

Satel
— ITALIA —

VERSA Plus

La risposta alle esigenze dei vostri clienti



Scarica
VERSA
Control



iOS

La centrale con 6 moduli integrati

Scopri di più su www.satel-italia.it

ELANFIRE "Sect." - CEI 20-22/III



Allarme/Sicurezza
PVC

ELAN HD RG6 75 OHM LSZH...



Allarme/Sicurezza
LSZH

Allarme Incendio

ELAN UTP...



Cavi Rete
LAN/Network

Coassiali
TVCC/SAT

Segnale/
FROR/Cancelli

Non rinunciare a
QUALITA' e SICUREZZA
- www.elan.an.it -

**BATTERIE
AL PIOMBO**

**BIGBAT Standard
(6V e 12V)**

**BIGBAT Long Life
(2V e 12V)**



Nuovi orizzonti visivi

Osserva un'intera area di parcheggio con immagini in campo lungo di straordinaria chiarezza e leggi le targhe di ogni veicolo allo stesso tempo. Scopri come Avigilon 7K HD Pro, la prima telecamera 7K (30 megapixel) del settore, migliora la risoluzione di quasi quattro volte rispetto alle telecamere 4K riducendo allo stesso tempo i requisiti di larghezza di banda e archiviazione.

7K



MASSIMA
CHIAREZZA

REQUISITI MINIMI
DI LARGHEZZA
DI BANDA
E ARCHIVIAZIONE

avigilon

Eco-Savvy Series 2.0

4-Megapixel IP Camera

- 4M@20fps; 3M@25/30fps
- Triplo stream video
- IP67 e IK10
- Analisi video integrata
- Ultra WDR (Wide Dynamic Range) fino a 120dB
- Zoom ottico 30x (telecamere speed-dome)



Le telecamere Dahua della serie Eco-savvy2.0 sono in grado di fornire prestazioni più elevate grazie al nuovo processore Ambarella S2LM che offre maggiori vantaggi con l'aggiunta di nuove funzioni tra cui la cui la risoluzione 4MP, WDR e analisi video. Inoltre, il sensore e la struttura meccanica delle nuove telecamere sono state migliorate per raggiungere una qualità di altissimo livello. Tutte queste innovazioni rendono la serie Eco-savvy2.0 di Dahua una soluzione con un ottimo rapporto prezzo/prestazioni e, quindi, ideale per una vasta gamma di applicazioni nella videosorveglianza in alberghi, fabbriche, negozi, edifici commerciali e nel terziario.



Modelli raccomandati:

- >> IPC-HPW5121/5220/5221/5421E-Z <<
- >> IPC-HDBW5121/5220/5221/5421E-Z <<
- >> SD59212T/220T/230T-HN (2MP) <<
- >> PC-HDBW4120/4220/4221/4421E <<
- >> IPC-HDBW4120/4220/4221/4421F <<
- >> SD50220T/230T-HN (2MP) <<



SECURITY FOR RETAIL SHOW

3-5 novembre 2015

Un innovativo format dedicato alle soluzioni
per la sicurezza nel mondo della distribuzione.

SICUREZZA

Security for Retail Show è un progetto condiviso da fiera **Sicurezza** e **essecome/securindex.com** per offrire un'opportunità alle aziende del settore di partecipare a **Sicurezza 2015** con un ottimo rapporto qualità-prezzo.

L'area è costituita da un insieme di postazioni in cui gli espositori potranno presentare le tecnologie, gli ambiti di applicazione e i loro sviluppi. Gli espositori avranno inoltre la possibilità di partecipare ai talk show che saranno organizzati all'interno dell'area vicina di **essecome/securindex.com**, e confrontarsi sui temi di grande attualità con il contributo di **security manager delle maggiori catene di distribuzione, rappresentanti delle categorie ed esperti.**

PACCHETTO A – ESPOSIZIONE

- Quota di iscrizione
- Area espositiva in spazio comune
- Allestimento e arredo stand (moquette, impianto elettrico, tavolo, desk, sedie)
- 1 park auto all'interno del quartiere
- Codici Invito alla Clientela
- Iscrizione all'EMP (Expo Matching Program)

PACCHETTO B – ESPOSIZIONE + COMUNICAZIONE

- Partecipazione come Espositori (Pacchetto A)
- Partecipazione a una tavola rotonda tematica organizzata da **essecome/securindex.com** con speech riservato
- Intervista televisiva durante l'evento, con montaggio dedicato
- n. 1 pagina ADV in **essecome** n. 5/2015 (speciale Sicurezza 2015)
- Logo nella cover interna di **essecome** n. 5-6/2015 e nella comunicazione correlata
- n. 1 articolo post-view in **essecome** n. 6/2015 e in www.securindex.com

PACCHETTO C – ESPOSIZIONE + COMUNICAZIONE PUSH

- Partecipazione come Espositori (Pacchetto A)
- Partecipazione a una tavola rotonda tematica organizzata da **essecome/securindex.com** con speech riservato
- Intervista televisiva durante l'evento, con montaggio dedicato
- n. 2 pagine ADV in **essecome** n. 5-6/2015
- Logo nella cover interna di **essecome** n. 5-6/2015 e nella comunicazione correlata
- n. 1 articolo/intervista di presentazione in **essecome** n. 5/2015 (speciale Sicurezza 2015)
- n. 1 articolo post-view in **essecome** n. 6/2015 e in www.securindex.com
- Organizzazione di workshop riservato di 30' con riprese televisive nel set di **essecome/securindex.com**

Per informazioni e prenotazioni scrivere a marketing@securindex.com

Può la Sicurezza della Cultura contribuire alla Life Continuity?

Perché l'Isis ha sostituito le immagini di Jihadi John che decapita prigionieri inermi, con le quali ci aveva "deliziato" per mesi, con quelle della distruzione delle tombe romane di Palmira?

Tra le possibili spiegazioni, c'è anche quella che gli esperti della comunicazione del Califfato abbiano valutato che l'abbattimento di un monumento riesca turbare l'opinione pubblica occidentale più dell'uccisione di un uomo. In effetti, se da una parte è (purtroppo) vero che la televisione prima e i social dopo ci hanno abituati allo spettacolo della morte in diretta dappertutto, nei modi più truculenti e in ogni momento del giorno, dall'altra la distruzione di un "segno" di valore religioso, artistico o storico, trasmette un messaggio esponenzialmente più drammatico.

Non a caso, fin dall'antichità gli invasori hanno sempre cercato di distruggere appena possibile i segni identitari degli sconfitti, per consolidare il successo. Tra le distruzioni di questo genere passate alla storia, quella del tempio di Gerusalemme a opera dei Romani nel 70 d.C. è forse ancora adesso la più devastante e fragorosa. Non sorprende quindi che l'Isis faccia saltare per aria, curando di farlo sapere al mondo intero, le tracce millenarie lasciate dai nostri antenati nel territorio che il Califfato rivendica, né che nel 2001 i Taleban abbiano preso a cannonate i due Buddha giganti di Bamiyan per affermare platealmente il proprio dominio sulla Via che fu prima della seta, poi dell'oppio.

Pur essendo di ben altro livello, anche gli hooligans olandesi che hanno sfregiato nella primavera scorsa a Roma la fontana del Bernini, si sono accaniti contro un monumento dell'avversario di turno, nell'idiota concezione del tifo calcistico come guerra permanente contro gli "altri".

In questo periodo, si sta consolidando il modello di Smart City, una "summa tecnologica" dichiaratamente rivolta a migliorare il benessere e la sicurezza dei melting pot metropolitani che, in tutto il mondo, stanno lievitando al ritmo di un milione di persone alla settimana (vedi articolo pag. 10).

Contemporaneamente, e non è un caso, si sta affermando il modello di Business Continuity come metodo per garantire la continuità operativa delle organizzazioni di fronte a calamità di ogni tipo - naturali, accidentali, dolose. Quanto accaduto a Palmira è solo un ultimo episodio di distruzione voluta (ma pensiamo al terremoto di Kathmandu o al degrado di Pompei) che dovrebbe far riflettere sul ruolo e il significato che i beni culturali possono avere per la "Life Continuity" dei popoli, a maggior ragione quando questi confluiscono in raggruppamenti sempre più vasti ed eterogenei, lontani dai luoghi d'origine.

Perché, dunque, non considerare il patrimonio artistico come una vera e propria Infrastruttura Critica, nel rispetto della definizione internazionale: "un sistema, una risorsa, un processo, un insieme la cui distruzione, interruzione o anche parziale o momentanea indisponibilità ha l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale della comunità"? E perché, allora, non comprendere la messa in sicurezza delle opere che rappresentano la cultura di un popolo tra i fattori importanti per la sua resilienza, definendo i criteri e gli strumenti di protezione come viene fatto per le IC?



IN COPERTINA: VERSA Plus



L'eccezionalità e l'unicità di Versa Plus è data dal fatto che con una sola centrale si possono raggiungere tutti i canali di comunicazione già integrati sulla scheda:

- Scheda di rete TCP/IP per gestione applicativi e per programmazione da remoto (ETHM-1 integrato)
- Linea Telefonica PSTN (Integrato)
- GSM/GPRS (GSM-4 Integrato con doppia SIM)
- Guida vocale (INT-VG Integrato)
- Ascolto ambientale (INT-AV integrato)
- Notifica e-mail
- Notifica Push

Un cuore wireless

VERSA Plus è una soluzione ibrida eccezionale in ogni situazione grazie alla sua grande flessibilità.

Costituisce infatti il cuore di un sistema totalmente wireless offrendo la possibilità di utilizzare anche tastiere totalmente senza fili. L'installatore ha la possibilità di scegliere tra un sistema totalmente wireless, ibrido o cablato con la stessa centrale. Nel caso si scegliesse o fosse necessario un sistema wireless, Versa Plus offre la doppia possibilità di utilizzare o il sistema bidirezionale ABAX (che lavora in frequenza digitale 868 MHz) o il sistema monodirezionale MCU (con frequenza 433 MHz).

Tastiera wireless VERSA-LCDM-WRL

Oltre alla tastiera tradizionale, VERSA PLUS, può essere comandata dalla tastiera wireless bidirezionale che ha la stessa FUNZIONALITA' e la stessa ESTETICA della tastiera filare. La tastiera totalmente wireless può essere fissata a muro o semplicemente appoggiata su di un mobile per offrire la massima libertà di espressione dell'utente.

Tastiera Touch

La serie Versa supporta inoltre la tastiera touch screen INT-TSG per quegli utenti tecnologici che amano il design minimalista e la funzionalità a cui sono abituati giornalmente con gli smartphone di ultima generazione. L'interfaccia grafica, intuitiva e piacevole, facilita qualsiasi tipo di operazione da parte dell'utente. Il design innovativo la rende adatta per qualsiasi tipo di ambientazione.

Satel server

Permette la connessione attraverso il server dedicato per l'accesso senza configurazione del router. L'installatore pertanto può programmare e modificare delle impostazioni attraverso Ethernet con la facilitazione di aprire porte o configurare il router in automatico.

VERSA control

L'applicazione dedicata VERSA CONTROL per smartphone, è gestita direttamente dalla scheda di rete ETHM-1 integrata in centrale per una semplice e comoda gestione del sistema di sicurezza da remoto. Le versioni sono scaricabili gratuitamente per IOS e per Android.

Con VERSA Control da remoto, è possibile attivare e disattivare il sistema, cancellare allarmi, visualizzare lo stato del sistema, escludere o reincludere le zone, verificare lo stato del sistema, visualizzare gli eventi con funzione filtro, visualizzare i guasti con possibilità di cancellazione memoria, attivare e disattivare le uscite.

Gestione conveniente: email e notifiche push

L'applicativo mobile VERSA CONTROL permette di ricevere anche le notifiche push. Questo tipo di segnalazione consente sia all'utente che all'installatore di ricevere informazioni di ogni evento di sistema. Il servizio viene eseguito in background, quindi il destinatario è sempre avvertito in tempo reale! Un ulteriore canale di notifica è tramite email. Sulla scheda di rete ETHM-1 integrata, basta inserire fino ad 8 indirizzi email e tutti i destinatari potranno essere raggiunti tramite un'email che potrà contenere tutte le segnalazioni di sistema.

Attualità

- 08 Il parere di Per Björkdahl su mercato globale, IoT, crisi cinese e non solo...
- 10 Euralarm: Smart Cities protette, sicure e resilienti
- 16 Le Eccellenze per la Sicurezza - Presentazione
- 20 Le Eccellenze per la Sicurezza - I Partner: Axitea
- 23 Le Eccellenze per la Sicurezza - I Partner: Iseo
- 26 Le Eccellenze per la Sicurezza - I Partner: Microntel
- 29 Le Eccellenze per la Sicurezza - I Partner: Mirasys
- 32 Le Eccellenze per la Sicurezza - I Partner: Samsung
- 35 Le Eccellenze per la Sicurezza - I Partner: T-Sec
- 38 Dalla sicurezza partecipata alla (c)lean security
- 44 Italia-Svezia, la sicurezza di una storia nella visita del Console a Gunnebo Italia
- 46 IoT, sicurezza fisica e sicurezza informatica: convergenza o interdipendenza? - Prima puntata

Technologies

- 48 Video Analisi e Forensics Analysis: cosa sì, cosa no, cosa forse...
- 53 Tre paradigmi di Citel per la sistemistica informatizzata di gestione della sicurezza fisica in architettura aperta
- 56 CAME apre le porte di EXPO Milano 2015 con XVIA
- 60 Avigilon: intelligence e video analisi, il futuro della videosorveglianza
- 62 ekey e il mercato globale dei sistemi fingerprint: ottime prospettive di ulteriore crescita
- 66 Dahua presenta le nuove telecamere di rete della serie Eco-Savvy 2.0
- 68 L'attenzione di Saet verso progettisti e installatori a tutela del cliente finale
- 70 L'ecosistema HomeControl+ Pyronix: controllo via IP per il XXI secolo

- 74 La videosorveglianza più evoluta entra nel mondo DIAS con SUNELL
- 72 Kaba 'Food Defence': più sicurezza nella produzione alimentare

Security for Retail

- 78 Cash-management, parte dall'Italia la leadership di Gunnebo nel Retail
- 80 Intelligent Article Surveillance: Adidas innova con le soluzioni intelligenti RFID-ready di Nedap

Fire & Smoke

- 83 La manutenzione dei presidi antincendio, una sicurezza da certificare contro le frodi

Cultura e Formazione

- 87 I racconti della Sicurezza - 2
- 88 Una borsa di studio per il miglior studente del progetto Campus Came nel ricordo di Paolo Tura
- 89 essecome, il "giochino" di Paolo nel ricordo di Valerio
- 91 100 studenti e 20 insegnanti coinvolti nel primo anno di Campus Came

Denaro Sicuro

- 93 Come cambia la sicurezza in banca - 4 La gestione del cash in MPS

Vigilanza & Dintorni

- 96 L'ANAC entra in scena per gli appalti pubblici dei servizi di vigilanza

Fiere

- 98 A Sicurezza 2015 saranno protagonisti i market leader e le soluzioni verticali
- 102 Domotica, IoT, Smart Building, LED, Efficienza Energetica a Home and Building 2015
- 104 Benvenuti a ShenZhen, la capitale della sicurezza in Cina

Redazionali Tecnologie

107-108-109-110-111

Il parere di Per Björkdahl su mercato globale, IoT, crisi cinese e non solo...

a colloquio con Per Björkdahl, Steering Committee Chairman di ONVIF a cura di Raffaello Juvara

Il mondo della sicurezza fisica sta attraversando una fase di profondi cambiamenti che, se anche hanno già scombinato gran parte degli equilibri costruiti progressivamente negli oltre quattro decenni di storia del settore, tutto fa pensare che siano appena all'inizio. L'avvento delle tecnologie IP, che pure ha rivoluzionato la concezione stessa di 'fare sicurezza', è stato solo il fatale battistrada per l'Internet of Things, che provocherà ben altre rivoluzioni e non solo nella security. Fra le altre, se la diffusione degli apparati in rete ha fatto cadere la distinzione tra physical security e cyber security, si può presumere che IoT abbatte le barriere tra la security e il resto del mondo.

