vero che sussiste, a livello internazionale, una tendenza abbastanza diffusa alla riduzione dell'uso del contante, ma è altrettanto vero che in Italia si mantengono "ottimi rapporti" tra i cittadini e il contante, almeno a giudicare dalle statistiche periodiche di Banca d'Italia, dalle quali è difficile cogliere segnali significativi di un rapido allineamento del nostro paese a quella tendenza. Riteniamo quindi che l'evoluzione del settore, nel medio periodo, non sarà condizionata in modo determinante dalla possibile "disaffezione" all'uso del contante ma, più verosimilmente, saranno ineludibili esigenze di efficientamento a tracciare il percorso. È così possibile ipotizzare cambiamenti, pur graduali, nel ciclo di raccolta e, ancor più in quello di distribuzione del denaro, accorciando un po' la catena; quindi, più che la *war on cash* – dichiarata ormai una decina di anni fa – riteniamo ci si debba dedicare sin d'ora a combattere l'inefficienza. Già nell'area euro sono presenti diversi modelli di organizzazione di questa catena, ognuno condizionato da precisi fattori e per questo non perfettamente replicabili in un paese diverso. Ed è innegabile che vi sia, a livello di Eurosistema, una spinta verso la convergenza dei servizi che riguardano il contante a livello di Banche Centrali, che potrebbe portare anche l'Italia a percorrere in modo più deciso la strada di "industrializzazione" dei processi del contante, che necessariamente dovrà passare attraverso gli operatori più solidi, con possibilità di cospicui investimenti e, soprattutto, con un'organizzazione adeguata. Una prospettiva, quindi, di più marcata concentrazione su un ridotto numero di *player*, il Gruppo Mondialpol sta già giocando questa importante partita.

Vigilanza e dintorni

Appalti pubblici, prezzi criminogeni: un nodo da tagliare

di GpG – Gossip Particolare Giurato

Secondo alcune ricerche, agli istituti di vigilanza derivano dagli appalti pubblici circa 600 milioni di euro di fatturato - pari al 20% del totale- a fronte dell'impiego di un terzo della manodopera complessiva, circa 15.000 guardie giurate. La differenza di proporzione deriva dalla preponderanza di piantonamenti fissi richiesti dalle stazioni appaltanti pubbliche, i servizi a minor valore aggiunto svolti dagli istituti. La distribuzione sul territorio nazionale non è omogenea, con le maggiori concentrazioni nei capoluoghi di regione e la punta massima a Roma, dove si stima siano oltre 5000 le guardie giurate impegnate per i servizi di sicurezza presso le diverse entità pubbliche italiane e straniere presenti nella capitale

La dimensioni economiche, le caratteristiche peculiari dei rapporti con le PA e, non per ultimo, alcune presenze non del tutto commendevoli tra gli imprenditori del settore (forse attirati proprio dai primi due fattori) hanno richiamato l'attenzione di diverse istituzioni di controllo, fra le quali anche l'**ANAC**, l'Autorità Nazionale Anti Corruzione guidata da **Raffaele Cantone**.

Il problema si è paradossalmente accentuato da quando la Corte di Giustizia Europea ha messo al bando le tariffe minime (2007). La conseguente possibilità di assegnare le gare al massimo ribasso da parte delle stazioni appaltanti pubbliche ha distrutto non solo i legittimi margini di redditività aziendale ma anche, ed è l'aspetto più grave, la possibilità di coprire i costi obbligati per realizzare con regolarità il servizio oggetto dell'appalto.

Retribuzioni, oneri sociali e fiscali, formazione, equipaggiamento, organizzazione: se la somma di queste voci è pari a 100 - magari con la certificazione di adeguati organismi di controllo - qualsiasi punto percentuale in meno determina un corrispondente mancato adempimento. Non è un'opinione, è matematica.

È dunque evidente che la legittima concorrenza si determini da 100 in su, potendosi esercitare la libertà d'impresa sui margini di utile. Da 100 in giù può diventare, a scelta: evasione fiscale, omissione contributiva, sfruttamento della manodopera, mancato rispetto dei regolamenti questurili, truffa nell'esecuzione dell'appalto, riciclaggio e, come l'ANAC intende verificare, anche corruzione e concussione. Le stesse banche, fierissime sostenitrici della libertà di mercato quando erano il principale macro-cliente degli istituti di vigilanza, hanno avuto modo di sperimentare anche di recente la rischiosità delle assegnazioni al massimo ribasso, dovendo ringraziare i propri santi protettori se, in qualche caso limite, hanno perso "solo" del denaro e non anche la reputazione o altro…

Sicurezza sussidiaria, importanti novità al convegno ANIVP

a cura della Redazione

"SICUREZZA SUSSIDIARIA E INFRASTRUTTURE CRITICHE - IL RUOLO DELLA VIGILANZA PRIVATA": questo il titolo del convegno organizzato da ANIVP il 19 maggio a Roma, che si è svolto davanti a un folto gruppo di operatori del settore, rappresentanti delle istituzioni e security manager di importanti utenti.

Il dottor Vincenzo Acunzo del Ministero dell'Interno ha spiegato le novità normative di riferimento per il settore, ricordando che le recenti modifiche al DM 269/2010 portano una nuova impostazione nel calcolo delle cauzioni e normalizzano il capitale sociale ai termini previsti dal Codici Civile, in un quadro di adeguamento complessivo che rende il decreto più attuale e applicabile. In merito alla certificazione da parte di Organismi indipendenti, è stato evidenziato che, allo stato attuale, sono ancora pochi gli OdC che hanno ottenuto l'accreditamento dal Ministero. È possibile che venga quindi presa in esame un'eventuale proroga dei termini previsti per l'adeguamento da parte degli istituti di vigilanza, attualmente comunque non in calendario. Per il Disciplinare per la formazione degli addetti ai servizi di sicurezza sussidiaria, sono state fornite ampie rassicurazioni sulla gestione della fase transitoria ma, nel contempo, è stata evidenziata l'importanza della formazione come fattore discriminante per l'impiego degli operatori in relazione al servizio richiesto. La successiva tavola rotonda è stata anticipata da un intervento di Mauro Bussoni, segretario generale di Confesercenti, che ha sottolineato l'importanza della sicurezza per la categoria dei negozianti e, di conseguenza, l'attenzione della Confederazione per la vigilanza privata. Il presidente AIIC Gregorio D'Agostino, il rappresentante di ANCI Antonio Ragonesi e il direttore di ICIM Paolo Gianoglio hanno affrontato i temi molto articolati della definizione di Infrastruttura Critica, delle esigenze di sicurezza rivolte in modo particolare al fattore umano, della città vista come paradigma di IC e del contributo offerto dagli Organismi di Certificazione indipendenti per assicurare il livello qualitativo dell'intera filiera della sicurezza partecipata. Con il rappresentante di ANCI è stato dibattuto il tema dei permessi di accesso alle ZTL per i mezzi di servizio degli istituti di vigilanza in modo uniforme sul territorio nazionale.

Presente e futuro dei servizi di sicurezza al convegno dell'EBiVeV

a colloquio con Cesarina Giani, presidente Ente Bilaterale Veneto per la Vigilanza
a cura della Redazione

L'**Ente Bilaterale Veneto per la Vigilanza (EBiVeV)** - emanazione a livello regionale dell'**Ente Bilaterale Nazionale per la Vigilanza Privata**, un organismo che unisce pariteticamente le associazioni che rappresentano gli istituti di vigilanza e le organizzazioni sindacali dei lavoratori firmatarie del Contratto Collettivo Nazionale di Lavoro per la categoria della vigilanza privata – ha organizzato un convegno dal titolo "**La vigilanza privata tra nuove esigenze e nuove opportunità" (24 giugno - Hotel Laguna Palace – Mestre Venezia) per fare il punto della situazione del complesso dei servizi di sicurezza, assieme ai rappresentanti delle Istituzioni di riferimento, dell'utenza e delle altre categorie di operatori, come le agenzie di investigazione e e società multiservizi.** È un momento importante per il settore della sicurezza privata in Italia: da un lato il comparto tecnologico (videosorveglianza, sistemi anti intrusione, controllo accessi) segna un +5%, a rimorchio della crescente domanda di sicurezza da parte dei cittadini; dall'altro il comparto della vigilanza privata tocca invece picchi di cassa integrazione inusitati, sotto la duplice pressione della crisi economica generale e della concorrenza "spuria" da parte di operatori non soggetti a normative (portierato e assimilabili). **Cesarina Giani,** presidente pro-tempore dell'EBiVeV, riassume in un'intervista a **essecome** i temi affrontati, in particolare sui problemi attuali e sulle prospettive future di un settore che, solo nel Veneto, conta oltre **3000 guardie giurate** ripartite tra circa **30 istituti di vigilanza**, con un fatturato stimato in **180 milioni di euro**.

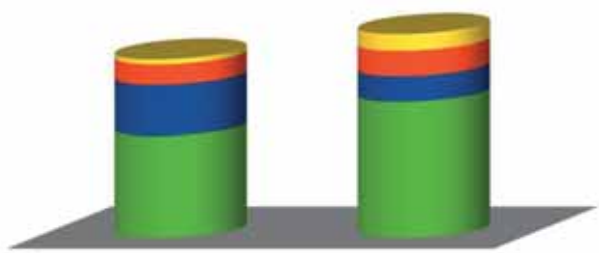
Signora Giani, qual è la situazione attuale del settore della vigilanza privata nel Veneto?
È una situazione molto critica per diversi motivi. Innanzitutto, la crisi economica degli ultimi sette anni ha colpito duramente anche gli istituti di vigilanza. Chiusura di aziende clienti, tagli delle spese per la sicurezza, difficoltà a recuperare i crediti, sono i tra motivi che hanno portato nel 2014 il Veneto ai primi posti nella classifica per regioni nel ricorso alla Cassa Integrazione Straordinaria e nelle domande di mobilità e disoccupazione. Inoltre, la concorrenza a volte spregiudicata da parte dei cosiddetti servizi di portierato ha sottratto moltissimi posti di lavoro agli istituti di vigilanza, sfruttando la mancanza di normative precise e la scarsa conoscenza della materia da parte dei clienti

che, pur di risparmiare, utilizzano personale privo delle qualifiche necessarie.
Infine, le nuove norme per gli istituti di vigilanza – mi riferisco al DM 269 del 2010 e al DM 115 del 2014 – che hanno introdotto migliorie indiscutibili a una norma che era diventata obsoleta, non riescono ancora ad essere pienamente applicate, penalizzando in tal modo le aziende che sono state più sollecite ad adeguarsi.

Ci può spiegare meglio questo problema, in particolare per quanto riguarda il rapporto con i clienti?
Le leggi italiane stabiliscono che i servizi di vigilanza per la prevenzione dei reati contro i beni (non le persone) vengano effettuati solamente da "guardie giurate", che diventano tali se possiedono i requisiti previsti dalla legge, se sono regolarmente assunte da soggetti appositamente autorizzati in quanto sono, a loro volta, in possesso di requisiti obbligatori (gli istituti di vigilanza), e se hanno ricevuto la formazione professionale prevista per le mansioni alle quali vengono impiegate. Al contrario, i cosiddetti "portieri", una definizione impropriamente derivata dai custodi degli stabili, sono operatori ai quali dovrebbero venire affidati solamente servizi di accoglienza e assistenza al pubblico, con addestramento specialistico (primo soccorso, antincendio ecc). Essendo mansioni che, in molti casi, sono prive di normative cogenti, questi lavoratori sono spesso impiegati senza adeguati contratti di lavoro e, quello che è peggio, vengono di sovente utilizzati per fare servizi di vigilanza a tutti gli effetti. I costi possono diminuire anche della metà, ma è evidente che si tratta di qualcosa di profondamente diverso rispetto alle guardie giurate, in particolare per quanto riguarda i criteri di selezione all'atto dell'assunzione, la formazione e le competenze operative. I clienti dovrebbero essere informati di questi aspetti, anche per assumere consapevolmente delle responsabilità ai fini, per esempio, della 231.

Dal suo punto di vista, cosa si dovrebbe o potrebbe fare per tutelare le parti coinvolte: aziende, lavoratori, clienti e istituzioni?
Innanzitutto, l'art. 134 del TULPS dovrebbe disciplinare anche i servizi di sicurezza alla persona e tutti i servizi cosiddetti "fiduciari". In altre parole, dovrebbe ricomprendere l'intera sfera dei servizi di sicurezza, chiarendo bene "chi può fare cosa". Poi, la definizione dei percorsi formativi per le guardie giurate, ma anche per le altre categorie di operatori, potrebbe consentire la determinazione di costi minimi incomprimibili, al di sotto dei quali non è possibile scendere. A tale riguardo, l'Ente Bilaterale può svolgere un'importante funzione di elaborazione dei dati e di supporto dei controlli da parte degli organismi preposti. Infine, i servizi di vigilanza, in particolare quelli definiti di "sicurezza sussidiaria" perché rivolti a obiettivi sensibili come le stazioni ferroviarie, i porti, i tribunali, non dovrebbero venir assegnati con il criterio del "massimo ribasso", innanzitutto per tutelare i cittadini utenti finali di quei servizi.

SERVIZI DI VIGILANZA ➡ SERVIZI DI SICUREZZA



	STIMA 2015	STIMA 2020
Sicurezza sussidiaria	3.000	10.000
Vigilanza, ispezioni, scorte	12.000	15.000
Piantonamenti armati	30.000	15.000
Servizi fiduciari	60.000	80.000
TOTALE	**105.000**	**120.000**

essecome
securindex.com

La tripla A della sicurezza in aeroporto: Axitea, Anteo e A-ICE

a cura della Redazione

Axitea, leader in Italia nel settore della sicurezza integrata, ha ospitato i principali player del mercato a livello nazionale e internazionale del settore per la presentazione di un approccio innovativo per la gestione integrata della sicurezza delle operazioni in ambito aeroportuale.

Ogni giorno in Italia decollano o atterrano circa 2.000 aerei e 300 mila passeggeri. Nel mondo, sono 7 milioni i passeggeri che transitano quotidianamente negli aeroporti, per un totale di 3,5 miliardi di persone ogni anno a livello internazionale (fonti: Enac, IATA 2014). Numeri significativi che mostrano la complessità del settore, che sempre più necessita di controllo e gestione del rischio, ma anche di cultura della prevenzione.

È in questa ottica che è stata ideata la piattaforma **SAMS** (Situational Awareness and Management System), sviluppata da **Anteo Worldwide**, multinazionale israeliana specializzata nella fornitura di software per la correlazione, l'analisi e la gestione delle informazioni critiche per le operation aeroportuali. Si tratta di una piattaforma software che mette insieme e integra tutte le soluzioni attraverso un duplice approccio: fisico e cyber. SAMS consente, quindi, di misurare e controllare in modo integrato l'intera filiera operativa di uno scalo con una elevata capacità di risposta, fornendo specifiche procedure di sicurezza a seconda degli eventi, garantendo elevate prestazioni, un alto livello di automazione e un aumento della produttività.

L'iniziativa è stata organizzata da Axitea in collaborazione con Anteo Worldwide, **A-ICE**, società italiana leader nelle soluzioni software per il mondo dell'aviazione, e **Appsento**, azienda svizzera specializzata nei Wireless Sensor Network (WSN). La collaborazione con queste società rafforza l'ecosistema di partnership sviluppato da Axitea.

Ha aperto i lavori – coordinati dal moderatore Andrea Marco Borsetti, Direttore di Appsento – il CEO di Axitea, **Marco Bavazzano**. A seguire, **Andrea Rigoni**, Partner & Chairman di Intellium LTD, ha illustrato l'importanza di una forte integrazione tecnica e organizzativa alla protezione delle infrastrutture critiche, come quelle aeroportuali, anche in termini di cyber security, ponendo l'accendo sulla necessità di strumenti evoluti in grado di processare dati provenienti da fonti diverse in ambienti complessi, nei quali la "continuità operativa" rappresenta un fattore potenzialmente critico.