D'altra parte, lo sviluppo della multifunzionalità dei sistemi sta già modificando il perimetro dei mercati originari, con un'interazione sempre maggiore con quelli limitrofi. La security, con la videosorveglianza in testa, è 'naturalmente' proiettata verso domotica e safety attiva e, tutte insieme, verso le Smart Cities. Si comprendono, quindi, gli interessi per la security di soggetti diversi, dovuti sempre a motivi economici ma non direttamente collegati al fatturato realizzabile vendendo 'scatole'. Google è il precursore paradigmatico di questi vicinissimi scenari.

Su questi argomenti non oziosi, che riguardano ciò che succederà domani nel giardino degli operatori del settore, abbiamo intervistato un esperto di reputazione mondiale, **Per Björkdahl**, presidente del consiglio direttivo di **ONVIF**, la più autorevole organizzazione globale per la standardizzazione dei sistemi di sicurezza fisica in rete, costituita nel 2008 da Axis Communications, Bosch e Sony. e che ora rappresenta oltre 500 produttori di ogni parte del mondo.

Björkdahl, che si trova probabilmente nel miglior punto di osservazione desiderabile per ricevere informazioni



di prima mano, cogliere i 'sentiment' dei maggiori produttori e percepire i trend del mercato globale, ha tracciato il quadro che proponiamo qui di seguito:

Come valuta le operazioni M&A tra produttori nel mercato globale della videosorveglianza?

Per diversi motivi, le recenti operazioni di acquisto e fusione tra produttori di sistemi di sicurezza fisica non avranno un impatto significativo sul mercato, soprattutto perchè le quote attualmente in capo a singole società sono in media piuttosto piccole. Secondo IHS Inc, nel

2013 nessuna singola società deteneva più del 5% del mercato globale della sicurezza fisica.

La sicurezza fisica - e la videosorveglianza in particolare - sono mercati enormi, letteralmente con migliaia di brand diversi nei singoli segmenti. Gli integratori e gli utenti finali hanno a disposizione un mercato talmente frazionato che, nonostante le aggregazioni in corso, i consumatori hanno ancora molte possibilità di scelta. La diversità dei prodotti e il grande numero di costruttori presenti sul mercato spingono in avanti il settore, in termini di innovazione e di ingegnosità. Dato che nuove aziende entrano sempre più numerose nella sicurezza fisica, i costruttori sono spinti a competere e a rimanere al vertice dello sviluppo delle tecnologie. Le nuove aziende spesso entrano nel mercato con una visione diversa di un'idea già sviluppata e, qualche volta, anche con un'offerta di prodotti completamente nuovi.

Ritiene che i cambiamenti in atto nell'economia cinese possano avere effetto nell'andamento del mercato globale della videosorveglianza?

Nell'economia globale nella quale operiamo tutti noi, ogni movimento o cambiamento può influenzare aree molto vaste e un grande numero di persone, di beni, servizi e anche l'informazione stessa. È difficile prevedere se e come l'economia cinese possa influire in particolare sul settore della videosorveglianza, data la crescita esponenziale che il mercato della sicurezza fisica ha vissuto negli ultimi cinque anni e con le aspettative di ulteriore crescita nei prossimi cinque anni (secondo MarketsandMarkets il mercato globale della sicurezza fisica passerà da USD 65.41 bl nel 2015 a USD 105.26 bl nel 2020, con un CAGR del 9.98% nel periodo - ndr).

Ci può parlare di cyber security/physical security e degli effetti che potrebbero derivare dall'avvento di IoT?

In parte, l'interesse crescente nella sicurezza fisica negli ultimi anni è legato agli attacchi, largamente pubblicizzati, alla cyber sicurezza e ai dati. Numerose organizzazioni pubbliche e private sono spinte a proteggere l'accesso fisico a postazioni di lavoro, centrali operative e server room che trattano o ospitano dati sensibili o registrazioni video; molti ritengono che la sicurezza fisica di queste strutture sia importante quanto la crittografia e altre forme di cyber security. La crescita dell'Internet of Things (IoT) sta certamente guidando l'innovazione e i costruttori sviluppano soluzioni e prodotti lavorando insieme, come mai era stato fatto in precedenza. Per quanto sia teoricamente

possibile, è comunque improbabile che la domanda di soluzioni di sicurezza fisica possa venire drasticamente ridimensionata dalla sfera di influenza dello IoT; del resto, si prevede che la videosorveglianza avrà un ruolo importante nello IoT, sia come hardware che come gamma di servizi offerti.

Quali sono le vostre azioni a supporto dell'integrazione tra sistemi di videosorveglianza, controllo accessi a antintrusione?

Il Profilo A, il nostro ultimo profilo per il controllo accessi, stabilisce un'interfaccia per i clienti ampliando il Profilo C, il primo profilo ONVIF dedicato al controllo accessi. Il Profilo A è più esteso e prende in considerazione un maggior numero di caratteristiche e di funzioni, che si traduce in ulteriori opportunità di integrazione. Anche se il segmento dell'antintrusione è stato attentamente esaminato come prossima, logica area di attività di ONVIF, noi siamo una struttura guidata dai suoi associati, che prende le decisioni in base alle indicazioni collegiali. In questo momento, la nostra attenzione è rivolta agli ulteriori sviluppi dei profili per il controllo accessi e la videosorveglianza. Tuttavia, se ci sarà un accordo sul fabbisogno di un profilo per l'antintrusione, ONVIF sarà certamente disponibile.

Può illustrare le linee guida che ONVIF seguirà per agevolare i test di conformità dei clienti ai Profili di ONVIF, come il test tool per i Profili S,G e C?

Nell'aprile di quest'anno, ONVIF ha realizzato per la prima volta un Client Test Tool per i propri associati. Il test tool è stato creato per rispondere alle richieste del settore per aumentare la responsabilità dei clienti nei confronti della conformità. Il Client Test Tool è a disposizione degli associati e permette a ONVIF di verificare in modo indipendente la conformità dei clienti al profilo ONVIF dell'hardware e del software, come i sistemi di video management systems, building management systems, physical security information management (PSIM).

In precedenza, per ottenere la Dichiarazione di Conformità i costruttori dovevano dichiarare che il loro cliente aveva lavorato con successo con almeno tre singoli apparati conformi al profilo. Il nuovo test tool permette a ONVIF di verificare che il cliente è stato testato con più dispositivi e che è conforme allo standard ONVIF. Le aziende associate possono anche verificare la conformità dei propri prodotti durante i nostri Developers' Plugfests, che vengono normalmente organizzati due volte all'anno, in località diverse in giro per il mondo.

Euralarm: Smart Cities protette, sicure e resilienti

di Paul Zaal (Beta PR & Media) per Euralarm
traduzione a cura della Redazione

Dopo il webinar realizzato in aprile, Euralarm e IFSEC Global hanno organizzato una conferenza sulle Smart Cities a Londra il 17 giugno, dedicata alle soluzioni digitali per la protezione e la sicurezza degli abitanti. Amministratori delle municipalità e rappresentanti dei produttori di sistemi di sicurezza e antincendio si sono confrontati sui punti chiave di questa tematica.

Smart Cities

In tutto il mondo si discute di un utilizzo più efficiente delle strutture pubbliche e private, per poter valorizzare maggiormente le risorse a disposizione. Una 'Smart City' utilizza sia tecnologie digitali che ICT (Information and Communication Technologies) per aumentare la qualità e la prestazioni dei servizi urbani, ridurre i costi e il consumo delle risorse, e potersi rapportare in modo più efficace e attivo con i propri abitanti. Lo **Smart City Council** definisce 'intelligente' la città che ha integrato la tecnologia digitale in ogni funzionalità urbana.

L'industria della Safety e della Security

Nelle aree pubbliche, così come nelle aree commerciali e residenziali, è presente una grande quantità di sistemi dedicati alla sicurezza (safety e security): videosorveglianza, controllo accessi, rilevamento incendi, allarmi antintrusione e sistemi di evacuazione sono solo alcuni dei sistemi in funzione. I sistemi moderni (digitali) consentono di avere informazioni utili di importanza vitale in caso di incidenti e di altre calamità. A nome dei suoi membri, Euralarm ha avviato progetti e partecipa attivamente a iniziative europee o globali dedicate alle Smart Cities. Come evidenziato nello **Euralam PEARS Project** (Public Emergency Alarm and Response System - ndr), il comparto della sicurezza (safety e security) può contribuire in maniera

significativa alla realizzazione di una Smart City: *"Euralarm considera una Smart City sicura, protetta e resiliente quella città in grado di pianificare e mantenere le funzionalità con i minori disagi in caso di incidenti, attentati o disastri naturali. La città deve poter sopravvivere, adattarsi e crescere di fronte a qualsiasi evenienza. L'industria della safety e della security è pronta sostenere le iniziative 'Smart Cities' con i dati forniti dai sistemi di protezione"*.

Agenda e panel della conferenza

Glen Dale, direttore generale di Euralarm, ha aperto la conferenza con una breve introduzione. Il moderatore **Martin Harvey**, chairman della Sezione Servizi di Euralarm, ha iniziato i lavori presentando tutti i relatori. Il primo relatore, **Rolf Sigg**, si è concentrato sulle prospettive del comparto produttivo rappresentato da Euralarm; il secondo relatore, **Jim Mc Hale**, managing director e fondatore di Memoori Research (www.memoori.com), ha affrontato il tema 'Big Data Software' negli edifici; **Neil Orbell**, assistente commissario della 'Fire Safety Regulation and Community Safety of the London Fire Brigade', è stato il terzo relatore. **Nico Tillie** della Delft University (NL) ha illustrato la propria esperienza nell'ambito del progetto 'Smart City' di Rotterdam. Ultimo ma non meno importante, **Jim Glockling**, PhD, direttore tecnico di MiFireE, ha spiegato il sistema denominato 'Building Information Management' (BIM).

Enzo Peduzzi, neo presidente di Euralarm, ha infine concluso la conferenza, riassumendone i contenuti.

Le città dormono mai!

In tutto il mondo, circa un milione di persone si trasferisce ogni settimana verso una città. Rolf Sigg ha presentato alcune tabelle, spiegando che nel 2020



la maggioranza della popolazione mondiale vivrà concentrata in piccole percentuali di superficie del pianeta. Come aveva prima comunicato Martin Harvey, ogni anno circa 100.000 persone si trasferiscono a Londra. Naturalmente, ogni persona ha delle motivazioni soggettive per trasferirsi in una città.

La maggioranza lo fa per motivi economici, di studio e/o sociali ed è difficile credere che vada in una metropoli solo perché è 'smart', ci devono essere altri motivi. Rolf Sigg ha preparato un riepilogo di indagini condotte da consulenti di terza parte sui motivi di attrazione delle città. Nelle prime 10 posizioni, i motivi sono diversi ma è evidente un interesse comune: in generale, le persone cercano una miglior qualità di vita e i centri urbani offrono maggiori possibilità di appartenere a una comunità e di integrarsi in una società.

Il problema è il benessere sociale, non le tecniche

Rolf Sigg ha spiegato come dovrebbe essere una città intelligente allo stato attuale. La gente non ha ancora ben focalizzato il concetto di 'Smart City', che comporta l'utilizzo delle tecnologie digitali per gestire tutte le funzionalità urbane. In questo momento, la maggior parte dei progetti di Smart Cities considerano una città 'intelligente' quando vengono impiegati servizi tecnologici evoluti e infrastrutture in campo energetico, nel trasporto e nell'ICT per rispondere alle esigenze sociali ed economiche dei residenti.

Per migliorare l'approccio, sarebbe opportuno non partire dalle tecniche, ma dalle persone che vivono nella città, perché la comunicazione con gli stakeholder

è più importante. L'attenzione per le Infrastrutture Critiche sarebbe il secondo punto da prendere in considerazione ma è soprattutto la 'resilienza' che dovrebbe diventare il punto di partenza per la realizzazione di una città intelligente.

L'Internet delle Cose e il Big Data Software

Jim McHale è un ricercatore specializzato nelle tecnologie per gli edifici. Anche lui si è focalizzato sulla funzione dell'edificio nella città intelligente. Assieme ad altri aspetti, safety e security sono di certo elementi importanti negli edifici intelligenti. Presentando una panoramica di tutti i servizi che devono essere disponibili negli edifici, ha sottolineato che l'insieme dei sistemi produce una quantità molto elevata di dati per il controllo e il monitoraggio delle funzionalità di un edificio. Ha fatto l'esempio della telecamera facente parte di un sistema di sicurezza, destinata a diventare un terminale IT importante nell'Internet delle Cose, perché è in grado di produrre molte informazioni intelligenti e utili su quello che sta succedendo nell'edificio.

Specialmente negli edifici ad uso non domestico, la maggior parte dei sistemi lavora di norma ognuno nel proprio ambito, del tutto scollegato dagli altri. Questi sistemi sono destinati ad avere incredibili benefici quando saranno connessi gli uni agli altri, al di fuori dei rispettivi ambiti funzionali, con vantaggi che non deriveranno solamente dall'aumento delle informazioni raccolte, ma dall'analisi dei dati aggiuntivi.

Le informazioni provenienti dall'interno degli edifici



potranno venire combinate con quelle dell'esterno, come le condizioni meteo, il traffico e i social media. Per aumentare le condizioni di sicurezza di un edificio, queste informazioni verranno combinate, analizzate, presentate e utilizzate effettivamente in modo efficiente. Per dare un senso al concetto di 'Smart City' in tutta la sua ampiezza, le informazioni per costruire il processo decisionale sono di grande importanza. Come Jim McHale ha dimostrato, la quantità di dati che possono venire ricavati dagli edifici è in rapido aumento, dai 1.200 Terabytes di qualche anno fa ai 37.200 Terabytes previsti nel 2020. Questo sul fronte dell'acquisizione dei dati, mentre su quello della loro diffusione le aspettative di crescita sono altrettanto positive. Un numero sempre maggiore di persone si possono connettere a internet ed avere anche dispositivi connessi 24 ore tutti i giorni. Secondo una ricerca effettuata negli USA, nel 2020 ogni persona avrà in media 6,5 dispositivi IP.

È già disponibile una grande quantità di informazioni dagli edifici, che aumenterà ancora nel prossimo futuro. Tuttavia, come ha sottolineato Jim McHale, sarebbe un errore prendere l'edificio intelligente come unico punto di partenza per realizzare una città intelligente. Una 'Smart City' è fatta dalle persone, non dai sistemi.

La London Fire Brigade



Neil Orbell ha svolto la sua parte con una panoramica sulle sfide del servizio anti incendio, spiegando innanzitutto che la 'prevenzione' parte da una costruzione degli edifici eseguita in modo appropriato e dalla possibilità di poterne controllare l'ambiente interno, mentre la 'protezione' si concentra dalla difesa delle persone più vulnerabili.

Neil Orbell ha sottolineato che i pericoli che i vigili del fuoco devono affrontare stanno cambiando. Dal punto di vista del professionista dell'antincendio, anche piccoli eventi possono determinare gravi conseguenze sociali. Alcuni mesi fa, è scoppiato a Londra un incendio di vaste proporzioni ma controllabile: solo uno dei tanti, dal punto di vista dei vigili del fuoco. L'edificio è andato completamente distrutto, e ci sono voluti due giorni di lavoro per completare lo spegnimento. In realtà, l'incidente ha provocato un serie di effetti collaterali per la gente che vive e lavora a Londra. Per ragioni di sicurezza, è stata evacuata un'area dove vivevano 5000 persone, con la chiusura dei negozi, degli alberghi e dei pub e l'interruzione della distribuzione del gas. L'incendio ha danneggiato seriamente le infrastrutture di telecomunicazione della città e ci sono voluti diversi mesi prima che le cose tornassero alla normalità per gli abitanti (e le squadre di soccorso). Neil Orbell ha citato questo esempio per far comprendere la gravità dei danni economici derivante dagli incidenti. In altre parole: la città dev'essere molto resiliente per poter garantire la 'normalità'.

Le opportunità tecnologiche di una Smart City possono aiutare i servizi antincendio nella loro operatività per la sicurezza della comunità e nel loro ruolo di 'regolatori'. Essi possono ricavare maggiori benefici dalle connessioni e dalle collaborazioni, facendo leva sulla tecnologia, che può mettere a disposizione dei vigili del fuoco le informazioni necessarie sulle persone e gli edifici, ma permette anche il monitoraggio e l'accesso da remoto.

In conclusione, secondo Neil Orbell, la cosa fondamentale che i vigili del fuoco chiedono ai produttori di sistemi è la 'trasparenza' in termini di capability e capacity dei loro prodotti.

Olanda: la città di Rotterdam

Rotterdam è la seconda città olandese ed è sede del più grande porto europeo. 'The Hague', l'area urbana di Rotterdam, è al 168° posto nella classifica mondiale delle aree più abitate. Rotterdam è conosciuta per l'università Erasmus, la posizione lungo il fiume, la vita culturale e il patrimonio marittimo. La ricostruzione

**RUN
Milestone Mobile
AND DOCUMENT
ANY EVENT WHILE
IT HAPPENS**

**POSSIBLE
STARTS
HERE**



Lascia che le persone del tuo staff vedano il flusso video in diretta dal loro smartphone, ovunque si trovino

Consentendo al tuo personale di vedere il video live direttamente dalla telecamera alla tua soluzione Milestone, la app Milestone Mobile offre agli operatori della centrale di sorveglianza una immediata consapevolezza degli eventi, non importa dove si verifichino.

Compatibile con tutti i software di gestione video Milestone XProtect® e con la serie Milestone Husky™ NVR, la app Milestone Mobile fornisce una visione estesa in tempo reale e la capacità di utilizzare i flussi video nelle indagini successive.

Esplora tutte le opportunità di sorveglianza e di sicurezza con le soluzioni di gestione video Milestone a milestonesys.com

Milestone Systems Italy
Tel: +39 02 4979 2717



The open platform company

della città dopo la II guerra mondiale ha prodotto un paesaggio di architettura moderna con grattacieli, inusuali nelle città olandesi. **Nico Tillie** della Delft University è responsabile dell'implementazione a Rotterdam della **ISO 37120:2014** (Sviluppo sostenibile delle comunità) e della **ISO 37121** (Raccolta e revisione degli indicatori esistenti sullo sviluppo sostenibile e la resilienza nelle città). Le norme definiscono e indicano le metodologie per una serie di indicatori per individuare e misurare le prestazioni dei servizi urbani, la qualità della vita e la resilienza. Nico Tillie è stato coinvolto nello sviluppo e nella scrittura della prima norma internazionale sui City Data ISO 37120 dal TU Delft e dal Comune di Rotterdam. Per due anni, Rotterdam si è prestata come prima città pilota, ponendosi come obiettivo principale del progetto di Smart City la riduzione delle emissioni di anidride carbonica. A seguito di questa esperienza, Tillie ha compreso che è necessario pensare in termini di 'evoluzione' e non di 'rivoluzione', essendo praticamente impossibile mettere a fuoco tutti i temi riguardanti una 'Smart City', che è un percorso in crescita progressiva. Prima di partire con un progetto di 'Smart City', è necessario realizzare una tabella di marcia con la struttura del programma.

Una delle prime lezioni acquisite è stato il 'data flow'. E' disponibile una grande quantità di dati, ma un dato non è la stessa cosa di un'informazione. La selezione dei dati diretti ai gruppi di lavoro è la prima tappa. Una seconda tappa è l'aumento del valore delle informazioni: la presentazione dei dati agli stakeholders è stata la parte difficile del lavoro. All'inizio, i dati venivano presentati come 'spreadsheet-look-alike', senza ottenere molto successo. Ora l'informazione è invece presentata su mappe, in modo dedicato ai diversi gruppi di lavoro. Combinando la selezione con le modalità di presentazione, è stato realmente aggiunto valore all'informazione. L'ultima lezione che Nico Tillie ha condiviso con i partecipanti è di non pensare di poter realizzare una città intelligente 'stando in una torre d'avorio'. Per riuscire a realizzare un progetto di Smart City è più importante dedicare molto tempo nei rapporti con gli stakeholders, facendoli diventare 'ambasciatori' del progetto di città intelligente. Dopo i primi risultati positivi ottenuti da Rotterdam come città pilota nell'implementazione della ISO 37120 avendo Nico Tillie come capo-progetto, molte altre nazioni e metropoli si sono interessate al progetto. Allo stato attuale, circa 20 città nel mondo stanno partecipando a gruppi di lavoro per realizzare città intelligenti e resilienti.



BIM (Building Information Modelling)

Spiegato da **Jim Glockling**, l'attuale progetto europeo per la sicurezza antincendio appare in realtà poca cosa. I regolamenti si focalizzano sugli incendi e sugli altri incidenti che possono avvenire all'INTERNO di un edificio ma non prendono in considerazione gli INCENDI ESTERNI che possono coinvolgere l'edificio. I regolamenti non prendono nemmeno in considerazione la resilienza e gli effetti dal punto di vista economico.

Neil Orbell (London Fire Brigade) ha pienamente condiviso questa affermazione, collegando alcuni incidenti avvenuti di recente a Londra. Jim Glockling ha parlato di Smart Cities e di Building Information Modelling (BIM), che è un sistema di progettazione virtuale di edifici fino al collaudo e alla sperimentazione, prima che qualsiasi cosa venga fisicamente costruita. Jim Glockling ha sviluppato il BIM, nel quale viene descritto ogni prodotto utilizzato in un edificio, per offrire la possibilità di lavorare con un approccio più evoluto alla protezione contro gli incendi. Ha continuato parlando della sicurezza nei

regolamenti degli edifici, che stabiliscono quello che i responsabili devono fare in caso di evacuazione, ma nulla dicono su quanto deve venire fatto quando l'evacuazione è completata. L'attenzione è di solito rivolta alla sostenibilità che, attualmente, si ottiene a scapito della resilienza. Secondo Jim Glockling, ottenere entrambe non è difficile, perché tutto deriva dalla scelta dei materiali.

Ha continuato l'intervento parlando delle responsabilità che dovrebbero venir prese in considerazione in ogni analisi di 'Smart City'. Ha citato diversi titoli di giornali che segnalavano che negli ultimi 18 mesi almeno l'80% delle imprese è stato coinvolto in incidenti gravi, arrivando alla conclusione che queste aziende sono state gestite in modo incompetente per tutti i 18 mesi. Tutto questo riporta a un corretto piano di Business Continuity. Il Building Information Modelling (BIM) può contribuire a questo. BIM stabilisce quali devono essere i materiali da costruzione e i sistemi dell'edificio, dove si trovano e quali sono le caratteristiche fisiche. Si può raggiungere la conformità raccogliendo e analizzando queste informazioni ma, oltre a verificare la sostenibilità, questo metodo può anche venire usato per determinare un 'Resilience Rating' per ogni edificio. Questo renderebbe la resilienza un criterio di selezione accessibile e determinante nella scelta dei materiali e nella progettazione degli edifici del futuro.

Conclusioni

La conferenza organizzata da Euralarm durante la fiera IFSEC a Londra il 17 giugno ha spiegato ai partecipanti che il focus della progettazione futura non dovrebbe essere rivolto alle tecniche ma alla resilienza. Tuttavia, anche se un gruppo di edifici 'intelligenti' non è sufficiente per realizzare un progetto di Smart City, le tecniche e la gestione dell'informazione potrebbero essere di importanza cruciale per consolidare il processo di creazione di comunità 'sicure'. Assumendo il dato che ogni settimana circa 1,3 milione di persone migra verso le città, è incontestabile che i governi debbano tenere la sicurezza urbana in cima alla lista delle loro priorità. Facendo leva sull'ubiquità degli smartphone e sull'Internet delle Cose, si potrà assicurare la sicurezza del 60% dell'umanità che nel 2030 vivrà nelle metropoli. In ogni caso, la sicurezza non è il primo motivo per cui la gente abita in città: la qualità della vita è la spinta principale ad andarci. Le città percepite come 'intelligenti' e 'sicure' tendono ad attrarre più investimenti, così come le persone più 'brillanti' e di reddito superiore sono più propense a abitarci e lavorarci. Detto questo, safety e security non sono il fine ultimo, ma un mezzo per raggiungere obiettivi superiori. Per la loro conquista, dovranno venire coinvolti tutti gli stakeholders e l'attenzione globale dovrà venire rivolta alla 'resilienza'.

Chi è Euralarm

Euralarm rappresenta i produttori di sistema di sicurezza e antincendio, offrendo guida e competenze per l'industria, il mercato, i decisori politici e l'attività normativa. I membri di Euralarm operano per una società più sicura realizzando sistemi e servizi antincendio, antintrusione, controllo accessi, videosorveglianza, trasmissione di allarmi e centrali di ricezione. Fondata nel 1970, Euralarm rappresenta oltre 5000 aziende, con un fatturato complessivo stimato in 18 miliardi di euro. I membri sono associazioni e aziende singole di oltre 17 paesi europei.



CONTATTI - EURALARM
pressoffice@euralarm.org
Tel. +31 (0)7 0427 5200

Le Eccellenze per la Sicurezza, un confronto tra esperti sul futuro della sicurezza fisica

di Raffaello Juvara

Il progetto è partito alla fine del 2014, chiacchierando con il ceo di una delle aziende produttrici di tecnologie di sicurezza più innovative che operano in Italia: "Perché non organizzate un seminario rivolto ai decisori dei più importanti utilizzatori, per fare il punto della situazione sul futuro della sicurezza fisica? - mi ha chiesto - Fino ad ora sono state utilizzate solo tecnologie sviluppate altrove, ma stanno nascendo soluzioni originarie che modificheranno i criteri di progettazione dei sistemi di sicurezza. Chi decide gli acquisti deve sapere adesso cosa succederà domani. D'altra parte, con lo IoT cambieranno tante di quelle cose che sarebbe utile per tutti capire dove stiamo andando, per poterci preparare in tempo". Come non accettare una sfida simile, mentre ogni giorno arrivano segnali di tendenze fondamentali, assieme a notizie praticamente da tutti gli angoli del pianeta sicurezza, che fanno capire che tutto sta cambiando per davvero? Solo per fare qualche esempio: a. lo sviluppo della definizione delle immagini e della video-analisi, assieme all'utilizzo dei **metadata**, sta modificando le nozioni di base della videosorveglianza, con le telecamere che diventano sensori sia di sicurezza che di **metasecurezza** con impieghi nei campi più disparati (business intelligence, controllo dei processi industriali, gaming, sport, medicina, protezione civile ecc); b. mentre **Symantec** annuncia di aver superato il primo miliardo di dispositivi IoT protetti da attacchi informatici (fra i quali gli ATM di **Wincor Nixdorf**), **Per Björkdahl**, chairman di **ONVIF**, ha spiegato in un'intervista rilasciata a **essecome** (in questo numero a pag. 8) che la crescita

a due cifre del mercato della sicurezza fisica di questi anni è dovuto anche al fatto che "numerose organizzazioni pubbliche e private sono spinte a proteggere l'accesso fisico a postazioni di lavoro, centrali operative e server room che trattano o ospitano dati sensibili o registrazioni video; molti ritengono che la sicurezza fisica di queste strutture sia importante quanto la crittografia e altre forme di cyber security";

c. **Euralarm**, l'associazione europea dei fabbricanti di sistemi di sicurezza e antincendio, sta dedicando la massima attenzione al tema della sicurezza e della resilienza del concept **Smart City**, contenitore e contenuto di ogni tecnologia per la protezione delle persone, delle Infrastrutture Critiche, delle cose;

d. Ma **Smart City** è anche il paradigma di **Business Continuity**, la disciplina che si sta affermando all'apice della gerarchia delle organizzazioni, alle quali deve garantire "l'assenza di pericoli" (ovvero la sicurezza) che possano interrompere il normale funzionamento...

Abbastanza argomenti per organizzare un incontro a porte chiuse tra top security manager delle maggiori organizzazioni pubbliche e private, esperti di caratura internazionale come **Gianna Detoni**, **Frediano Di Carlo** e **Giuseppe Mastromattei**, e un gruppo selezionato di produttori all'avanguardia nelle rispettive tecnologie (**Axitea**, **ISEO**, **Microntel**, **Mirasys**, **Samsung Techwin**, **TSec**) per un confronto sull'esistente e sul futuro della sicurezza fisica, nella straordinaria sede delle **Gallerie d'Italia Piazza Scala** (Milano, 21 settembre 2015).



Gianna Detoni



Frediano Di Carlo



Giuseppe Mastromattei

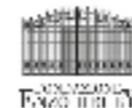

Gallerie d'Italia Piazza Scala Milano
21 settembre 2015

LE ECCELLENZE PER LA SICUREZZA

PARTNER



In collaborazione con:



Il cambiamento che sta attraversando il Mondo della Sicurezza coinvolge l'intera filiera degli Operatori Professionali: produttori, progettisti, systems integrators e gestori, e ogni categoria di Utilizzatori: banche, infrastrutture critiche, impianti industriali, catena della distribuzione, pubblica amministrazione. Di fronte alla caduta del confine tra Sicurezza Fisica e Sicurezza Logica e alle possibilità offerte dall'evoluzione tecnologica di condividere infrastrutture e servizi con centri di costo diversi dalla Security aziendale, le scelte dei Decisori sono quanto mai determinanti per la tutela degli investimenti in Sicurezza e della loro capacità di produrre ROE nel tempo.

Le Eccellenze per la Sicurezza, seminario a inviti riservato ai Responsabili della Sicurezza dei maggiori Utilizzatori, propone un momento di confronto e di riflessione per analizzare le principali tendenze che definiscono questo cambiamento a livello globale, assieme a esperti di caratura internazionale e ai rappresentanti di sei produttori di tecnologie e di servizi accomunati dal massimo livello di innovazione nei rispettivi ambiti di specializzazione.

Una straordinaria ed esclusiva occasione di conoscenza e di approfondimento, in una cornice altrettanto straordinaria come le Gallerie d'Italia Piazza Scala a Milano.