Maurizio Tondi, VP Strategy & Operations Governance di Axitea, ha sottolineato: "L'aeroporto deve essere considerato e trattato come una smart city, un luogo vitale con una serie di vulnerabilità che necessita quindi di essere governato attraverso un sistema integrato. Di qui l'idea – continua Tondi – di dare vita a questo gruppo di lavoro/partnership tra Axitea, Anteo e A-ICE che consente di mettere a regime le rispettive competenze nell'ambito della security, creando a livello pratico un approccio integrato".

Claudio Ferrari, CEO di A-ICE, ha infatti rilevato come: "Oggi la gestione operativa all'interno degli

aeroporti si basa su un approccio multi-compartimentale che presenta una serie di criticità in termini di costi ed efficienza, cui si aggiunge la mancanza di una copertura dei servizi 24 ore su 24. È fondamentale dunque – ha concluso Ferrari – creare una collaborazione tra tutti gli enti coinvolti che operano a vario titolo in un aeroporto".

La soluzione all'approccio gestionale delineato da Axitea e A-ICE è stata presentata da **Israel Livnat,** Chairman & Founder di Anteo Worldwide, proprio attraverso la piattaforma SAMS: "Da un punto di vista operativo, questa piattaforma permette, per prima, l'integrazione di dati provenienti da differenti data source siano essi sensori, esseri umani e/o computer. Il grande valore espresso dalla soluzione sta nel rendere computabili dalla logica delle procedure operative tutte queste informazioni anche quando non nascono digitali".

Il workshop è poi proseguito con una visita presso il Padiglione di Israele ad Expo 2015.

Axitea è la società leader in Italia nel settore della sicurezza, specializzata nello sviluppo di soluzioni integrate e personalizzate. Con oltre 1.500 dipendenti, Axitea offre servizi per la sicurezza di aziende, attività commerciali, istituzioni, residenze private, mezzi e beni mobili. L'offerta prevede l'integrazione di tecnologie innovative personalizzabili, la capacità di progettazione, di gestione delle infrastrutture e sistemi e un portfolio completo di servizi di sicurezza e di vigilanza. L'azienda è presente su tutto il territorio nazionale, grazie alle proprie filiali, alle Centrali Operative e alla rete degli Axitea Partner, società affidabili, accuratamente selezionate e certificate. Circa 35.000 clienti in tutta Italia hanno già scelto Axitea per la loro sicurezza.

CONTATTI

AXITEA
Serena Olivieri
marketing@axitea.it
www.axitea.it

La svolta di IVRI, il più grande operatore di sicurezza in Italia

a colloquio con l'avv. Rosario Basile, presidente di IVRI spa
a cura di Raffaello Juvara

Ad un anno dall'acquisizione di IVRI, il Presidente, l'avvocato **Rosario Basile**, fa il punto della situazione, in un'intervista concessa a **essecome**, sulla più importante compra-vendita mai realizzata nella storia della vigilanza privata italiana.

Un'operazione dalla quale è nato il maggior operatore nazionale, con 40 sedi e 27 centrali operative distribuite sul territorio nazionale, 70.000 clienti, 7200 addetti.

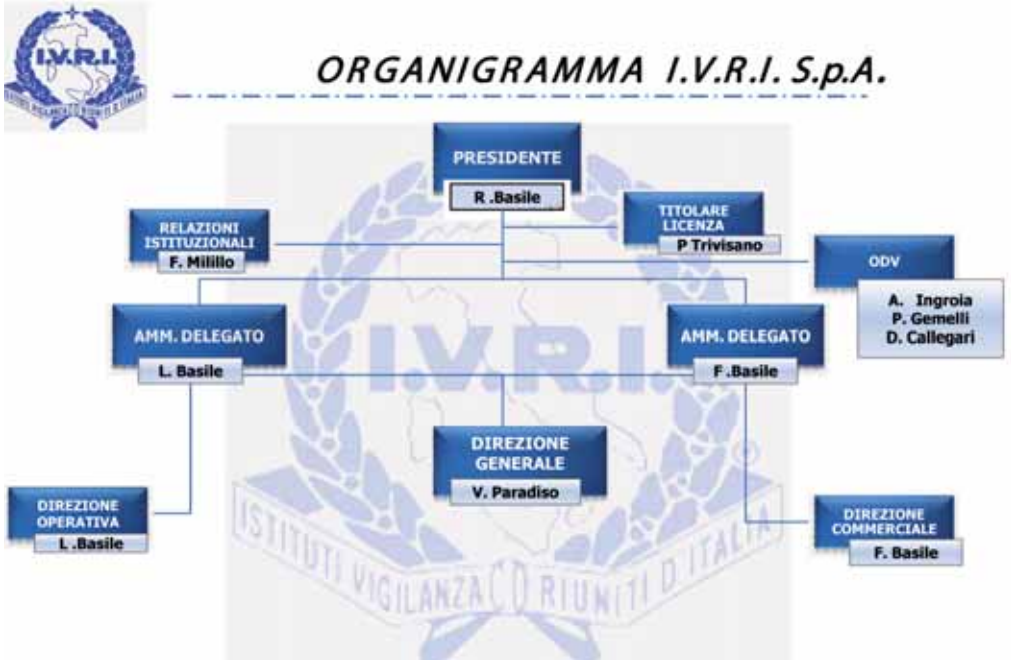
Oltre alle dimensioni del nuovo soggetto e agli effetti che ha determinato nei rapporti di forza nel mercato, l'operazione verrà ricordata anche per l'uscita di scena di 21 Investimenti, che nel 2006 aveva acquistato il gruppo IVRI direttamente dalla famiglia Zanè, con l'intento di traghettarlo verso un modello aziendale più simile a quelli internazionali, meno "padronale" e più "manageriale" e con la prospettiva di un'eventuale quotazione in Borsa.

Negli anni successivi, tutto il settore ha risentito pesantemente della crisi globale iniziata nel 2008 e le aziende più indebitate, come quelle acquistate dai fondi, non hanno potuto attivare la leva finanziaria, diventata impraticabile per imprese ad alta intensità di manodopera come gli istituti di vigilanza.

Dopo sette difficili anni, 21 Investimenti ha dovuto infine azzerare la partecipazione costata svariate decine di milioni di euro, passando la mano a una delle più antiche e blasonate dinastie della vigilanza italiana, la famiglia Basile. Un passaggio apparso quasi una nemesi, considerando i rapporti di collaborazione storicamente intercorsi tra le famiglie Basile e Zanè, quando quest'ultima possedeva IVRI.

Dopo il deal, l'avvocato Rosario si è letteralmente rimboccato le maniche assieme ai figli Luciano e Filippo, assumendo direttamente la conduzione del processo di riorganizzazione del gruppo milanese e del suo consolidamento con le aziende di famiglia KSM e Sicurtransport.

Come viene spiegato nell'intervista, questa formidabile sfida imprenditoriale e finanziaria è stata affrontata avendo ben presente anche la responsabilità derivante dal ritrovarsi a capo della più importante azienda italiana della sicurezza privata, operante in ogni comparto di un settore particolarmente delicato. Una responsabilità anche morale, che ha stimolato delle risposte decisamente sorprendenti per un ambiente storicamente poco sensibile al tema come la vigilanza. La costituzione di un organo di controllo interno a presidio dell'etica comportamentale del gruppo, in particolare negli appalti, con la partecipazione dell'ex-magistrato Antonino Ingroia e l'affidamento della gestione dei rapporti istituzionali al generale Giuseppe Fausto Milillo sono la rappresentazione concreta di questa sensibilità.



Avvocato Basile, come si presenta la situazione di IVRI ad un anno dall'acquisto da parte del gruppo KSM/Sicurtransport?