Gallerie d'Italia Piazza Scala Milano
21 settembre 2015

LE ECCELLENZE PER LA SICUREZZA

PROGRAMMA

- | | |
|--|--|
| <p>14:30 Presentazione del seminario
Raffaello Juvara - Direttore esecome</p> <p>14:40 La nuova sicurezza dell'edificio
Presentazione a cura di
TSEC - ISEO - MICRONTEL</p> <p>15:20 Security & Business Continuity
Gianna Detoni
(Business Continuity Institute)</p> <p>15:35 Utenti globali, sicurezza globale
Tavola rotonda con:
Jerome Bertrume (Guess Europe),
Gianna Detoni (BCI),
Pier Luigi Martusciello (BNL Paribas),
Corrado Miralli (Saipem),
Tommaso Profeta (Finmeccanica).
Conduce Raffaello Juvara</p> <p>16:20 Coffee break</p> | <p>16:50 Cosa sono i Metadata
Frediano Di Carlo (analista free lance)</p> <p>17:05 Video: sorveglianza e intelligenza
Presentazione a cura di
Samsung - Mirasys - Axitea</p> <p>17:45 L'evoluzione del Security Management
Giuseppe Mastromattei (H&M)</p> <p>18:00 Sicurezza fisica vs sicurezza logica
Tavola rotonda con:
Maurizio Tondi (Axitea),
Claudio Clerici (ISEO Serrature),
Giuseppe Migliasso (Microntel),
Elio Argenti (Mirasys),
Francesco Paradiso (Samsung Techwin),
Giordano Turati (TSec).
Conduce Maurizio Callegari (HESA spa)</p> <p>18:30 Visita guidata alle Gallerie d'Italia</p> <p>19:15 Cocktail party</p> |
|--|--|

PARTNER



In collaborazione con:



BARRIERE A RAGGI INFRAROSSI
CODIFICATI

Serie Smart Line™

Semplicemente perfette

- FASCIO A RAGGI INFRAROSSI DI TIPO QUAD
- RIDUZIONE DEI FALSI ALLARMI
- TECNOLOGIA DI PROTEZIONE DALLA LUCE SOLARE
- CIRCUITO INNOVATIVO DI ALLINEAMENTO AUTOMATICO DEL FASCIO
- A.T.P.C. - CONTROLLO AUTOMATICO DELLA POTENZA TRASMESSA



HESA S.p.A.
Via Triboniano, 25 - 20156 MILANO
tel +3902380361 - fax +390238036701
hesa@hesa.com - www.hesa.com

I PROTAGONISTI



AXITEA SpA

Axitea SpA rappresenta la sintesi di molteplici conoscenze, competenze ed esperienze sviluppate in ambito Vigilanza e Sicurezza dal 1914 ad oggi, ed arricchite nel tempo sia nel rafforzamento dell'attività di presidio del territorio e di gestione proattiva degli allarmi e degli interventi, sia attraverso lo sviluppo di competenze specialistiche nella progettazione, realizzazione, integrazione, manutenzione e gestione di piattaforme e soluzioni tecnologiche dedicate alla sicurezza fisica, al controllo accessi, alla videosorveglianza, al monitoraggio satellitare ed alla protezione di infrastrutture ICT.

Oggi Axitea esercita il ruolo chiave di **Global Security Provider** – operando nel virtuoso incrocio tra tecnologie innovative, servizi end-2-end, processi ed organizzazione – all'interno di un mercato in forte trasformazione, anche per la convergenza tra informatica, telecomunicazioni, controlli, automazione e Internet of Things. Questo origina non solo un nuovo segmento di mercato, ma un complesso e articolato "sistema di impresa" da proteggere, monitorare e far evolvere con continuità operativa in termini di asset, infrastrutture critiche, dati, informazioni e persone.

L'aumentato bisogno di Sicurezza Integrata da parte di aziende pubbliche e private in ogni settore merceologico e per ogni dimensione impone, da un lato, una risposta puntuale in termini di competenze specialistiche, mappate sulle più innovative tecnologie della sicurezza e sui punti di vulnerabilità del sistema di business dell'impresa; dall'altro, una visione più ampia ed articolata in grado di mettere a disposizione del mercato un "single point of contact" che possa fornire soluzioni complete al cliente, che spaziano dalla manutenzione multi tecnologia alla gestione integrata di eventi, allarmi ed interventi, in ogni ambito attraversato dal nuovo bisogno di sicurezza e protezione: impianti tecnologici, sistemi di controllo ed automazione, sistemi di sicurezza fisica, infrastrutture ICT e cyber security.

Attacchi hacker, malfunzionamenti, guasti, incidenti, errori umani, eventi atmosferici: uno scenario dai risvolti anche inquietanti che evidenzia l'attualità di una visione ed un'attenzione sempre più irrinunciabile alla sicurezza delle cose e delle persone, al controllo delle operazioni, alla programmazione delle attività di manutenzione, alla necessità di analisi e correlazione di dati, informazioni ed eventi per comprendere velocemente la "situazione", per reagire con efficacia alle emergenze e per prevenire, fino dove possibile, il verificarsi di situazioni di rischio. Piani per la Continuità Operativa delle aziende a supporto di eventi o incidenti che ne minano la sopravvivenza; piattaforme software evolute ed innovative in grado di analizzare dati ed informazioni cruciali, in tempo reale; programmare e coordinare le attività di manutenzione; automatizzare attività ricorrenti; definire le procedure standard di intervento in contesti mission critical come gli aeroporti, i porti, le banche, le centrali di telecomunicazioni e di distribuzione dell'energia elettrica.

Una visione ed una proposizione su cui Axitea è impegnata in termini di risorse, competenze, accordi tecnologici, definizione dei servizi per supportare le aziende italiane, ad ogni livello, nella creazione e poi nel mantenimento durante l'intero ciclo di vita, di un solido "impianto" di sicurezza che integri le migliori tecnologie e le procedure

SERVIZI DI SICUREZZA AXITEA

INTERVENTO SU ALLARME



LOCALIZZAZIONE E MONITORAGGIO ALLARME SATELLITARE



LOGISTICA SATELLITARE



MANUTENZIONE E ASSISTENZA TECNICA



MANUTENZIONE E ASSISTENZA TECNICA RETI INFORMATICHE



MONITORAGGIO ALLARME



MONITORAGGIO RETI INFORMATICHE



PATTUGLIAMENTO



PIANTONAMENTO



PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI RILEVAZIONE INTRUSIONE



PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI ALLARME GAS E INCENDIO



PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI CONTROLLO ACCESSI



PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI VIDEOCONTROLLO



PROGETTAZIONE E REALIZZAZIONE DI SISTEMI DI SICUREZZA PER LE RETI INFORMATICHE



TELEGESTIONE DI SISTEMI



VIDEOALLARME



VIDEOSORVEGLIANZA



GUARDIA VIRTUALE





operative più personalizzate. Nell'ambito della Sicurezza Integrata, così come in quello della collaborazione di impresa, il **video** rappresenta oggi un'applicazione di straordinaria potenzialità per la gestione real time di situazioni di pericolo o per la prevenzione, oltre che per l'analisi forense di eventi criminosi. In questo contesto in forte evoluzione, soluzioni di video analisi innovative in grado di correlare con precisione gli eventi, ridurre o eliminare i falsi positivi, gestire flussi di immagini ad alta definizione ma anche di integrare soluzioni analogiche in campo, rappresentano una piattaforma cruciale per la sicurezza. Tale piattaforma, arricchita da algoritmi software sofisticati, non solo eleva il livello di protezione e l'efficacia dell'intervento, ma abilita l'analisi di marketing per il potenziamento delle attività di vendita ed il miglioramento del sistema di ingaggio con il cliente e il consumatore. La proposizione di Axitea, come Global Security Provider, può fornire una risposta efficiente ad un bisogno integrato che prevede l'utilizzo di piattaforme software fortemente personalizzabili, in termini di esperienza d'uso e funzionalità, ma altamente interoperabili per garantire l'integrazione con tecnologie legacy ed un percorso di evoluzione scalabile. Un esempio è rappresentato dalle soluzioni più moderne di Situation Management a supporto degli operatori specializzati nella gestione di situazioni di emergenza anche correlate al CERT (Computer Emergency Response Team) che soprassedie alla sicurezza informatica ed alla cyber security. I punti di controllo non sono più solo quelli tradizionali e la diffusione e l'applicazione dell'IoT è sempre più in crescita; tale fenomeno da un lato incrementa il livello di distribuzione, di accesso, fruizione ed interazione tra informazioni, sistemi ed utenti; dall'altro, se non controllato, rappresenta un ulteriore potenziale punto di vulnerabilità ed amplificazione del rischio. Attraverso l'attività professionale e l'utilizzo di tecnologie innovative, Axitea fornisce una soluzione integrata, programmabile e interoperabile per la sicurezza trasversale di tutti questi ambiti.

Axitea mette a disposizione oggi le proprie competenze e risorse per la sicurezza e la protezione delle infrastrutture mission critical, per contribuire a realizzare, sostenere e far evolvere la protezione di aziende private e pubbliche. La visione e la realizzazione di una propria architettura di servizi e soluzioni dedicate alla continuità operativa delle imprese, comprende risk assessment, disaster recovery, la creazione di un piano di continuità operativa e la disponibilità di risorse specializzate, incluse quelle impegnate nell'ambito della vigilanza per la prevenzioni dello sciaccallaggio ed eventi predatori a seguito di calamità naturali, incidenti e crisi.

I PROTAGONISTI


LE ECCELLENZE PER LA SICUREZZA

ISEO Serrature SpA

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.

APERTURA CON IPHONE

Grazie alla tecnologia Bluetooth Smart, da oggi anche iPhone può interagire con tutti i dispositivi di controllo accessi della serie Smart, senza alcun bisogno di hardware aggiuntivi. Grazie all'App gratuita Argo, ogni telefono Bluetooth Smart Ready (iOS o Android) può essere abilitato all'apertura della porta.

APERTURA DA REMOTO

La tecnologia Bluetooth Smart consente di utilizzare qualsiasi smartphone come controllo remoto di apertura della porta fino ad una distanza di 10 metri.



GESTIONE DELLA LISTA UTENTI

Con l'App Argo, l'amministratore può gestire le autorizzazioni all'accesso dei vari utenti in modo intuitivo e senza il bisogno di alcun software aggiuntivo o connessione internet. È possibile aggiungere, cancellare o modificare le autorizzazioni fino a 300 utenti. La lista degli utenti, inoltre, può essere trasferita da una porta all'altra.

LETTURA DELLO STORICO DEGLI EVENTI

L'amministratore può consultare lo storico degli ultimi 1000 eventi rilevati su ogni porta, e inviare il report via e-mail.

AGGIORNAMENTI SOFTWARE GRATUITI

Gli aggiornamenti del software dei dispositivi di controllo accesso sono gratuiti e garantiscono la migliore performance alla porta. Lo smartphone segnala con una notifica quando viene reso disponibile un aggiornamento, e l'installazione del nuovo software sul prodotto verrà effettuata direttamente dallo smartphone.

In questo modo, ogni utente potrà continuamente usufruire di nuove funzionalità del sistema, salvaguardando pertanto l'investimento effettuato con i prodotti elettronici ISEO Zero1.

Con i sistemi elettronici di controllo accessi della serie Smart, possono essere utilizzate diverse credenziali di apertura: tessere ISEO, tessere e tag MIFARE e tutti gli smartphone con tecnologia NFC e Bluetooth Smart.

L'app Argo si presta per diversi tipi di installazioni.

È la soluzione ideale per **HOTEL E BED & BREAKFAST**, dove i clienti possono accedere alle loro camere tramite il loro smartphone: in questo modo, non c'è più il rischio di chiavi rubate o perse. Inoltre, gli accessi alle camere tramite smartphone possono facilmente essere gestiti a seconda delle date di check-in e check-out.

Per **UFFICI, NEGOZI, AZIENDE E STUDI PROFESSIONALI**, l'amministratore può consentire l'accesso ai locali riservati solo a persone selezionate, anche per periodi prestabiliti, e cambiare le autorizzazioni quando serve. Inoltre, può controllare chi, dove e quando è entrato (fino agli ultimi 1000 accessi), per una maggiore sicurezza, e organizzare fino a 300 autorizzazioni di utenti.

L'app Argo è la soluzione ideale anche per le **ABITAZIONI PRIVATE** non solo per la sicurezza, ma anche per il comfort: è, infatti, possibile aprire la porta anche da una distanza di 10 metri. Quando si è fuori casa, è possibile autorizzare l'entrata di parenti e collaboratori esterni (giardiniere, colf, etc.) ed è possibile controllare i tentativi di apertura non autorizzati.

PRODOTTI COMPATIBILI

La gamma di prodotti compatibili con l'app Argo comprende non solo il cilindro elettronico Libra Smart, ma anche la maniglia elettronica Aries Smart, la serratura per porte blindate x1R Smart e il lettore di credenziali Stylos Smart, che fanno parte della nuova linea ISEO Zero1 – Electronic Solutions. Si tratta di una nuova linea di prodotti e soluzioni del gruppo ISEO, che racchiude in sé tutti i prodotti più innovativi dal punto di vista della sicurezza e del controllo degli accessi.

Tutti i prodotti ISEO Zero1 si caratterizzano per l'alto contenuto tecnologico dei loro componenti e permettono di gestire in modo flessibile ed intelligente gli accessi, garantendo in ogni momento massima affidabilità e sicurezza.

La microelettronica, applicata alla sicurezza, fornisce un'alternativa alla chiave tradizionale, mentre il design elegante e minimale, unito alle diverse finiture disponibili, permette l'integrazione dei dispositivi in ogni tipo di ambiente, da classico a moderno. Libra, inoltre, è stato selezionato da ADI Design Index 2013 ed ha ottenuto la Menzione d'Onore nell'ambito della XXIII Edizione del premio Compasso d'Oro.

iseo.com

ISEO®

LA MIA
CHIAVE È
SMART.



.....
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



I PROTAGONISTI



LE ECCELLENZE PER LA SICUREZZA

Microntel SpA

Per la realizzazione di edifici sempre più sicuri, **Microntel** si propone tra i principali attori nello scenario dell'innovazione tecnologica, con un'offerta di soluzioni per il controllo accessi complete ed integrabili con l'intera infrastruttura di qualsiasi tipologia di edificio, per fornire soluzioni concrete alle più diversificate esigenze progettuali di sicurezza.

Innovazione ed evoluzione tecnologica costituiscono i principi cardine sui quali Microntel ha costruito la propria proposta per il controllo accessi, per rispondere al mercato della sicurezza che richiede sempre maggiore flessibilità, scalabilità ed interoperabilità tra i sistemi, per ottenere il massimo livello di protezione dell'edificio, dalla identificazione e gestione dei transiti alla organizzazione degli spazi in funzione dei livelli d'accesso.

La modularità delle soluzioni offerte, con un hardware ed un software interamente progettati e realizzati dall'R&D di Microntel, consente di risolvere dalle più semplici esigenze di tipo "stand alone", alle richieste più articolate, basate su architetture complesse e con elevato grado di integrazione con funzionalità ausiliarie.

Le soluzioni di controllo accessi di Microntel sono progettate per interagire con gli altri sistemi di sicurezza e di gestione dell'edificio, realizzando quindi integrazioni efficaci e personalizzate con sistemi sia di Risk Management, sia di Building Management.

Per il controllo accessi e sicurezza, Microntel ha progettato **MicronPass®**, soluzione software totalmente web, dinamica e flessibile per assicurare la massima protezione e sicurezza del Building.

MicronPass® nasce come strumento di definizione delle regole di accesso alle aree da controllare, fornisce in tempo reale la situazione del personale presente negli edifici, effettua il monitoraggio completo dei varchi e produce una vasta reportistica riepilogativa degli eventi rilevati.

La versatilità di MicronPass® consente di gestire il controllo accessi in diverse modalità in funzione delle esigenze infrastrutturali, del livello di sicurezza richiesto e della tipologia di varco da controllare.

Microntel offre una soluzione disponibile in versioni alternative ed al tempo stesso complementari "On-line Realtime" ed "Off-line", per fornire una risposta completa e tecnologicamente avanzata nell'ambito del controllo accessi.

Una soluzione On-line è particolarmente indicata per risolvere esigenze di sicurezza in termini di:

- disponibilità in tempo reale della lista dei presenti in area in caso di emergenza/evacuazione;
- controllo delle aree critiche con porte allarmate;
- acquisizione streaming video di aree sensibili a fronte di un certo evento.

Una soluzione Off-line invece è maggiormente indicata per varchi da controllare difficilmente raggiungibili dall'infrastruttura di rete aziendale, come ad esempio aree decentrate ed anche in tutte quelle condizioni ambientali dove l'alimentazione elettrica o la rete dati potrebbero risultare un limite di infrastruttura.



Nessuno passa inosservato

SISTEMI DI CONTROLLO ACCESSI
RILEVAZIONE PRESENZE DEL PERSONALE
RACCOLTA DATI DI PRODUZIONE



MICRONTEL

MICRONTEL S.p.A.
Via G. Reiss Romoli, 147
10148 Torino (TO)
Tel. 011 2234811
www.microntel.com

La soluzione MicronPass® è composta da:

1. una componente hardware che, in base al tipo di applicazione, è costituita da:

- Dispositivi On-Line su rete ethernet: centraline/controllori di varco con una vasta gamma di lettori Rfid Biometrici/Banda magnetica;
- Dispositivi Off-line: cilindro, placca maniglia elettronici Rfid, cilindro mecatronico con chiavi elettroniche. I dispositivi Off-line elettronici e mecatronici sono installabili senza collegamenti elettrici e funzionanti con batteria;

2. una componente di identificazione utente, costituita da dispositivi con tecnologia NFC/Bluetooth, badge, codici, chiavi elettroniche o credenziali dirette (biometria);

3. un sistema di acquisizione e comunicazione dati:

- MicronService® OnLine per una comunicazione Realtime tra l'applicativo utente MicronPass® e i dispositivi raggiungibili sulla rete Ethernet;
- MicronService® OffLine per una comunicazione tra l'applicativo utente MicronPass® e il sistema di programmazione badge ed acquisizione delle transazioni memorizzate sul chip del badge;

4. una procedura di controllo accessi totalmente via WEB: MicronPass® WEB, piattaforma altamente performante ed unica in grado di gestire sia varchi on-line che varchi off-line.

Entrambe le applicazioni in versione On-Line Realtime e Off-line possono essere operative nell'ambito dello stesso sistema di controllo accessi.



MicronPass® è un sistema totalmente scalabile, una soluzione ottimale sia per impianti di medie dimensioni, sia per impianti con migliaia di varchi, in uno o più siti, geograficamente distribuiti in diversi paesi o continenti.

Numerosi moduli opzionali ed articolati sottosistemi completano la soluzione MicronPass®: Gestione Aziende Esterne, completa di Gestione Documentale, Gestione Visitatori di agevole utilizzo per il Personale di Reception, Gestione Visualizzazione Transiti per il controllo immediato del varco da qualsiasi postazione di lavoro, Gestione Turni con abilitazioni di accesso abbinate agli orari di lavoro, Riconoscimento Targhe per la gestione integrata anche con il varco carraio, Generazione ed Invio automatico di Report di notifica sullo stato impianto, su allarmi o altri eventi, parametrabili a scelta dell'utente.

Le molteplici applicazioni realizzate per prestigiose realtà in contesti diversificati, nella pluri-decennale esperienza di Microntel, rendono MicronPass® una risposta innovativa ed efficace ad ogni esigenza di controllo accessi, consentendo, oltre all'incremento del livello di protezione dell'edificio ed alla gestione organizzata del varco, di fruire di ulteriori significativi vantaggi che vanno dall'impiego più razionale del personale con conseguente economia di esercizio, alla integrazione ed interoperabilità con gli altri sistemi di sicurezza, a garanzia degli investimenti effettuati e della continuità del servizio.

I PROTAGONISTI



Mirasys Ltd

Mirasys Ltd è un'azienda finlandese con sede ad Helsinki. Fin dall'inizio, Mirasys ha sempre avuto il fine di essere un'azienda multinazionale. Ha iniziato le sue attività nel 1997 a Helsinki come azienda specializzata nella sorveglianza in ambito bancario, dietro richiesta dell'Associazione Bancaria Finlandese, e si è evoluta da subito nell'ambito IP, intuendo la grandi potenzialità del mercato di questa tecnologia.

Mirasys ha uffici di vendita in oltre 40 paesi europei e nel mondo, con oltre 50.000 clienti worldwide. Le videocamere attualmente connesse ai sistemi Mirasys sono circa un milione, e la società lavora con oltre 500 Partner e Distributori. Il software Mirasys supporta in modo nativo oltre 2200 modelli di telecamere IP delle maggiori case costruttrici e, praticamente, tutte le telecamere analogiche.

Mirasys è presente in Italia dal 2010, sia con la vendita che con il supporto. La presenza locale del supporto è considerata fondamentale, soprattutto per installazioni di una certa dimensione. La struttura italiana permette quindi un interfacciamento tra l'utenza locale e le strutture di Mirasys in Finlandia, in caso di esigenze sia di natura commerciale che tecnica.

LA SOLUZIONE

Poiché gli scenari stanno variando, diventerà sempre più probabile la convivenza in ambito aziendale tra Sicurezza Fisica e Sicurezza Informatica. Per fare fronte a questa nuova necessità, anche il mercato si sta preparando a dare risposte sempre più integrate, al fine di permettere al management di prendere decisioni corrette.

Mantenendo la sua caratteristica di Sistema Aperto in ambito VMS, Mirasys tende ad avere un'attenzione sempre più focalizzata sulle soluzioni, anziché sui singoli prodotti. Questo significa avere maggiori possibilità di integrare o di integrarsi con altre soluzioni. Noi forniamo principalmente sistemi per applicazioni corporate multisito in progetti su larga scala, disponendo di un vasto ecosistema di partner: infatti collaboriamo direttamente con tutti i principali produttori di telecamere, di sistemi di analisi video e di controllo accessi, gli integratori di sistemi, ed i fornitori di servizi di sicurezza. Noi crediamo che la partnership con altre aziende sia il modo per fornire soluzioni che soddisfano qualsiasi specifica esigenza.

I PRODOTTI

Mirasys VMS Enterprise è la base per passare da prodotto a soluzione. Infatti, utilizzando il sistema VMS Enterprise come base, è possibile integrare soluzioni di VCA (analisi video), AVM (video wall), ANPR+ (lettura targhe), FailOver ed altre funzionalità come Reporting e Server Expansion. Il software Mirasys è quindi, come detto in precedenza, pronto sia per essere utilizzato come singolo prodotto, sia per essere utilizzato in ambito di soluzioni complete. Spesso, durante la vita di un sistema di sorveglianza, ogni azienda deve affrontare diversi cambiamenti operativi riguardanti l'ambito della sicurezza, come l'utilizzo di outsourcing, l'aumento delle proprie sedi, l'integrazione con sistemi di sicurezza, o la necessità di centralizzazione. Quindi, in caso di modifiche



operative, una buona soluzione iniziale fa la differenza tra l'acquisto di un nuovo sistema e l'ampliamento di uno già esistente.

Mirasys VMS Enterprise è la soluzione perfetta per le aziende e centri di sicurezza di qualsiasi dimensione. Estremamente flessibile e personalizzabile, può adattarsi a qualsiasi soluzione di sorveglianza. In aggiunta alla sua estrema adattabilità, la filosofia progettuale alla base di VMS Enterprise è sempre stata la facilità d'uso, rendendolo un sistema intuitivo, veloce da implementare e da utilizzare. Inoltre, l'estrema scalabilità di Mirasys VMS Enterprise permette di gestire centinaia di utenti, così come di server VMS.

La forza della soluzione Mirasys è nella sua aperta modularità. Ciascun server può agire in modo indipendente, o come parte di una rete di server controllata da un server principale - o entrambi contemporaneamente. Tutte le nostre soluzioni sono intrinsecamente modulari.

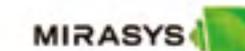
STRATEGIA DI MERCATO

In Italia, Mirasys collabora con Partner o OEM che sono in pratica System Integrator ad alto valore aggiunto. Tale strategia permette al Cliente finale di avere la migliore soluzione per le proprie esigenze. Per quanto riguarda quindi il mercato italiano, e proprio a causa della particolarità delle soluzioni richieste, Mirasys è orientata da tempo a collaborare con System Integrator che adottino e propongano soluzioni Enterprise ai loro clienti, fino ad arrivare a soluzioni ad alto livello di integrazione, che comprendano molteplici campi del settore PSIM, come ad esempio il controllo degli accessi ed i sistemi di allarme ed anti intrusione, ma anche il Building Management ed il controllo del traffico.

Per poter fornire la gestione ottimale di una soluzione complessa, è necessario assicurare al Cliente finale una catena di elementi fondamentali, quali sono la conoscenza del prodotto, la consulenza sui progetti, il Supporto tecnico ed il training, oltre al contatto diretto con la produzione. Sicuramente un valore aggiunto è rappresentato dalla presenza locale, che può mettere a disposizione dei Partner, e quindi dei Clienti finali, i necessari elementi di queste strutture.



Open Architecture Video Management System



Open Awareness Hardware Integration

- Cameras and Command Center Hardware
- IP cameras, cameras new & legacy camera technology
- Encoders Cameras Box, Fixed Dome, Megapixel, High Definition Camera technology
- Popular brands include AXIS, Sony, Bosch, Samsung, Panasonic, Vivitek, Mobotix, etc.
- Networking Infrastructure: NVR, DVR and other legacy systems;
- Hi-Speed network availability

Open Awareness Access Control Technology

- Integration with Access Control via biometric identification & authentication
- Federated view to all access controls; Intruder alarming, fire systems, help points
- System acts as "single source of truth"
- Detection of explosives, weapons, drugs, dangerous goods (CBRN), platforms
- Intruder / Fire Detection and proactive alarming Hazard awareness hardware
- CNRE Nuclear, Bio Hazard detection technology



Open Video Content Analysis Integration

- Intelligent Algorithms technology camera or server based
- Metadata powered Smart Search
- Audio-video analytics powered alerting/forensics
- Examples include:
 - Automatic number plate recognition; illegal parking
 - Crowd monitoring static/dynamic object recognition
 - Anti-vandalizing and alerting in zones of interest

Window into various Industry Applications

- Critical infrastructure protection:
 - Airports, ports, maritime, homeland
- Building Management systems
- Retail experience enhancement, loss prevention
- Banking ATM, Power Utilities
- Education

Collaborative Risk Management: A Continuous Loop

- Risk management program, process and organization is integrated
- Risk assessment and response models, for complex or integrated infrastructure and services
- Threat assessment modelling
- Sophisticated risk calculator

I PROTAGONISTI



LE ECCELLENZE PER LA SICUREZZA

Samsung Techwin Europe Ltd

VIDEOSORVEGLIANZA OPEN PLATFORM: DA CENTRO DI COSTO A BUSINESS TOOL

L'evoluzione della tecnologia di ripresa e di compressione video, ha portato anche la VideoSorveglianza a considerare immagini con risoluzione HD, FullHD e 4K.

Diventa tuttavia riduttivo pensare che, con le nuove tecnologie, l'unico vantaggio sia quello di avere immagini live o registrate con una risoluzione maggiore, e non considerare la possibilità di applicazioni e funzionalità diverse ed innovative. L'aumento di qualità video rappresenta di per sé già un vantaggio ed una motivazione forte all'investimento. Ma sono altre le opportunità che oggi vengono offerte e che aprono di fatto la possibilità di nuove applicazioni che consentono da un lato di migliorare i processi di gestione della sicurezza degli ambienti e delle aree esterne, ma anche di rendere fruibili agli utenti servizi legati alla business intelligence.

Da un punto di vista tecnologico, quello che rende possibile queste funzioni, è la capacità di calcolo dei processori utilizzati all'interno delle telecamere che, oltre ad effettuare la compressione del segnale generato dai sensori, possono utilizzare parte delle risorse per attività di analisi e generazione di Metadata.

Il Metadata rappresenta la base su cui è possibile costruire le nuove piattaforme aperte di VideoSorveglianza, passando da un concetto di TVCC, ad un concetto più ampio di Open Platform.

Open Platform – una nuova visione per la VideoSorveglianza

Il mercato oggi presenta opportunità e sfide interessanti da cogliere. Se da un lato lo sviluppo tecnologico ha contribuito a rendere sempre più disponibili elevate qualità di immagine e funzionalità avanzate, è aumentata in contemporanea l'attenzione da parte degli utenti su aspetti importanti legati all'ottimizzazione dell'utilizzo dei budget, delle risorse economiche e dei benefici che si ottengono dalla realizzazione di un sistema di VideoSorveglianza. Si è consolidato un trend che vede la scelta di una soluzione di VideoSorveglianza influenzata non solo dal semplice aspetto economico, ma anche da elementi come il ritorno sugli investimenti, sui benefici portati e sulla possibilità di essere aperta allo sviluppo tecnologico.

In questa ottica, Samsung Techwin ha scelto di operare all'interno degli standard più consolidati offrendo, con il concetto di Open Platform, la possibilità ulteriore di adattare al meglio le funzionalità sulla base delle singole esigenze. L'Open Platform rappresenta un interessante elemento di sviluppo e di crescita tecnologica e culturale del mercato in generale.

La nostra tecnologia, integrata nelle telecamere, è virtualmente al centro di una infrastruttura che, partendo dall'unità di ripresa, risponde alle esigenze sempre più complete di sicurezza, efficienza operativa, analisi video e supporto al business.

Il cuore dell'Open Platform: il DSP WiseNet III

Tutte le nuove funzioni e le nuove potenzialità sono supportate da un processore di ultima generazione integrato nelle telecamere Samsung Techwin, chiamato WiseNet III. Interamente sviluppato da Samsung Techwin, rappresenta il risultato di una analisi che ha identificato le maggiori esigenze operative degli utenti, a cui è stata aggiunta la possibilità di accogliere nuove funzioni e algoritmi di analisi che, grazie allo sviluppo diffuso della tecnologia e della conoscenza, verranno resi disponibili.

WiseNet Lite

The Power of Simplicity



Telecamere FullHD semplici, affidabili e complete per VideoSorveglianza IP di qualità

Un range completo di telecamere Dome e Bullet IR 2MP e 1.3 MP, con il nuovo processore WiseNet Lite, con la qualità e l'affidabilità che da sempre Samsung offre sui propri prodotti.

Ma non solo.

Le nuove telecamere offrono anche funzioni aggiuntive come la possibilità di registrare su scheda SD integrata e su NAS esterno o come la funzione Hallway View, per la ripresa di aree strette e verticali come corridoi, tunnel e strade.

Scoprite subito come Samsung offre la possibilità di migrare su soluzioni IP e dimenticare il vecchio cavo coassiale.

Securing your future
Samsung Techwin Europe (Italy)
www.samsungsecurity.com
stesecurity@samsung.com – T. 02 38608.220



SAMSUNG TECHWIN



Grazie all'Open Platform, Samsung Techwin ha potuto consolidare partnership tecnologiche con altre aziende, contribuendo a fare crescere il livello tecnologico oggi disponibile, ed aprendo nuove opportunità di utilizzo delle telecamere, con una ricaduta positiva sul business per tutti i player coinvolti, compreso gli utenti.

Le nuove funzionalità rese disponibili con l'Open Platform possono facilmente essere integrate nelle telecamere con una logica simile a quella utilizzata per caricare una nuova App su uno smartphone.

L'utilizzo dei Metadata

Le App disponibili per l'Open Platform aumentano le funzionalità della telecamera, arricchendola di capacità di analisi real-time per molteplici applicazioni. Come risultato di questa attività, la telecamera, oltre a fornire immagini video, genera

anche Metadata, che racchiudono tutte le informazioni risultanti dalla attività di analisi. Tramite i Metadata generati a fronte dell'analisi video, è possibile inviare informazioni, ad esempio, su un numero di targa, sul numero di persone o veicoli presenti in un'area o in transito da un varco virtuale.

Da qui, le molteplici nuove applicazioni possibili, che vedono le telecamere come uno strumento di ausilio al business ad esempio di un'area commerciale o un ufficio pubblico. L'analisi comportamentale e la possibilità di identificare a fini statistici, parametri come range di età e genere, possibili con alcune delle App già disponibili, diventano uno strumento utile per definire al meglio la "customer experience" all'interno di un punto vendita o per rendere più veloce ed efficiente la fruizione di servizi in una filiale di banca.

Analogamente, ottimizzando le stesse logiche per il controllo del traffico veicolare è possibile poter intervenire per ottimizzare il flusso e i tempi di percorrenza.

Vantaggi di una soluzione Edge-based

La scelta di delegare l'analisi video alle telecamere riduce di molto la necessità di gestire streaming video di elevata qualità sulla rete con notevoli vantaggi in termini di infrastruttura.