Fin dal primo momento abbiamo dedicato tutti i nostri sforzi per comprendere il modello organizzativo preesistente dell'azienda e sviluppare un piano di interventi finalizzato ad armonizzare la nuova realtà con il gruppo KSM/Sicurtansport, avendo ben chiaro che da questa unione stavamo facendo nascere il più importante player nazionale del settore.

Abbiamo inserito innanzitutto un nuovo management, con il compito di riconfigurare il modello di business partendo dalla razionalizzazione delle strutture presenti sul territorio, dall'accorpamento delle società controllate per snellire l'organigramma del gruppo, e dalla ridefinizione degli obiettivi strategici.

Oggi la vigilanza privata deve essere all'avanguardia nell'uso delle tecnologie per dare servizi a valore aggiunto agli utenti, e nella qualificazione degli operatori di ogni livello, che determinano la qualità del servizio offerto all'utente finale. Questi sono i capisaldi strategici del nostro gruppo che, per di più, è caratterizzato da una presenza globale sul territorio nazionale che lo rende interlocutore privilegiato per i grandi clienti di ogni categoria con elevate esigenze di sicurezza.

Le nostre capacità operative ci danno un grande vantaggio competitivo: oltre all'estensione territoriale, siamo leader in tutti i segmenti – dal trasporto valori ai servizi di sicurezza sussidiaria, dalle applicazioni tecnologiche ai servizi fiduciari - e garantiamo la formazione delle nostre persone al massimo livello per tutti i servizi prestati. Per rispondere completamente alla domanda, posso affermare che siamo molto soddisfatti del lavoro compiuto in questo primo anno di attività e già stiamo cominciando a raccogliere i frutti dell'intenso sforzo che abbiamo profuso e che continueremo a produrre.

IVRI fa parte del raggruppamento di imprese che garantisce i servizi di sicurezza all'EXPO. Cosa significa per voi la partecipazione a un evento di questa entità?

EXPO è una straordinaria opportunità per mettere in evidenza il nostro modello organizzativo e per dimostrare il livello di professionalità del nostro personale. Abbiamo formato gruppi di guardie con competenze superiori a quelle già molto elevate richieste per operare in aeroporto, avvalendoci di istruttori israeliani e, per questo motivo, oltre ai servizi facenti parte dell'appalto diretto di EXPO, ci siamo aggiudicati i servizi di sicurezza all'interno dei padiglioni di numerosi paesi con elevate esigenze di sicurezza, tra i quali Israele, Stati Uniti, Brasile e Messico. Sono molti gli aspetti per i quali EXPO è per noi una vetrina, anche per servizi non necessariamente riferiti all'evento o alla sua area fisica, ma che rappre-

sentano nostri precisi target operativi. Mi riferisco, ad esempio, alla sicurezza informatica e ad attività di intelligence che rientrano tra quelle di pertinenza degli operatori privati.

Come coniugate la vostra vocazione di leader a livello nazionale con i problemi di etica e di immagine che, anche in tempi recenti, hanno coinvolto operatori di primo piano del settore?
Questo è per noi un tema di fondamentale importanza, al quale rivolgiamo il massimo impegno possibile. Un'azienda con le nostre caratteristiche e le nostre dimensioni deve poter svolgere un ruolo di guida anche sul piano etico, in un settore troppo esposto a presenze e comportamenti inaccettabili. Per questo motivo, abbiamo preso un'iniziativa fuori dagli schemi, costituendo un comitato di garanzia con tre persone di altissimo livello morale professionale, fra i quali l'ex-magistrato Antonino Ingroia, con il compito di vigilare sulla correttezza dei comportamenti dei nostri manager in ogni manifestazione dell'attività societaria ma, in particolare, sulla gestione degli appalti. Ai garanti si affianca il generale dei Carabinieri, gen. Giuseppe Fausto Milillo, al quale abbiamo affidato le relazioni istituzionali, un altro capitolo di estrema delicatezza sul piano etico.

Per effetto dell'unione tra aziende che avevano seguito percorsi diversi nello scenario rappresentativo del settore, oggi il gruppo è presente in più associazioni che non sempre tengono comportamenti convergenti. Qual è la vostra posizione in merito?
Nelle diverse associazioni in cui è presente, il gruppo svolge solamente un ruolo da associato, sia pure di rilevanti dimensioni. Come tale, chiede agli organismi associativi di rappresentare correttamente le istanze più importanti per la categoria. In questo momento, l'applicazione della legge sugli appalti al settore della vigilanza è una priorità, in parallelo alla definizione degli aspetti legati al prezzo dei servizi. Sono temi sui quali siamo certi che tutte le associazioni debbano convergere, essendo di interesse per tutti gli operatori del settore.

Quali sono i vostri obiettivi per il futuro?
Intendiamo innanzitutto consolidare la posizione di global player della sicurezza sul mercato nazionale, proponendoci come interlocutori di riferimento per tutte le categorie di utenti ma, innanzitutto per i grandi clienti con una presenza estesa. Abbiamo inoltre programmi di espansione all'estero, per dare una dimensione internazionale al gruppo in un mercato sempre più globale ma intendiamo impegnarci anche per il rilancio dell'immagine della categoria, che negli anni passati è stata compromessa da comportamenti non consoni al ruolo e alla storia delle guardie giurate e degli istituti di vigilanza.

IFSEC International, una “tre giorni” di eccellenza industriale

comunicato stampa – traduzione a cura della Redazione

IFSEC International ha chiuso i battenti a giugno dopo tre giornate molto intense al Centro ExCel di Londra. Il più grande evento europeo annuale della sicurezza ha richiamato ancora una volta nella capitale britannica le ultime novità tecnologiche e dei servizi del settore, con svariate sessioni di approfondimento con la guida di esperti e la tradizionale attività di networking.

Un punto culminante dell’edizione di quest’anno è stata la nuovissima proposta delle Inspirational Speaker Series, che ha visto la baronessa Karren Brady, sir Ranulph Fiennes e sir Chris Hoy salire sul palco per tenere discorsi pieni di consigli utili e aneddoti stimolanti ricavati dalle loro illustri carriere. Con un argomento da approfondire ogni giorno, ogni oratore si è rivolto a una folta platea, con molti spettatori che hanno avuto la possibilità di porre direttamente delle domande nelle sessioni Q & A che sono seguite.

Un’altra novità per IFSEC International 2015 è stata la Benchmark Innovation Arena, dove sono stati accolti gli oltre 40 finalisti del premio annuale, offrendo a ognuno una presentazione per punti di 10 minuti, includendo operatori come Bosch Security, Vidicore, UTC Fire & Security e Secure Logiq, solo per citarne alcuni; tutti hanno fatto una breve presentazione dei loro prodotti e poi hanno lasciato il campo alle domande. Questo nuovo ed entusiasmante format ha dato modo ai visitatori di IFSEC International di esaminare nel dettaglio le novità presentate, fornendo un beneficio reale agli utenti finali, agli integratori e agli installatori.