Anche la registrazione oggi può avvenire a bordo della camera stessa, con la possibilità di recuperare le immagini solo quando necessario. Ai fini di business intelligence ed analisi comportamentale, ad esempio, non è necessario avere accesso ad archivi di immagini registrate.

È sufficiente gestire i Metadata, raccoglierti in un applicativo al centro che sia poi in grado di renderli fruibili in modo intuitivo e semplice per l'utente. La possibilità di gestire queste funzioni di analisi e di intelligence unicamente tramite Metadata e non sulle immagini, consente inoltre di semplificare le procedure necessarie per garantire la tutela della privacy previste dalle normative vigenti.

Da centro di costo a business tool

È chiaro quindi che risulta essere ormai riduttivo pensare che lo sviluppo tecnologico porti come unico vantaggio quello di poter fruire di sistemi di VideoSorveglianza con immagini sempre più risolte e di qualità.

I vantaggi offerti dalle soluzioni di ultima generazione vanno ben oltre, e aprono di fatto nuove opportunità di utilizzo, e quindi di business, anche per gli utenti. Tutto ciò presuppone un cambio, oltre che tecnologico, anche di mentalità e di modalità di azione, passando dal concetto di semplice TVCC, Televisione a circuito chiuso, che già nel nome indica elementi di limite, a soluzioni Open Platform, aperte, standard e pronte a cogliere le sfide del futuro.

I PROTAGONISTI



LE ECCELLENZE PER LA SICUREZZA

TSec SpA

In quale modo la partecipazione di TSec al seminario "Le Eccellenze per la Sicurezza" testimonia la volontà dell'azienda di segnare la differenza rispetto agli altri competitor diretti, nella ricerca e lo sviluppo di nuovi prodotti e di nuove soluzioni?

È una partecipazione "assertiva", per spiegare che le soluzioni tecniche offerte dal mercato e da certe tecnologie ormai obsolete, non sono sufficienti in moltissimi casi a garantire l'auspicata tranquillità a chi pensa di essere protetto da un efficiente sistema di allarme intrusione.

Un esempio classico è la protezione dei varchi, dove si usano ancora sensori basati su una tecnologia che risale al 1930, pur con varie evoluzioni successive. Tecnologia che presta il fianco alla neutralizzazione dei sensori e, di conseguenza, del sistema di rilevamento intrusione di cui fanno parte, con effetti più o meno clamorosi per l'utente.

La nostra percezione dell'attuale stato dell'arte del mercato della sicurezza fisica nell'insieme, è che non vengano in generale sviluppate soluzioni nuove e comunque "originali", come se mancasse, in qualche modo, il coraggio di investire nella R&S di questo comparto.

Secondo noi, non è azzardato affermare che nella sicurezza vengano utilizzate sostanzialmente tecnologie di "seconda mano", ovvero concepite e sviluppate in altri ambiti e solo successivamente adattate. Di conseguenza, mai come ora nell'era dell'Internet of Things, soprattutto la sensoristica appare tecnologicamente arretrata rispetto all'evoluzione delle esigenze di sicurezza di ogni tipologia di edificio, dall'abitazione al grattacielo. Solo per fare un esempio, non è una novità che venga molto spesso privilegiata la riduzione dei falsi allarmi, a sfavore della rilevazione dell'effrazione, con tutti gli effetti conseguenti sulla reale sicurezza dell'utilizzatore finale. Pensiamo, insomma, che ci sia molto da fare per chi ha voglia di sviluppare nuove tecnologie che nascano dalle esigenze del settore e non importate da altri mercati.

Noi abbiamo le idee chiare rispetto al futuro del nostro mercato, per questo stiamo investendo risorse importanti nei nostri progetti. Non è dunque un caso che TSec sia stata il primo produttore ad introdurre sul mercato europeo sensori di varco passivi a singolo switch, non mascherabili dall'esterno del perimetro protetto.

Quali sono gli scenari di prevedibile evoluzione tecnologica nel segmento in cui opera TSec?

Come abbiamo visto, secondo noi gli scenari tecnologici cambieranno molto in fretta e saranno molto diversi dalla realtà attuale. Ci sono sempre più segnali evidenti verso la ricerca di "scorciatoie" che unifichino tutti i sistemi della building automation e, quindi, anche dell'impianto di allarme antintrusione. Allo stesso modo, è inevitabile che la rapidissima evoluzione tecnologica che ha subito negli ultimi 15 anni il settore dell'ICT (Information and Communication Technology) debba presto o tardi (noi pensiamo presto!) coinvolgere anche il mercato della sicurezza. Questo avrà necessariamente ripercussioni importanti non solo sulle tecnologie, ma sull'intero mercato: cambieranno i player, i modi di fare business e, in ultima analisi, anche i servizi offerti agli utenti finali.



Quali sono le soluzioni (o i prodotti) presentate ai security manager partecipanti a “Le Eccellenze per la Sicurezza” a dimostrazione del potenziale innovativo di TSec?

La nostra presentazione è dedicata a un approccio progettuale contro l’insider attack, con soluzioni innovative per la protezione dei varchi. Gli attacchi interni costituiscono, in generale, un problema rilevante per l’intero sistema economico, con risvolti importanti sul piano legale e della tutela dei dati personali.

Presenteremo due soluzioni, delle quali la prima è relativa al sistema più efficace oggi esistente per la protezione dei varchi con sensori passivi. E’ la piattaforma **CST (Coded Sensor Technology)**, che consente la codifica univoca tra sensore e magnete, un nostro brevetto di cui andiamo naturalmente orgogliosi.

In pratica, anche a varco aperto e ad impianto disinserito, il sensore è in grado di riconoscere un tentativo di sabotaggio magnetico.

Questa piattaforma può essere integrata anche con un sensore di vibrazione a tecnologia ibrida/magnetica per prevenire, a varco chiuso, i tentativi di scasso. Le applicazioni sono molteplici ma quelle più classiche sono per i mezzi blindati, per le porte interbloccate e per le casseforti.

La seconda soluzione guarda ancora più al futuro: si tratta di un sistema per il monitoraggio dello spazio, realizzato con nuove tecnologie hardware, software e di signal processing. Senza utilizzare la videoanalisi, sarà in grado di riconoscere il movimento generato da persone, animali e cose, sia in interno sia in esterno.

Un altro tassello che va ad aggiungersi ad una nuova piattaforma per l’erogazione di servizi di sicurezza integrati. La presenteremo ufficialmente a Sicurezza 2015 ma, naturalmente, ne anticipiamo i contenuti principali al seminario del 21 settembre.



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



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



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**

Dalla sicurezza partecipata alla (c)lean security

di Giuseppe Mastromattei – Head of Security Department H&M

Nel corso degli ultimi anni ho avuto modo di condividere un nuovo o, meglio, diverso approccio alla sicurezza aziendale, avendo avuto l'opportunità di confrontarmi sia con colleghi, sia con giovani studenti universitari durante seminari accademici e convegni.

In tali circostanze mi sono sempre trovato davanti interlocutori la cui principale attesa era quella di capire fondamentalmente quale fosse il ruolo del *security manager* o del *risk manager* e quali funzioni, compiti e responsabilità fossero riconosciute all'interno dell'organizzazione aziendale. Ma soprattutto, quando la platea era composta da studenti, quali fossero le prospettive di questa misteriosa, e a volte sconosciuta, professione.

È stato quindi importante definire quello che forse è il concetto più semplice ma determinante: come *comunicare la sicurezza*, come *comunicare cosa fa la sicurezza e non solo quello che dice* - e rappresentare, in un'adeguata forma comunicativa, la componente emotiva nella percezione del rischio delle persone, nella consapevolezza che questa è fisiologicamente diversa per ognuno.

Partendo quindi dal concetto di comunicazione, il passaggio successivo, quasi naturale, è stato quello di introdurre la definizione di *sicurezza partecipata*: Sicurezza partecipata vuol dire *"garantire una maggiore integrazione e una migliore gestione del rischio, offrendo il massimo contributo alla redditività e al successo dell'organizzazione stessa"*. In altre parole, una responsabilità della tutela aziendale non più dispersa o confusa, ma definita in un processo chiaro, condiviso e fruibile per tutti.

Ma anche questo non era sufficiente, era necessario fare un passo avanti, dare qualcosa in più, un metodo che non solo potesse essere riconosciuto come valido strumento di management ma che, in qualche modo, coniugasse quel principio di semplicità e comprensibilità



indicato nella definizione di sicurezza partecipata. Nel settembre 2012, ho partecipato a Stoccolma ad una entusiasmante lezione sul *lean management* di Niklas Modig, docente della Stockholm School of Economics ed autore del libro "This is Lean: Resolving the Efficiency Paradox".

Ovviamente, tutto è rimasto lì per qualche tempo, in un quaderno pieno di appunti tirato fuori di tanto in tanto per prendere qualche ispirazione anche se, da quel momento, ho iniziato a pensare alla *lean security*. Ma procediamo con ordine: prima di parlare di *lean security* e poi di *(c)lean security*, è necessario partire da quello che è il *lean thinking*.

Lean Thinking

Il *Lean Thinking* o 'pensiero snello' nella sua accezione italiana, è innanzitutto un atteggiamento diverso degli individui che vivono l'azienda, un atteggiamento che ti porta dritto al cuore delle cose, un atteggiamento che



ti porta a rispondere prontamente ad una domanda fondamentale in qualsiasi attività aziendale: qual è il vero cliente per ciò che sto facendo?

Il *lean thinking* è una filosofia aziendale che trae origine dal modello di produzione Toyota, ideato da Taiichi Ohno per migliorare le performance attraverso l'utilizzo ottimale delle risorse: fare di più e meglio (efficacia) con meno (efficienza).

Il termine *lean thinking* fu coniato da J. Womack, D. Jones e D. Roos, i quali, nei primi anni '90, pubblicarono il libro dal titolo "La macchina che ha cambiato il mondo", in cui venivano messi a confronto i modelli imprenditoriali giapponesi con quelli occidentali del settore automobilistico, partendo dall'organizzazione di Toyota. La definizione che gli autori danno del pensiero snello è *"un modello manageriale volto ad ottimizzare l'organizzazione aziendale per ottenere sempre di più, utilizzando sempre meno risorse: meno sforzo umano, meno tempo, meno spazio, meno attrezzature e materiali"*.

I tradizionali modelli fordisti e tayloristi venivano superati da una nuova concezione di produzione snella, che consentiva di rispondere in modo più efficace ed efficiente alle richieste del cliente, sempre più focalizzato sulla riduzione dei costi e sull'acquisizione di un buon livello di competitività.

Dagli studi e dalle ricerche condotte dai tre autori, fu evidente che l'andamento dell'impresa giapponese era sempre più orientato ad essere flessibile, in quanto l'organizzazione snella consente di *produrre di più, con meno sforzo e con un migliore utilizzo delle risorse*, siano esse umane o materiali.

Il *lean thinking* non può che essere definito come la ricerca dei *muda* (termine giapponese che identifica attività inutili o che non aggiungono valore o improduttive) e la loro eliminazione, con lo scopo di produrre di più con un minor consumo di risorse.

Womack e Jones (1990) definivano lean un modo di *produrre di più con meno*, essendo tuttavia in grado di fornire ai clienti esattamente ciò che essi vogliono. Pensare snello aiuta ad interpretare e capire le esigenze del cliente operando in modo diretto ed immediato, riducendo al massimo i costi e utilizzando nel miglior modo possibile le risorse a disposizione.

Che si stia concependo o producendo capi di abbigliamento, componenti automobilistici, servizi di formazione, procedure interne e routine di sicurezza, non è mai scontato che quello che si sta preparando, sviluppando e elaborando sia allineato a quello che il cliente pensa di ricevere.

Porsi la domanda insieme al cliente favorisce la definizione del valore anche da parte del cliente che, spesso, non ha perfetta cognizione di causa di quello che vuole o, soprattutto, di quello di cui ha bisogno, ma può essere indirizzato attraverso proposte alternative, domande giuste al momento giusto, per capire meglio cosa si aspetta in termini di contenuti dei servizi offerti, con quali tempistiche e modalità. Una volta chiarito quale valore si aspetta il cliente, diventa allora facile cominciare la vera attività rivoluzionaria del mondo *lean*: andare a riconoscere tutti gli sprechi disseminati nei meandri delle attività che quotidianamente vengono svolte, per cercare di accontentare il cliente stesso nei tempi e nelle modalità definite prima.

Ma cosa si intende per *spreco*, cosa significa riconoscere un'attività priva di valore aggiunto rispetto a un'attività a valore aggiunto? Tutto ciò che non contribuisce ad accrescere o a raggiungere il valore precedentemente definito, è spreco.

Si può distinguere tra spreco necessario e spreco non necessario: ad esempio è uno spreco necessario l'adempimento di un requisito di sicurezza, di una normativa legislativa, ma è bene riconoscere la non necessarietà e la necessarietà degli sprechi, che sempre sprechi rimangono, perché su quello si dovrà lavorare per snellire i processi e ridurre i tempi di attraversamento, nel tentativo di raggiungere nel più breve tempo possibile l'agognato valore per il cliente. Nel *Lean Thinking*, il primo principio fondamentale consiste nella riscoperta della centralità del cliente. La definizione del valore deve partire dal cliente, il valore è quello che lui percepisce, che lui sente e riscontra nei prodotti e nei servizi a lui destinati.

Alla fine, quello che veniva auspicato nella definizione di sicurezza partecipata, definire un processo di sicurezza chiaro, condivisibile e fruibile per tutti.

Lean Security

Perché allora non usare il *lean thinking* come strumento per aumentare il valore che i *security manager* possono offrire alle loro organizzazioni?

Soprattutto oggi, quando il ritmo organizzativo è talmente elevato e quando gli scenari economici, sociali e legislativi in cui le aziende operano localmente e globalmente, possono cambiare drasticamente da un giorno all'altro. Tali cambiamenti hanno un impatto devastante nella gestione del rischio e della sicurezza. Gestione che deve essere sempre pronta a fornire il tipo di controlli di sicurezza e delle risposte che le loro organizzazioni hanno bisogno, quando ne hanno bisogno. Questa è la sfida della *leadership* della sicurezza oggi. Quello che viene sempre più richiesto ai moderni *security manager* è un alto grado di allineamento al *business*, una elevata capacità di adattarsi e di adeguare la funzione di sicurezza ai rischi connessi al cambiamento. Allo stesso tempo però, senza perdere di vista i valori e i principi fondamentali nella progettazione o riprogettazione dei processi di sicurezza. Al fine di applicare i principi *Lean* per la gestione della sicurezza, è importante definire ciò che è opportuno che si intenda per cliente, valore e spreco rispettando i principi del *lean thinking*.

Chi è il cliente per la sicurezza?

La più facile delle domande. I clienti per la sicurezza sono, a seconda della natura dell'organizzazione e dei prodotti o servizi che fornisce, non i clienti commerciali, ma il management e i dipendenti stessi che, a loro volta, forniscono prodotti e/o servizi al cliente commerciale. Pertanto, spetta alla funzione *security* capire quali siano le esigenze di sicurezza del *business* per garantire il successo commerciale e raggiungere i propri obiettivi di business. È pertanto fondamentale creare un adeguato livello di empatia tra il dipartimento sicurezza e le altre funzioni aziendali, per capire al meglio il cliente e le proprie esigenze di sicurezza.

Non ci dobbiamo aspettare che siano le altre funzioni a chiedere informazioni su quello che facciamo, ma dobbiamo noi stessi chiedere e partecipare.

Ma ciò è possibile se il management e dipendenti hanno chiaro quello che fa la sicurezza e se la stessa sicurezza è adeguata ai cambiamenti di cui abbiamo parlato prima.

Che cosa è "Valore" per la sicurezza?