C’erano davvero tante novità e curiosità, come quelle

powered by intersec

ТБ FORUM®

Security and Safety Technologies

09-11. 02.2016

CROCUS EXPO
MOSCOW I RUSSIA

Your Access to Key Decision Makers of $2.8 Billion Market

Groteck Business Media

www.tbforum.ru

portate da NICE Systems e Safran, per segnalare un paio di nuovi prodotti interessanti. NICE ha presentato Suspect Search Software, un brevetto in attesa di essere premiato che utilizza gli ultimissimi sviluppi di analisi video non soltanto per individuare in pochi istanti una persona in una vasta area, ma anche per ricostruire come vi è arrivata.
Safran ha presentato il sistema biometrico MorphoWave, in grado di raccogliere da una a quattro impronte digitali completamente senza contatto, fornendo tutti i dettagli per l'identificazione. Il nuovo dispositivo può venire impiegato per riconoscere più di diecimila persone, garantendo un elevato livello di precisione.
Ci sono stati anche molti approfondimenti messi a disposizione da relatori esperti provenienti dal mondo della sicurezza e dell'anti-incendio. Il futurologo Simon Moores ha richiamato un folto pubblico quando ha presentato mercoledì 17 la sua sessione su 'Safe, Smart and Connected Cities', esaminando i trend e le tecnologie emergenti, e l'impatto di Big Data e dell'Internet of Things. Tra le relazioni interessanti c'era quella di Paul Adams, il direttore delle strategie marketing EMEA di Alcatel Lucent, che ha tenuto una sessione su 'Evoluzione della Sicurezza Pubblica con le Tecnologie Intelligenti e le Infrastrutture Sicure', e quella di Richard Berkeley che ha analizzato come i disordini del 2011 (*in Inghilterra ndr)* abbiano cambiato le modalità delle prove televisive.
Ulteriori spunti di interesse dalla parte espositiva comprendevano numerosi lanci di alto profilo da parte di alcuni dei principali nomi dell'industria, come Immer Vision con il primo obiettivo al mondo a 360° a 6k, la nuova telecamera ad alta definizione di Avigilon a 7k, la rivoluzionaria gamma domotica di Comelit, e il Laser Guardian, l'innovativo scanner a raggi laser di SICK. Capita Technology Solutions ha lanciato il servizio Capita Cloud Vision, un nuovo servizio di video sorveglianza e analisi video su Cloud che utilizza una tecnologia automatizzata per semplificare la gestione della sicurezza e la raccolta delle informazioni.

Questi erano solo alcuni dei nuovi lanci e prodotti presentati nell'edizione di quest'anno, che hanno confermato che IFSEC International è la "casa della sicurezza". IFSEC International tornerà l'anno prossimo all'Excel di Londra dal 21 al 23 giugno.

intersec

BOOK YOUR STAND NOW!

January 17 – 19, 2016
Dubai, UAE
www.intersecexpo.com

Ensure another year of security for your business plans

We're achieving new heights with each passing year!

2015 Exhibitor Facts

- 1,235 exhibitors
- 52 countries
- 82% international exhibitors

2015 Visitor Facts

- 27,303 visitors
- 118 countries
- 52% international visitors

What's new in 2016?

- Smart Home and Home Automation Equipment
- Safety Design in Buildings
- Extended IT-Security Section
- Physical & Perimeter Security
- Job Pavilion

messe frankfurt

SICUREZZA 2015: soluzioni per il retail ma non solo

a cura della Redazione

Pronte tante iniziative per la manifestazione che si propone di lanciare uno sguardo anche al futuro.

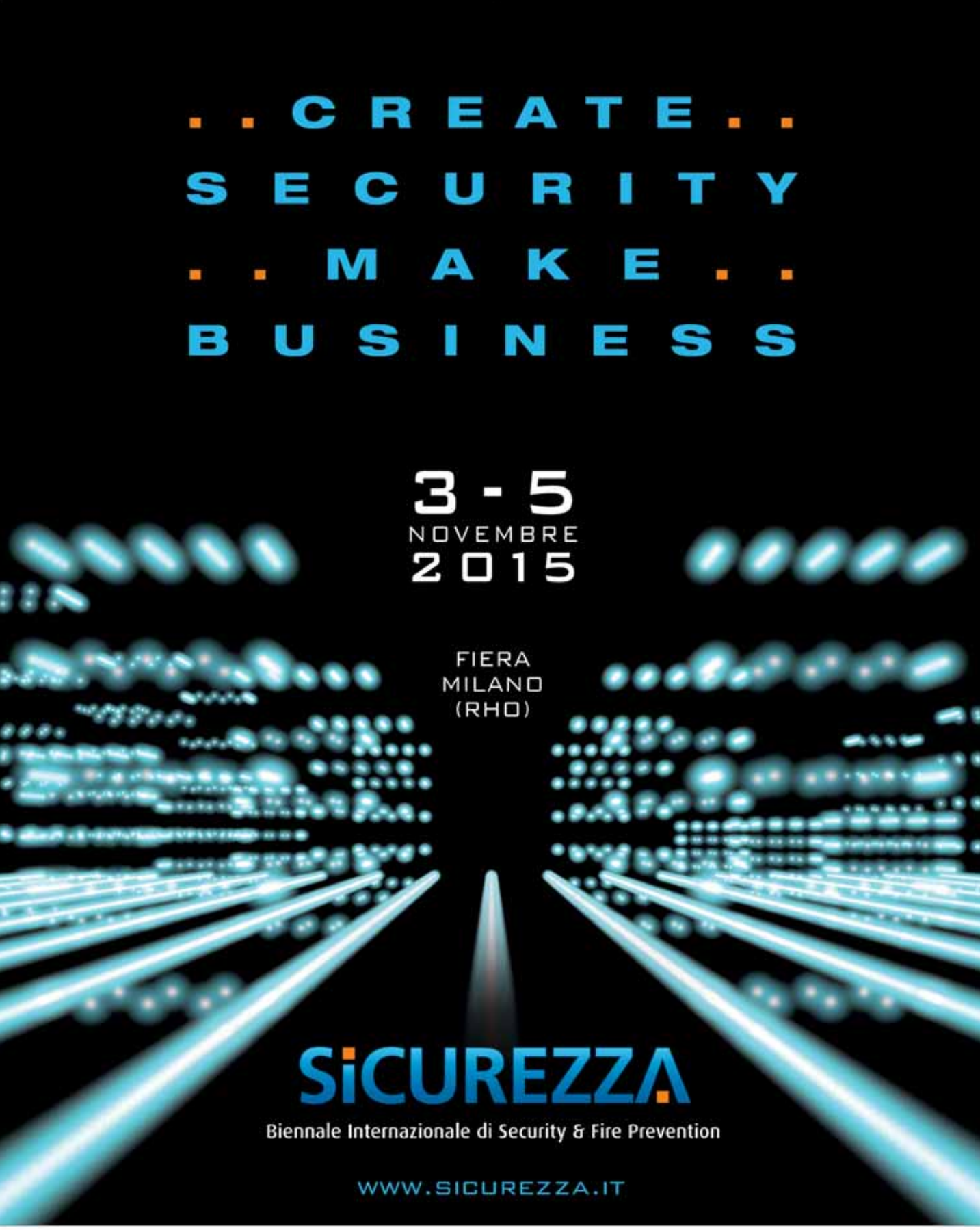
Parola d'ordine: Soluzioni applicate. **SICUREZZA 2015,** unico evento internazionale in calendario nel secondo semestre di quest'anno dedicato a Security & Fire Prevention, **dal 3 al 5 novembre 2015** a **Fiera Milano** non offrirà soltanto un panorama completo di tecnologie dei più grandi produttori italiani e internazionali, ma proporrà anche iniziative speciali dedicate a un mondo di applicazioni in continua crescita. Gli operatori avranno dunque a disposizione esempi concreti per comprendere a pieno le potenzialità delle tecnologie all'interno di ambiti, confrontando in modo diretto le proposte delle aziende con le necessità degli utenti.

Così, sia grazie agli espositori che metteranno a disposizione dei visitatori le proprie *case histories* più interessanti, sia attraverso progetti pensati per dare il giusto spazio all'innovazione, **SICUREZZA** si caratterizzerà per un'offerta ricca di interessanti proposte pensate su misura per i vari contesti di impiego.

Tra i temi più attuali del momento ci sono sicuramente le proposte per il retail. Grazie alla collaborazione con **essecome/securindex.com**, **SICUREZZA** ospiterà la prima edizione del "**Security for Retail Show",** un'area dedicata a soluzioni specifiche per questo settore, una realtà complessa e sempre più interessata ai sistemi di protezione e business intelligence. Infatti, che si tratti di vie ad alta concentrazione di esercizi commerciali o di negozi isolati, di grandi centri o di piccole botteghe, di paesi o di città, secondo gli ultimi dati del Barometro Mondiale dei

Furti nel Retail, nel 2013 si sono registrate differenze inventariali per un totale di 3,1 miliardi di Euro, di cui più di 1,5 miliardi per taccheggi. Si tratta di cifre che danno l'idea concreta di un problema verso cui occorre fare fronte comune.