Nella *lean security* "Valore" è una parte variabile, a seconda delle esigenze e delle aspettative dell'organizzazione, oltre a una parte più generica valida per ogni specifica organizzazione. Un sistema di sicurezza aziendale fornisce un valore ottimale per l'organizzazione se:

- supporta attivamente il raggiungimento degli obiettivi di business e di conformità dell'organizzazione (la parte variabile);
- è un processo efficiente, agile e integrato, in grado di affrontare e coesistere con il sempre più dinamico ambiente delle minacce;
- utilizza poche risorse e poco tempo;
- traduce la gestione del rischio, in linea con la propensione al rischio dell'organizzazione;
- definisce solo i controlli di sicurezza strettamente necessari e sufficienti, facili da usare, efficienti e misurabili da tutti.

Che cosa è lo "Spreco" per la sicurezza?

La parte più importante. Per analizzare quali siano gli sprechi maggiormente diffusi in un sistema di sicurezza, di seguito vengono proposte alcune tipologie che sono necessariamente da evitare in sede di attuazione di un modello di *lean security management*. Nell'elencare tali sprechi, si è

ovviamente tenuto conto delle indicazioni dei modelli di *lean management* adattandoli ad esempi concreti di *security management*. Nella tabella seguente per ogni tipologia di spreco è riportato un esempio

chiarificatore e quello che è l'*outcome*, nel senso di risultato percettivo connesso al *business*, per l'organizzazione stessa nei confronti del sistema di sicurezza.

Tipologia	Esempio	Risultato
Sovraproduzione	Controlli di sicurezza inutili dovuti ad una poco realistica identificazione del rischio basata su una cultura lontana dal contesto organizzativo. Adeguamento normativo insensato, non calato alla realtà organizzativa ed inteso solo come mero adempimento normativo (paper is ok so everything is ok).	Costi elevati ed inutili e spreco di risorse materiali ed immateriali.
Difetti	Controlli complicati e non monitorati o mal configurati. Sistemi di audit esclusivamente ispettivi e non dediti al confronto finalizzato al miglioramento costante.	Falso senso di fiducia e costi elevati.
Comunicazione	Report, documentazione e presentazioni complicate che non vengono capite o non adatte allo scopo, o meglio non in grado di raggiungere la componente emotiva nella percezione del rischio delle persone.	Falso messaggio non conforme alla realtà.
Analisi priva di valore aggiunto	Elaborazione di modelli teorici di valutazione del rischio inefficienti e duplicazione dei processi di revisione e di reporting.	Burocratizzazione del processo. Costi non sostenibili.
Conoscenza dei dipendenti	Elaborazione di politiche di sicurezza disallineate con la realtà operativa e gestionale. Perdita di tempo con controlli inadeguati e non condivisi dal personale.	Aumento dei costi e delle spese generali, aumento del livello di rischio, riduzione della fidelizzazione dei dipendenti.
Attesa	Sistema di controllo scarsamente flessibile che allunga tempi di realizzazione delle contromisure di sicurezza compromettendo l'intero sistema.	Flessibilità ridotta, riduzione della produttività, aumento del livello di rischio a causa dell'aggiramento delle procedure ritenute troppo lunghe.
Inesattezza	Risultati dall'analisi del rischio sovrastimati e/o sottostimati dovuti a controlli inadeguati e non conformi alla realtà. Applicazione di standard di sicurezza inappropriati.	Perdita di credibilità.



Ovviamente focalizzare l'attenzione sui concetti di cliente, valore e spreco non basta per mettere in piedi un *Lean Security Management System*.

Come per tutte le applicazioni *lean*, la *lean security* non è un esercizio di una volta. È un percorso da seguire per far sì che la sicurezza resti costantemente allineata con il *business*, al fine di poter essere sempre pronta ai cambiamenti e in linea con le esigenze organizzative di *business* e garantire un ottimale sistema di gestione dei rischi. L'obiettivo della sicurezza è quello di ridurre i rischi a livelli accettabili e a costi accettabili, ma soprattutto in modo armonico con il *business*. *Lean security* non è solo un insieme altamente efficace degli strumenti, ma deve essere un nuovo modo di pensare. Ma come rendere possibile questo cambiamento all'interno delle organizzazioni aziendali? Oltre ovviamente al focus costante sul cliente e sugli sprechi, è di fondamentale importanza il valore aggiunto che la sicurezza è in grado di offrire alla propria organizzazione, attraverso le procedure e gli strumenti che ha a disposizione.

Ad esempio adottare un sistema di videosorveglianza che, oltre a svolgere funzioni di prevenzione possa, collocato all'interno di un esercizio commerciale, svolgere anche attività di rilevazione del comportamento della clientela attraverso la funzione di analisi degli *hotspot* o di *area counting*; oppure rivedere il processo di *cash in transit* adottando procedure e sistemi in grado di ridurre i tempi di lavorazione del denaro ottimizzando i prelievi e tutte le operazioni connesse, coinvolgendo non solo la società che si occupa di trasporto valori, ma anche la banca, il produttore di casseforti e il proprio dipartimento responsabile della contabilità, e quindi

rivedere le macchinose procedure esistenti riducendole, o meglio, snellendole il più possibile.

Ma anche la semplice ronda potrebbe diventare *lean* se invece di limitarsi a verificare controlli e varchi fisici, fosse dotata di strumenti per analizzare varchi virtuali della rete *wifi* aziendale prevenendo eventuali tentativi di accesso non autorizzato.

(c)Lean security

Perché (c)*lean*? Mi sembra giusto concludere introducendo una "c" a quanto detto sino ad ora, riassumendo in maniera estremamente semplice il concetto di *lean security*.

Parte del cambiamento deve avvenire dall'analisi degli sprechi, e questo è alla base del *lean thinking*, e *clean* vuol dire in inglese *pulire, chiarire* per rendere comprensibile, se vogliamo, quella che per molti è ancora non solo ignota, ma difficile da comprendere: la *security* aziendale.

Giocare con le lettere sicuramente è estremizzare e semplificare, ma il vero significato di questa conclusione è, se vogliamo, provocatorio. Quanto i *security manager* sono disponibili a modificare la propria forma mentale? Quanti sono pronti ad aprire le porte dei loro uffici? E quanti sono pronti a confrontarsi con funzioni aziendali che cercano la sicurezza aziendale quando ormai è troppo tardi?

Rivedere la *security aziendale* dal punto di vista del cliente (che appunto inizia per "c") analizzando gli sprechi, ovviamente per eliminarli, potrebbe essere un nuovo modo per dare valore aggiunto al delicato ruolo che ogni *security manager* ricopre all'interno della propria organizzazione aziendale.

Ideale:
certifica i depositi,
esclude i falsi,
gestibile da remoto.

Perfetta:
elimina conteggi manuali,
verifiche e compiti ripetitivi.

Flessibile:
offre soluzioni diversificate
in funzione del volume di
contanti presente nel
punto vendita.

...e il Servizio?
Capillare, rapido,
affidabile.

In una parola:
SCRD
la gamma modulare
di sistemi di
deposito per il Retail

Soluzioni che creano valore

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

GUNNEBO
For a safer world®

www.gunnebo.it

Italia-Svezia, la sicurezza di una storia nella visita del Console a Gunnebo Italia

a colloquio con Marco Frazzica, Console Onorario di Svezia a cura della Redazione

In occasione di una recente visita alla sede di **Gunnebo Italia**, una delle più importanti aziende svedesi operanti nel settore della sicurezza, il Console di Svezia, avvocato Marco Frazzica, ha espresso interessanti considerazioni sulle possibilità di sviluppo dei rapporti economici tra i due Paesi.

Signor Console, quali sono i motivi che l'hanno portata a visitare la sede di Gunnebo Italia?

In quanto Console di Svezia, ho rapporti costanti con le organizzazioni che si occupano dello sviluppo delle relazioni Svezia-Italia, tra le quali anche la Camera di Commercio Italo-Svedese Assosvezia che, da quasi mezzo secolo, è uno dei centri attorno ai quali si articolano i rapporti commerciali tra le due nazioni. Da qualche tempo, Gunnebo recita un ruolo molto attivo e di primo piano in Assosvezia, con Marco Depaoli fortemente impegnato quale membro del Board of Directors. Avendo avuto modo di conoscere Marco Depaoli, ho potuto anche cominciare a conoscere la storia di Gunnebo in Italia, storia che mi è sembrata molto interessante ed indicativa dei risultati che la collaborazione tra Svezia ed Italia può conseguire. Sono stato perciò felicissimo di accettare l'invito di Marco Depaoli a visitare l'azienda.

La presenza del gruppo Gunnebo in Italia con unità produttive e commerciali crea occupazione in loco e produce risultati positivi per l'Italia e anche per la Casa madre svedese. Questo esempio è seguito da altre aziende svedesi. Come possono tutte queste aziende fare insieme sistema per ulteriormente sviluppare la loro presenza ed il loro business in Italia?

In Italia la Svezia è molto rispettata e viene percepita come portatrice indiscussa di importanti valori positivi come la responsabilità sociale, la trasparenza, la tutela dell'ambiente, il rispetto e la valorizzazione delle diversità e, non ultimo, la capacità di fare innovazione sostenibile. Di fatto, questo significa che un prodotto ed una azienda svedese possono godere, per il solo motivo di "essere svedesi", di una percezione positiva che può essere molto importante, anche dal punto di vista commerciale. Credo, quindi, che le aziende svedesi potrebbero cercare, magari anche cooperando assieme in organizzazioni quali la Camera di Commercio Italo-Svedese Assosvezia, di condividere maggiormente le loro esperienze in Italia ed individuare modi per dare ancora più risalto ai valori positivi di cui sono portatrici, dando così, perché no, anche spunti per un miglioramento del Sistema Italia.



Ritiene che gli investitori svedesi siano pronti ad aumentare il volume degli investimenti in Italia grazie ai cambiamenti strutturali in atto per ridurre la rigidità del mercato del lavoro, le carenze infrastrutturali e l'influenza della corruzione?

La risposta è senz'altro positiva a patto che il quadro politico italiano mantenga quella stabilità che sembrava aver raggiunto e che il Governo faccia seguire i fatti alle parole, soprattutto nella lotta alla corruzione che, a mio parere, nell'ottica svedese è probabilmente il singolo fattore che pesa di più, in negativo, nella valutazione di possibili investimenti nel nostro paese.

Quali sono secondo Lei le prospettive nel prossimo futuro per gli scambi e la cooperazione fra industrie italiane e svedesi?

Sono ottimista. Dal mio punto di osservazione vedo un maggior dinamismo rispetto agli anni scorsi ed un incremento delle iniziative. Quindi, se il quadro politico italiano resterà stabile, penso che gli scambi e la cooperazione registreranno un sensibile miglioramento.

IoT, sicurezza fisica e sicurezza informatica: convergenza o interdipendenza? - Prima puntata

a cura della Redazione

L'Internet of Things è un tema di estrema importanza per la sicurezza, in ogni sua declinazione (attiva, passiva, security, safety, fisica, informatica...). Gli scenari sottostanti alla sua diffusione - in parte già ben chiari, in parte ora solo intuibili - potranno venire percepiti come opportunità da cogliere e/o rischi da evitare ma, di sicuro, interesseranno chiunque operi nella sicurezza, a qualsiasi titolo: dal security manager alla guardia giurata, dal costruttore al progettista, dall'installatore all'assicuratore eccetera. Un tema di questo peso ci ha spinto a chiedere il parere ad alcuni protagonisti della scena della sicurezza, per aiutarci a "razionalizzarlo" e proporlo nel modo più adeguato ai nostri lettori, nel percorso di informazione dedicata che faremo da qui in avanti. Iniziamo con Citel Spa, la società italiana che vanta la maggiore presenza nei sistemi informatici della sicurezza fisica nella fascia della grande utenza, che certamente ha familiarità con la materia, considerando che è in continuo contatto con una clientela composta dalle principali banche, Poste Italiane, ENI, ENEL, SNAM, Finmeccanica e, quindi, dalle principali infrastrutture critiche del Paese.

Nell'editoriale di esecome n. 3/2015 "IoT, cancellato il confine tra la sicurezza fisica e quella logica" abbiamo riportato alcuni episodi criminosi e un rapporto di origine USA, che dimostrerebbero la caduta del confine tra sicurezza fisica e sicurezza logica. Cosa ne pensate di questa teoria? E, visto che ci siamo, possiamo fare chiarezza sui concetti che stanno dietro la terminologia e sulle implicazioni pratiche? Parto dall'IOT, l'Internet delle cose. Di sicuro, si può solo dire che se sempre più "cose" vengono connesse a una infrastruttura di per sé aperta come Internet, sarà il caso di implementare protezioni sempre più stringenti (antivirus e anti-malware) per mitigare il rischio. Lo dimostra il fatto stesso che il rapporto citato nell'editoriale è di fonte Symantec e mi pare naturale che la società metta



in evidenza questo aspetto. Peraltro, se c'è qualcuno che connette via Internet la sicurezza fisica di una infrastruttura critica a un centro di controllo e ci viene chiesto un parere, noi rispondiamo "no comment" nel senso che operiamo su altri livelli di sicurezza e proponiamo quindi di chiedere a utenti come SNAM o ENEL cosa ne pensano. Non mi è chiaro, invece, in base a quali argomenti si possa sostenere che il confine tra sicurezza fisica e logica sia stato cancellato grazie (o a causa) dello IoT. La domanda più generale sull'eventuale convergenza operativa ce la siamo già fatta più di una volta, senza però trovare una ragionevole motivazione né un'applicazione pratica. Per adesso, ci limitiamo a fare proposte di convergenza sulle definizioni dei due concetti e delle loro relazioni, che - lo ribadisco - non devono essere necessariamente di convergenza operativa se non sussistono delle oggettive

basi tecniche e funzionali. Per cominciare, quella che non è "Sicurezza Fisica" nel nostro mondo si chiama "Sicurezza Informatica" e non "Logica", se non altro perché è la traduzione più vicina a quella dell'inglese "Cyber Security" che, ormai, ha prevalso su "Computer Security", anche secondo Wikipedia.

Gli addetti ai lavori del mercato italiano hanno le idee chiare a proposito della distinzione tra sicurezza fisica e sicurezza informatica e dei rispettivi contenuti?

Se parliamo di organizzazioni grandi e medio-grandi la risposta è affermativa. Non potrebbe essere diversamente: le responsabilità e le interazioni operative verso le strutture da proteggere e verso le fonti del rischio sono oggetto di politiche e procedure stringenti nei settori in cui operiamo. Aggiungo anche che incrociamo sempre più spesso i consulenti specializzati chiamati per i penetration test e per la certificazione della compliance per nuovi impianti o dispositivi che connettiamo alla rete dati. D'altra parte, i nostri più grandi utenti sono banche e infrastrutture critiche nel campo dell'energia, ed è scontato che noi siamo sempre di fronte a interlocutori ad elevata professionalità. Pertanto, nella nostra esperienza tutti gli addetti ai lavori operano in una chiarezza di competenze e di ruoli e, fino ad oggi, non abbiamo rilevato nessuna "zona grigia". Nelle organizzazioni di dimensioni minori o in settori dove i rischi sono più contenuti, c'è una certa varietà di situazioni, legata al tipo di settore e ai rischi prevalenti, ma comunque con una sensibilità e una preparazione decisamente accettabile e in crescita negli anni, grazie anche alla diffusione della cultura informatica nella sfera della persona, delle aziende e della società.

È possibile - in base ai rapporti con la grande utenza - definire oggettivamente le relazioni - anche indirette - tra sicurezza fisica e sicurezza informatica e individuare una terminologia neutra e di uso corrente?

Certamente, sono convinto che sia particolarmente opportuno, ma non vorrei limitarmi a un glossario, che non risulterebbe utile perché i termini sono legati a concetti da contestualizzare. Preferisco pertanto illustrare per punti il contesto PSIM, proponendo di **evidenziare in grassetto** la terminologia significativa o a rischio di ambiguità, spiegata in 3 punti:

1 - Citel realizza progetti di **sicurezza fisica che utilizzano strumenti informatici** e reti dati strutturate dell'utente per ottenere soluzioni di protezione dei suoi asset fisici (palazzi, sedi periferiche, stabilimenti, strutture commerciali, impianti di produzione energia, ecc.). Fin qui siamo nella sicurezza fisica che viene ottenuta usando strumenti informatici (il computer, il PSIM, le centrali di

gestione eventi) **transitando su LAN e WAN** dell'utente per concentrare la gestione degli eventi in una control-room ma anche su posti operativi presso centri servizi o su apparati mobili.