Non bastano però solo le soluzioni tecnologiche, ma occorre una cultura diffusa e una collaborazione tra tutte le parti in causa: gli esercenti e i fornitori di sistemi e servizi di sicurezza, le Forze dell'Ordine e la Vigilanza Privata. Per favorire il confronto su queste problematiche e proporre soluzioni su misura per ogni tipologia di punto vendita, le aziende che si rivolgono a questo comparto, all'interno del "Security for Retail Show"**,** avranno la possibilità di presentare tecnologie e soluzioni verticali dedicate.



INTERNATIONAL NETWORK

EXPOSEC INTERNATIONAL SECURITY FAIR
www.exposec.tmp.br

FISP INTERNATIONAL FAIR OF SAFETY AND PROTECTION
www.fispvirtual.com.br

Follow us on

EXPO MILANO 2015

FIERA MILANO

Official Partner

L'obiettivo è quello di individuare obiettivi condivisi che possano cambiare le prospettive per il futuro della sicurezza nei punti vendita di ogni dimensione.
L'area accoglierà inoltre eventi tematici come talkshow, tavole rotonde e workshop, offrendo un'occasione interessante per favorire l'informazione e la formazione degli esercenti, mettendo in contatto con i *retailer* i produttori di sistemi e servizi di sicurezza che possono dare un nuovo impulso all'evoluzione dei negozi di prossimità. Ma non si tratta dell'unica iniziativa verticale: si parlerà di integrazione tra ICT e security, di esempi di eccellenza in ambiti verticali, ma si getterà anche uno sguardo alle prospettive future, con un'attenzione alle ricadute della diffusione dell'internet of things: il mondo delle applicazioni integrate e interconnesse consentirà infatti alla security di diventare sempre più integrata, versatile e trasversale nel mondo dell'automazione, della comunicazione e del controllo di cose e persone.
Tante dunque le proposte della manifestazione, che si arricchiranno con l'avvicinarsi dell'evento.

SICUREZZA 2015, intanto, alla vigilia del suo esordio negli anni dispari, continua a crescere, confermandosi evento di riferimento per tutti i professionisti del settore**.** In particolare, si stanno formalizzando a ritmo serrato adesioni da aziende in tutti i comparti, in linea con le soluzioni richieste dal mercato, e si conferma una forte presenza delle soluzioni dedicate alla Videosorveglianza, alla Sicurezza passiva e al Controllo Accessi, tra i settori con il maggior numero di aziende iscritte. Notevole, inoltre, la presenza di brand leader del settore, che hanno scelto la manifestazione perché in contatto con i loro mercati di riferimento e potenziale via di sbocco verso nuove opportunità commerciali.

I vantaggi di giocare d'anticipo
L'appuntamento è dal 3 al 5 novembre 2015. **SICUREZZA** per questa edizione gioca dunque d'anticipo, non solo rispetto all'anno, ma anche sulle iniziative collaterali e ai servizi per gli operatori.
Sul sito **www.sicurezza.it** è già disponibile l'elenco aggiornato degli espositori.
Ai più previdenti inoltre piacerà la possibilità di poter già oggi ottenere una scontistica interessante e prezzi agevolati sui costi di vitto e alloggio durante la manifestazione. In particolare, grazie a Trenitalia, per raggiungere **SICUREZZA** a prezzi vantaggiosi visitatori ed espositori possono acquistare pacchetti speciali, che includono il viaggio in treno A/R e pernottamenti in hotel 4 stelle. I viaggi inseriti nei pacchetti verranno effettuati con treni Frecciarossa e FrecciaBianca dalle principali città italiane (esempio, Roma, Firenze, Bologna, Torino, Venezia e Trieste).
Sempre sul sito della manifestazione è possibile consultare l'orario dei treni che saranno interessati all'iniziativa e prenotare. Da luglio è infine disponibile anche la pre-registrazione e il preacquisto on line, che consentono di ottenere il proprio biglietto al 50% di sconto. Allora che aspettate? Prendete subito il treno giusto!

DAHUA
(+39) 0362-1791300
marketing@videotrend.net

Nuove telecamere Dahua HDCVI 1080p 1200 Lite e DVR Tri-bridi S2

Sono IR bullet e dome, con obiettivi fissi e varifocali. Adottano un chipset più performante con sensore e nuovo ISP incorporati che danno immagini di qualità eccezionale con colori vivaci ed abbondanza di dettagli, angolo visivo più ampio e dimensioni più contenute. La tecnologia smart IR rende più accurato il cambio giorno/notte. L'eccellente riduzione del rumore limita l'occupazione di spazio sull'hard disk e rende le immagini più dettagliate anche con poca illuminazione. Per questo sono l'ideale nei parcheggi sotterranei o in situazioni con scarsità di luce.La serie S2 di DVR HDCVI può sostituire tutti i DVR convenzionali: hanno tre tipi di segnale in ingresso (analogico, HDCVI e IP) e la miglior riproduzione del colore mai vista.La serie S2 è in grado di supportare una maggiore distanza di trasmissione per le telecamere (1.100 metri @720p con immagini chiare e 800 metri per @1080p); Wi-Fi e 4G, per una trasmissione dati più fluida e più veloce. **Distribuiti da Videotrend. VIDEOTREND è il distributore ufficiale per l'Italia di DAHUA Technology**

DIAS SRL
(+39) 02 38036901
www.dias.it

DIAS presenta il sistema EPIR3 di ELDES

DIAS presenta **EPIR3,** un innovativo sistema di sicurezza appartenente alla linea **ELDES,** con una gamma completa di prodotti che offrono massima affidabilità, funzionalità avanzate (quali la parte radio completamente bidirezionale e la gestione tramite app) e un rapporto qualità-prezzo di assoluto interesse. Il cuore del sistema EPIR3 è un doppio rivelatore PIR con funzioni di una centrale d'allarme con modulo GSM integrato, 1 ingresso zona cablata e 1 uscita logica a bordo, espandibile fino a 16 rivelatori senza fili bidirezionali, e 32 uscite programmabili. Con una memoria di 100 eventi e la possibilità di assegnare fino a 10 codici utenti, il sistema è dotato di un modulo GSM/GPRS per invio chiamate alla centrale di sorveglianza, chiamate vocali e SMS fino a 10 numeri telefonici. Sono semplici e veloci da installare e programmare e sono configurabili sia in loco sia da remoto. Il sistema EPIR3 è esteticamente uguale ad un rivelatore e si adatta all'ambito residenziale, oltre che per la protezione di piccoli negozi, camper e barche.

ERMES ELETTRONICA
(+39) 0438 308470
www.ermes-cctv-com

Interfonia e diffusione sonora per gli istituti di pena

ERMES ha messo a punto soluzioni specifiche per i sistemi di interfonia e diffusione sonora Over IP destinati all'uso negli istituti di pena. In particolare, l'interfono **InterLAN-EC.1P** della serie EASY è stato studiato per l'impiego nelle celle delle carceri. È un apparato in esecuzione antivandalo per montaggio ad incasso recanti sul pannello frontale un pulsante di chiamata, un led di segnalazione, un microfono ed un altoparlante. Questi ultimi hanno una protezione che impedisce il danneggiamento. La scatola da incasso è realizzata in acciaio con spessore 15/10 con alette antistrappo che impediscono la rimozione dal muro; il pannello frontale è in acciaio inox con spessore di 30/10 ed è fissato con viti anti-manomissione monouso, con testa che permette il solo avvitamento. Grazie all'elevata qualità dell'audio, questo interfono può anche essere utilizzato come altoparlante di un sistema di diffusione sonora per la riproduzione di annunci; tra le funzioni implementate è anche presente quella di ascolto ambientale silenzioso.

EKEY BIOMETRIC SYSTEMS SRL
(+39) 0471 922 712
www.ekey.net

Nuovo driver ekey per la domotica Control4

ekey annuncia che è stata messa a punto una nuova interfaccia per integrare i **lettori d'impronte digitali** nel sistema **Control4.** Il driver è gratuito e funziona con tutte le soluzioni ekey per il controllo dell'accesso fisico: ekey home, ekey multi e ekey net. Ad ogni uso di un lettore ekey, il driver trasmette a Control4 i dati degli utenti ekey, compreso il numero d'utente, il numero del comando e l'ID del terminale. Integrando i lettori d'impronte digitali all'avanguardia, **chiavi perse o codici dimenticati appartengono al passato**. Oltre a controllare l'accesso, i lettori d'impronte possono **provocare determinate azioni** oppure **richiamare impostazioni personalizzate** (temperatura della stanza, intensità luminosa ecc.). Con il passaggio del dito si può controllare il sistema d'allarme, ridurre il consumo energetico ecc. Sono **disponibili driver per molti marchi di home automation**. Quanto al sistema ekey, occorrono il lettore impronte, la centralina di comando e l'interfaccia (convertitore UDP). Per ottenere il driver contattateci sotto: italia@ekey.net

FRACARRO RADIOINDUSTRIE SPA
(+39) 0423 7361
www.fracarro.it

Impianto filare o wireless? Da oggi Defender Hybrid

Defender Hybrid è il nuovo sistema antintrusione per utilizzare nello stesso impianto dispositivi filari e wireless. La centrale gestisce di serie fino a 40 dispositivi wireless e 8 filari; gli ingressi sono espandibili a 64 (filari e/o WL), con i moduli accessori su BUS 485. Hybrid utilizza la stessa logica di programmazione dei sistemi Fracarro, è integrabile con i dispositivi della gamma Defender filare ed è molto interessante per l'**affidabilità** contro i falsi allarmi. Grazie alla comunicazione dinamica su 4 canali, in caso di disturbo il sistema sceglie un canale alternativo su cui comunicare (funzione *frequency hopping)*, entrando in allarme solo se è realmente necessario. La sicurezza è ulteriormente assicurata dalla trasmissione radio 868 MHz bidirezionale e da funzionalità come il *test radio*, che segnala il livello di batteria dei sensori, e la *supervisione radio programmabile*, per la verifica periodica dell'impianto. Il sistema Hybrid è controllabile con il telecomando 5 tasti con feedback sonoro e visivo dello stato dell'impianto. Per informazioni: ufficio. comunicazione@fracarro.com

GUNNEBO ITALIA SPA
(+39) 02 267101
www.gunnebo.it

SafePay™ Gunnebo

Il sistema di **Cash Management SafePay™** offre vantaggi notevoli rispetto ai punti cassa tradizionali: elimina errori nel conteggio dei resti, le differenze di cassa, identifica eventuali falsi (certificazione BCE) e consente al personale di fornire un miglior servizio ai clienti. Nella configurazione a ciclo chiuso, il versamento immediato dell'incasso rende inaccessibile il contante, azzerando il rischio di furti e rapine. Il software di back office permette di gestire da remoto la gestione manuale del contante. **SafePay™** è veloce nel dare il resto esatto, azzera i tempi di calcolo del fondo cassa e riduce l'immobilizzo per il cambio turno, garantendo il ritorno sull'investimento in tempi rapidi. **SafePay™** è disponibile anche con le esclusive valigie SCL iBox, dotate di meccanismo di inchiostratura e localizzazione satellitare, pronte per essere prese in carico dal servizio di trasporto valori scelto dal distributore. Il flusso di contante dalle casse al CIT non è mai stato così efficiente: rapido, sicuro e completamente chiuso dall'inizio alla fine.

HESA SPA
(+39) 02 380361
www.hesa.com

Termocamere FLIR Serie FC

Nella gamma FLIR distribuita da HESA si segnalano le termocamere **Serie FC**, che offrono costi contenuti e prestazioni eccellenti. La Serie FC si avvale della stessa tecnologia che caratterizza i più sofisticati sistemi FLIR rivolgendosi agli utenti la cui applicazione primaria è la sicurezza a medio raggio. Si tratta di strumenti eccellenti che permettono di vedere intrusi e altri pericoli nel buio totale, offrendo in qualsiasi condizione atmosferica immagini ad alto contrasto ottimizzate con il Wide Dynamic Range Thermal, per sfruttare al meglio il software di video analisi. Dotate di "lenti atermiche", le termocamere Serie FC riescono a mantenere automaticamente la messa a fuoco a prescindere dalla temperatura ambiente. Grazie all'alto grado di integrazione garantito dallo standard ONVIF, queste termocamere possono essere utilizzate in installazioni di sicurezza nuove o già esistenti. Alla Serie FC si affianca oggi la nuova Serie T41, presentata in anteprima da HESA in occasione del Meeting Concessionari e Installatori Autorizzati 2015.

PYRONIX
01709 700100
www.pyronix.com

Sorveglia la tua abitazione, ovunque tu sia!

La nuova APP HomeControl+ è compatibile con S.O. Android e iOS per controllare la centrale Enforcer32-WE APP utilizzando lo smartphone come tastiera wireless. L'infrastruttura Cloud (www.PyronixCloud.com) garantisce agli utenti una piattaforma semplice e sicura per il collegamento da remoto tramite l'App HomeControl+.

Solo con un tocco allo smartphone, si possono Inserire e disinserire le aree, conoscere lo stato, escludere i sensori, leggere lo storico degli eventi, attivare le uscite domotiche. Con le Notifiche Push, si ricevono ovunque aggiornamenti in tempo reale dello stato, utilizzando l'HomeControl+ e il PyronixCloud.

Presto l'App HomeControl+ integrerà i sistemi intrusione Pyronix con la gestione del video attraverso l'infrastruttura PyronixCloud, per poter verificare in tempo reale le immagini attraverso l'App HomeControl+, oltre al controllo della centrale di allarme. L'infrastruttura PyronixCLoud, inoltre permette all'installatore abilitato di collegarsi alla centrale per programmare e diagnosticare da remoto le proprie installazioni.

SAET ITALIA SPA
(+39) 06 24402008
www.saetitalia.it

Da SAET Italia spa la Centrale MIURA

La Centrale Miura è un sistema potente e ricco di prestazioni, per sistemi di sicurezza personalizzati al 100% sulle esigenze dell'utente finale, consentendo all'installatore di esprimere tutta la sua professionalità. Alcune novità che creano valore per l'utente finale:

- multitasking: Miura è dotata di un algoritmo di scheduling che permette di eseguire più operazioni senza dover uscire dal processo principale di funzionamento;
- comunicazione integrata: invia messaggi vocali, SMS o mail, può centralizzare gli eventi verso un centro di raccolta tramite TCP/IP. Inoltre si può accedere alle informazioni tramite consolle locale e da remoto tramite smartphone o PC.
- funzioni vocali: oltre alle chiamate di allarme offre tre importanti servizi: la gestione da remoto tramite guida vocale; l'aiuto vocale con le istruzioni per effettuare le principali operazioni sulla consolle; l'eco vocale sull'esito dell'attivazione e della disattivazione.

Da segnalare Inoltre: personalizzazione del menu, metodo di attivazione e automazione integrata.

SATEL ITALIA SRL
(+39) 0735 588713
www.satel-italia.it

Tastiera total wireless La nuova tastiera dedicata alla serie Versa e Versa Plus

VERSA-LCDM-WRL, nasce per accrescere la già ampia gamma di accessori compatibili e per offrire un'ottima soluzione ad utenti ed installatori che danno importanza alla qualità ed alla funzionalità del sistema, senza dover necessariamente fare opere di muratura.
La tastiera è completamente bidirezionale ed è compatibile con tutti i dispositivi della serie VERSA e VERSA Plus.
L'eccezionalità di questa tastiera è il fatto che sia esattamente uguale alla tastiera cablata per estetica e per funzionalità. Ha sempre i sedici caratteri di visualizzazione e la retroilluminazione led bianca.
È stato aggiunto il lettore di prossimità per un controllo a più livelli per facilitare la gestione dell'utente. Con questa novità, Satel vuole essere sempre più attenta alle mille sfaccettature nell'interpretazione degli impianti in modo che si possano progettare sistemi tagliati su misura degli utenti o dei luoghi da proteggere.

TSEC S.P.A.
(+39) 030.5785302
www.tsec.it

CLV-03 Sensori inerziali con contatto magnetico di grado 3 integrato

I sensori inerziali CLV di TSEC S.p.A. sono i primi al mondo ad utilizzare la tecnologia magnetica Magnasphere® per il rilevamento delle vibrazioni. Basati su un nuovo principio ibrido inerziale/magnetico, non sono soggetti a vincoli di posizionamento e possono venire installati dove il pericolo di scasso è più alto.
La loro sensibilità è paragonabile a quella della migliore sensoristica, rendendoli compatibili con le schede di analisi più usate dai maggiori produttori. Il contatto magnetico ad alta sicurezza integrato ne fa un dispositivo completo per la protezione di qualunque varco.
Sono disponibili nelle versioni a cavo e a morsetti. Quest'ultima consente l'adozione del pratico sistema plug per l'inserimento rapido di resistenze di fine linea.
Basandosi su tecnologia passiva i sensori della serie CLV garantiscono grande affidabilità nel tempo e un'elevata immunità ai disturbi ambientali. Sono garantiti 10 anni. Accoppiati alle schede di analisi VAS permettono la gestione puntuale di sensibilità molto elevate.

VIDEOTREND SRL
(+39) 0362 -1791300
marketing@videotrend.net

Vedi di notte come se fosse giorno e con analisi video incorporata

Videocamera bullet IPC-HFW8281E-Z Dahua di ultima generazione, con le prestazioni più elevate in assoluto nel mercato: 2Mp IP, IR camera, ultra smart, certificata IP66 con analisi video e Light hunt.Analisi video con motion detector con 396 aree (22x18) e 6 livelli video: video loss, anti mascheramento, abbandono e rimozione oggetti, occupazione posteggi, analisi direzionale con discriminazione della velocità, cambio inquadrature, audio detection. Lavora con scarsa luminosità e mostra le immagini come se fosse giorno e con colori perfetti. Dotata di: sensore CMOS progressivo 1/1.9 Sony Exmor low illumination, risoluzione 2Mp con 50Fps, ICR meccanico, ottica motorizzata 4-8 mm auto IRIS DC, uscita video, porta LAN 10/100/1.000, ingresso e uscita allarme, ingresso e uscita audio, 1 slot SD-Card per brevi backup, seriale RS485, privacy mask 4 aree, 2-3D, WDR 120db, ROI (funzione region of interest) ed EIS.
Distribuzione Videotrend
VIDEOTREND è il distributore ufficiale per l'Italia di DAHUA Technology

ELENCO FIERE

AFRICAN BUSINESS CONTINUITY AND EMERGENCY REPONSE SUMMIT
8/18/2015 8/19/2015
Johannesburg, South Africa

Aviation Security 2015
9/16/2015 9/17/2015
Dubai, U.A.E.

BALKAN DEFENCE EXPO - BDE2015
9/25/2015 9/27/2015
Sofia, Bulgaria

HOME AND BUILDING
10/27/2015 10/28/2015
Verona, Italia

CPSE EXHIBITION 2015
10/29/2015 11/1/2015
Shenzhen, China

SICUREZZA 2015
11/3/2015 11/5/2015
Milano, Italia

ALL-OVER-IP
11/18/2015 11/19/2015
Moscow, Russia

FORUM RETAIL
11/24/2015 11/25/2015
Milano, Italia

INTERSEC 2016
1/17/2016 1/19/2016
Dubai, U.A.E.

TB FORUM powered by Intersec 2016
2/9/2016 2/11/2016
Moscow, Russia

essecome security&safety

n. 03 maggio-giugno 2015

ISSN: 2384-9282

Anno XXXV-III
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO A QUESTO NUMERO
Frediano Di Carlo, Bruno Fazzini, Jan Noten, Gennaro Percannella, Massimo Riboli, Piero Ricciardi. Pietro Tonussi

SEGRETERIA DI REDAZIONE
redazione@securindex.com

GRAFICA/IMPAGINAZIONE
servizio interno dell'editore

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Bozzini 3/A
Milano - Via Montegani, 23
Tel. +39 02 36757931

ISCRIZIONE AL ROC
Secman srl è iscritta al ROC (Registro Operatori della Comunicazione) al n. 22892 del 26/10/2012

REGISTRAZIONE
Tribunale di Verona n. 1971 R.S. del 21 dicembre 2012

STAMPA
PINELLI PRINTING Srl
Via Redipuglia 9
20060 Gessate (MI)
Sede Operativa: Via E. Fermi 8
20096 Seggiano di Pioltello (MI)
Tel. 02.9267933 - Fax 02.9266527
www.pinelliprinting.it

Partner Essecome

A.I TECH	www.aitech-solutions.eu	31-34
ANIVP	www.anivp.it	88
AXIS COMMUNICATION	www.axis.com	66, 76-79
AXITEA	www.axitea.it	91-92
BETAFENCE	www.betafence.it	13, 59-61
BOSCH SECURITY SYSTEMS	http://it.boschsecurity.com/it/	35-36, 38
CITEL	www.citel.it	52-54
DAHUA	www.dahuasecurity.com	2-3, 47-48, 57-58, 103, 106
DIAS	www.dias.it	15, 103
ELAN	www.elan.an.it	II copertina
EKEY BIOMETRIC SYSTEMS	www.ekey.net	41-43, 56, 104
ERMES	www.ermes-cctv.com	60, 103
FLIR	www.flir.com	67
FONDAZIONE ENZO HRUBY	www.fondazionehruby.org	67-69
FRACARRO	www.fracarro.it	37, 104
GUNNEBO	www.gunnebo.it	64-65, 75, 104
HESA	www.hesa.it	III cop, 14-16, 44-46, 105
HONEYWELL	www.honeywell.com	11
IFSEC 2015	www.ifsec.co.uk	96-98
INTERSEC 2016	www.intersecexpo.com	99
ISEO SERRATURE	www.iseoserrature.it	17
IVRI	www.ivri.it	93-95
KABA	www.kaba.it	39-40, 55-56
MILESTONE SYSTEMS	www.milestonesystems.com	23-24
MONDIALPOL GROUP	www.mondialpol.it	83-85
PYRONIX	www.pyronix.com	49-51, 105
SAET ITALIA	www.saetitalia.it	I copertina, 105
SATEL	www.satel-italia.it	IV copertina, 106
SICUREZZA 2015	www.sicurezza.it	100-102
TB FORUM	http://eng.tbforum.ru	97
T-SEC S.P.A.	www.tsec.it	I romana, 106
VANDERBILD	www.vanderbiltindustries.com	21
VERIZON	www.verizonenterprise.com	18-19
VIDEOTREND	www.videotrend.net	2-3, 47-48, 57-58, 103, 106

FLIR®

Termocamere di rete Serie FC

La sicurezza più sofisticata non è più un miraggio

Le termocamere Serie FC permettono di vedere intrusi e altri pericoli nel buio totale, anche in condizioni atmosferiche avverse.

Offrono la stessa tecnologia dei più sofisticati sistemi di sicurezza FLIR a costi contenuti, per gli utenti la cui necessità primaria è la sicurezza a medio raggio.

Sono strumenti eccellenti per installazioni di sicurezza sia nuove che esistenti grazie all'alto grado di integrazione garantito dallo standard ONVIF.

www.hesa.com

HESA®

VERSA Plus

sicurezza, flessibilità, comfort

La risposta alle esigenze dei vostri clienti

Versa Plus è la centrale compatta ideale che, grazie ai suoi 6 moduli integrati sulla scheda, rende il sistema adatto ad ogni tipo di esigenza.

- integrati: GSM, GPRS, PSTN, scheda di rete, modulo vocale, ascolto ambientale
- impianto filare, ibrido o totalmente wireless
- scelta tra 8 diversi modelli di tastiere filari, wireless e touch
- comunicazione multivettoriale
- notifiche e-mail e PUSH
- applicativo mobile **VERSA Control**

Scopri di più su **www.satel-italia.it**

Satel® ITALIA