2 - Quindi, il sistema informatico dipartimentale di sicurezza fisica, il PSIM Centrax nel caso di Citel, è connesso a LAN e WAN dell'utente utilizzando a livello centrale, secondo le dimensioni del progetto: una semplice Workstation oppure un insieme di Server, Posti di lavoro, Front-end, ecc.. Mentre in campo gli apparati che generano eventi sono raggiunti perché connessi ai router di una LAN che porta alla WAN. **La rete dati usata dal sistema informatico aziendale veicola quindi anche i dati di un PSIM che potrebbe introdurre delle vulnerabilità con un impatto potenziale sul sistema informatico gestionale dell'azienda.** Le vulnerabilità non sono quelle del software PSIM, ma quelle che (ad esempio attraverso una centrale di allarmi) potrebbero creare una sorta di pericolosa "porta di servizio" in un punto di una rete dati che per il resto è stata blindata da accessi non previsti. Il rischio per il sistema informatico gestionale non riguarda quindi il sistema Centrax in sé, ma deriva dalla eventualità dell'introduzione volontaria di **malware in rete che possa corrompere i dati gestionali trasmessi su LAN/WAN** o ne possa impedire la circolazione. Ma, se questo è un rischio originato dall'innesto di apparati del PSIM scelti dall'utente (intrusione, accessi, videosorveglianza, ecc.), non è altro che quello che accade ogni volta che qualsiasi altro sistema informatico dipartimentale dell'azienda (produzione, logistica, personale, ecc. con i relativi dispositivi specializzati da mettere in rete) viene innestato nella rete dati aziendale per ottenere un unico sistema informatico gestionale sempre più integrato.

3 - Ma l'azienda, che utilizza l'informatica per ogni processo produttivo e gestionale, ha anche l'esigenza di minimizzare i rischi di un attacco alla struttura fisica del Data Centre, cuore e sistema circolatorio dell'informatica aziendale. E, pertanto, si richiedono **misure di sicurezza fisica** che proteggano i computer, gli organi fisici di alimentazione e di comunicazione da attacchi esterni che ne possano bloccare il funzionamento interrompendo il servizio del sistema informatico e quindi l'operatività aziendale. **Pertanto, il cerchio si chiude constatando che in questo caso il PSIM, sistema di sicurezza fisica utilizzatore del Sistema Informatico anche contro attacchi di cyber security, in questo caso lo protegge da attacchi e incidenti di tipo fisico.**

Sembra un giuoco di parole ma serve a descrivere sinteticamente l'interdipendenza (non la convergenza!) della sistemistica di Sicurezza Fisica e della Sicurezza Informatica.



Le soluzioni sui Metadata dei partner Milestone presentate a MPOP 2015

Seconda parte - la prima parte è stata pubblicata in essecome n. 3/2015

Video Analisi e Forensics Analysis: cosa sì, cosa no, cosa forse...

di Simone De Titta, managing director di TecnoAware srl



La telecamera in piazza XX è stata messa lì per monitorare e segnalare in tempo reale tramite video analisi l'assembramento di persone. Tuttavia, una notte avviene un furto con scasso in uno dei negozi monitorati dalla telecamera. Non arrivano allarmi perché, di fatto, non ci sono stati assembramenti in quella zona. Nessuno sa a che ora è successo l'evento, e la Polizia deve rivedere il video di tutta la notte per trovarlo. Sarebbe invece molto utile poter impostare una semplice query alla piattaforma di

gestione del tipo "trova un soggetto che è rimasto in quella area per più di 30 secondi" e avere la risposta in pochi secondi. E' fantascienza? Forse no, la risposta corretta a questa domanda è: dipende. Vediamo in questo articolo da cosa può dipendere. La video analisi oggi comincia effettivamente a consentire di estrarre informazioni utili da un ambiente, da eventi, dalla descrizione di soggetti di interesse e dai dati ad essi correlati (conteggio, posizionamento ecc ..). Il miglioramento negli anni degli algoritmi stessi, ma anche il miglioramento della qualità dei sensori e l'aumento della potenza computazionale dei processori permettono di fare sempre più cose e di estrarre da un ambiente informazioni sempre più dettagliate e affidabili.

Tuttavia, dobbiamo continuare a fare molta attenzione alla fantascienza ancora troppo millantata in questo argomento "pericoloso". In questi ultimi 10 anni, il mercato della video analisi ha continuato a denunciare scottature e disillusioni dovute a improbabili favole raccontate da mass media (e vendor...) sempre più spregiudicati. E, nonostante questo, in particolare in questi ultimi 2 anni molti vendor sembrano non aver imparato la lezione, e hanno ulteriormente "pompato" nel mercato pericolosa disinformazione, spesso davvero ridicola e in totale contrasto con la più banale fisica e aritmetica di base. Purtroppo, spesso il mercato ci casca, continuando a credere a improbabili giochi di prestigio preparati per fiere o per spettacolari video da postare su YouTube. Sulla stessa "Forensic Analysis", ovvero la capacità di acquisire e gestire a priori informazioni di un ambiente monitorato per poi richiederle a posteriori su specifica esigenza funzionale, c'è

una terribile confusione nel mercato. Il caso più drammaticamente divertente è quando viene chiesto (vi assicuro, più di una volta...) di recuperare le immagini di un furto da una telecamera PTZ che, però, era girata in quel momento dall'altra parte! "Eh, ma come non si può? Tizio ha detto che lo fa...!"

Occorre, quindi, fare un pragmatico ripasso generale su questo tema e su quali informazioni siano effettivamente affidabili e in quale contesto, e quali no.

La Forensic Analysis

Come scritto nell'introduzione, per "Forensic Analysis" (nello specifico ambito della videosorveglianza) si intende la capacità di estrarre a posteriori dati e immagini dall'archivio di un impianto di video sorveglianza. dalle immagini. Ad esempio, il ritrovamento a posteriori delle immagini archiviate da una telecamera dell'evento del passaggio di un veicolo rosso da una data via.

Il primo problema da affrontare è metodologico. Come si può fare analisi forense? In 2 maniere: in tempo reale o tramite query immediate a un database di dati archiviati insieme alle immagini.

Nel primo caso, parliamo di impianti di video sorveglianza tradizionali, con semplice archiviazione delle immagini. Si tratta, quindi, di processare off-line video archiviati, impostando la regola di video analisi richiesta e aspettando che il modulo processi tutto il video. Possono, per esempio, venir messi in parallelo i video di più telecamere e più fasce orarie, impostando per ognuno la regola di interesse e lanciarli in batch, per esempio durante la notte. E, al mattino, si ritrovano i risultati. Purtroppo questo modulo, come detto, lavora in tempo reale: ovvero, per un video di 12 ore impiegherebbe 12 ore per fornire i risultati. Questo perché il video, di fatto, verrebbe processato per la prima volta da un modulo di video analisi, come se fosse una telecamera in tempo reale, andando, quindi, analizzato per intero. In alternativa, occorrerebbero diversi operatori concentrati su più video e, comunque, sempre in tempo reale: si capisce, quindi, quanto sia elevato il valore della possibilità di dare tutto "in pasto" a un modulo automatico.

Nel secondo caso, del quale ci occuperemo nel dettaglio in questo articolo, i moduli di video analisi già hanno lavorato a priori in tempo reale su quei video archiviati, e i dati descrittivi di tali video sono già stati archiviati opportunamente in un database corrispondente. Abbiamo, quindi, impianti dove la video analisi è già presente a priori. A questo punto, è possibile effettuare query specifiche, che otterranno la risposta in pochi secondi, perché i dati sono già stati estratti ed archiviati in precedenza: adesso, si tratta solo di consultarli. Da un lato, è evidente il valore ancora maggiore, in termini di tempo necessario per avere il dato richiesto rispetto alla metodologia precedente; dall'altro, lo ripetiamo, la video analisi deve già essere presente al momento dell'archiviazione dei video. Una prima, grande confusione che si vede nel mercato è proprio su questo punto: la richiesta (o la vendita spregiudicata) della seconda modalità su video archiviati in maniera tradizionale, senza alcun database di dati generato precedentemente! E' banalmente impossibile fare query a database che non ci sono... Ma non è sempre semplice farlo capire e molti, purtroppo, approfittano di questa confusione per generare messaggi fuorvianti.

L'altra grande confusione che regna su questa seconda modalità è legata ai dati effettivamente estraibili con sufficiente affidabilità, e come. Non è sufficiente avere dei semplici moduli che estraggono, per esempio, dimensione, posizione e colore del target per rilevare eventi complessi. Comunque, anche queste stesse feature di base possono essere efficacemente rilevate e archiviate solo in certe condizioni.

Nei prossimi paragrafi analizzeremo nel dettaglio come e quali dati possiamo ritenere affidabili e in quale contesto.

Rilevazione ed archiviazione di feature di base

Per "feature di base" intendiamo le informazioni descrittive legate a un target rilevato: ad esempio, la sua posizione nello spazio (o nell'immagine), il suo colore dominante, la sua velocità, la sua dimensione, eccetera. Analizzeremo adesso una per una queste feature, richiamando con ordine come, cosa e quando è realmente possibile acquisire con efficacia.



Posizione del target

Innanzitutto, occorre stabilire se parliamo di posizione nell'immagine o posizione stimata nello spazio reale. Per stabilire, per esempio, se un target ha attraversato una linea virtuale disegnata sull'immagine, non occorre stimare la posizione nello spazio reale, poiché la linea disegnata è comunque solidale con l'immagine. Basta, quindi, rilevare ed archiviare la sua posizione sull'immagine. Attenzione, però: nell'esempio dell'immagine qui sotto, la testa della persona nell'immagine sembra attraversare, nella prospettiva, un'area più lontana.

L'area che si vuole allarmare è l'interno del laghetto (poligono rosso); tuttavia, quando le persone passano sulla strada, per effetto della prospettiva più del 50% del loro corpo risulta dentro l'area configurata, pur non essendo, evidentemente, dentro al laghetto. Diventa, quindi, fondamentale poter determinare quali pixel del target siano effettivamente efficaci per la sua rilevazione: in questo caso, il punto a terra è la configurazione più corretta. Anche nel caso di una persona che tocca un quadro in un museo, probabilmente un punto esterno sarebbe più efficace. Bisogna avere quindi una piattaforma in grado di poter salvare più punti del target, e poter scegliere quello più efficace in funzione a seconda dello specifico utilizzo.

La posizione nello spazio reale, o "assoluta" del target è, in realtà, un corollario che si realizza calibrando l'immagine, ovvero creando una corrispondenza precisa tra punto immagine e punto nella realtà. Si può arrivare a dare un'informazione di posizionamento in coordinate geodetiche. Tuttavia, quello che realmente serve a livello pratico è sapere dove si trova un soggetto in relazione all'immagine con la quale si lavora, eventualmente mappata staticamente con una pianta della scena. Conoscere le coordinate geodetiche di un target in un range statico di meno di 100 metri è molto "bello da vedere" e anche da raccontare come effetto speciale, ma è utile solo in certe applicazioni molto specifiche, pur essendo tecnicamente possibile. La posizione nello spazio reale diventa, invece, molto critica e non affidabile quando si parla di spazi piccoli. Per esempio, è decisamente difficile sapere con precisione dove si trovi nello spazio una persona all'interno di una biblioteca piena di scaffali e scrivanie perché, come si può intuire, il target risulterà sempre parzialmente nascosto da tutti gli ostacoli presenti nella scena e la sua sagoma non avrà punti di riferimento precisi da proiettare sulla mappa.

Dimensione del target

La dimensione del target è un parametro molto delicato e spesso utilizzato per proporre improbabili classificazioni di soggetti. Innanzitutto, la dimensione del target deve invece essere necessariamente riferita alla sua posizione nello spazio: una persona lontana può essere grande come un gattino vicino. Occorre quindi calibrare a priori l'immagine, per ottenere un'informazione di prospettiva efficace. A questo punto, è evidente che il target sarà stabilmente ben visibile per intero solo in scenari particolarmente semplici, con ottima illuminazione, senza ostacoli e senza troppi altri soggetti che interagiscono con lui. In altri casi, dove la visibilità della sagoma del target non sia stabilmente visibile, la sua dimensione sarà un'informazione spesso inaffidabile risultando, per esempio, molto più piccolo nel caso in cui sia parzialmente coperto o poco contrastato come, ad esempio, dei pantaloni neri nell'ombra. In questi casi, diventa poco plausibile definire "trova target di dimensioni x", a meno che non si parli di dimensioni molto differenti tra loro, come una persona e un camion. Di certo, chi millanta di poter discriminare grossi cani o animali dalle persone, non fa che alimentare la confusione che regna in questo settore: una persona che cammina a gattoni o striscia apparirà sempre come un grosso cane; mentre un grosso cane che cammina frontalmente verso la telecamera apparirà sempre come una persona... Implicita, inoltre, la necessità di avere a disposizione algoritmi solidi, in grado di filtrare efficacemente fattori

come le ombre e le dinamiche di sfondo. Ad esempio, le dimensioni di un target con la sua ombra o che stia passando davanti a una siepe in movimento, potrebbero risultare decisamente alterate. Senza contare le immagini notturne, dove non venga utilizzata una telecamera adeguata per filtrare le fonti di luce artificiale: ad esempio, i fari delle macchine sono ancora fonti di "rumori" devastanti anche per la miglior video analisi del mondo.

Colore del target

Questa è una delle feature più "pericolose" da proporre. Di che colore è, nell'immagine, la vettura in ombra ripresa dalla telecamera nella figura 2? E di che colore è in figura 3, mentre passa in una zona illuminata dal sole?

Ebbene, quella macchina è verde scuro! Ma nella prima immagine la si direbbe grigia, mentre nella seconda appare grigia o addirittura bianca. L'informazione del colore è purtroppo molto poco affidabile in ambienti generici, soprattutto esterni, con cambi di luce, ombre e riflessi, ma anche per la stessa manipolazione che correttamente compie la telecamera stessa con i processi di wide dynamic range, guadagno automatico, eccetera.

Quindi, pensare di fare una query del tipo "trova il passaggio di una persona con il maglione rosso da quella strada": di nuovo, è molto bella da raccontare ma, oggettivamente, poco realizzabile se non in casi particolari. Il colore può, invece, venire efficacemente utilizzato in scenari con luce controllata, dove il colore è stabile ed è ben visibile dalla telecamera. Oppure, quando si vogliono comunque riconoscere colori molto lontani tra loro, come un fumo bianco o un fumo nero.

E riconoscere il cliente dalla commessa di un negozio con una maglietta sempre gialla? Beh, "ni": basta che nessun cliente entri mai con vestiti gialli e che la commessa non abbia capelli neri lunghi...!



Classe del target

Anche sulla classe, o tipologia del target bisogna fare molta attenzione. La maggior parte dei prodotti sul mercato classificano i target solo in base alle dimensioni, quindi con tutte le limitazioni scritte in precedenza. In realtà, la classificazione può dipendere anche da altre feature descrittive, come la forma, il colore stesso, la presenza di assi geometrici specifici, momenti dinamici, eccetera. E' tuttavia chiaro che tutte queste feature sono, come le dimensioni, affette da una certa possibilità di errore, in generale molto dipendente dalla complessità della scena.

E' possibile immaginare di classificare target le cui feature siano molto lontane tra loro: camion da persone o veicoli, piccoli animali da persone, rumori generici dai target di interesse, mentre è privo di senso pensare, come qualcuno si ostina a raccontare, di poter distinguere, per esempio, gli autobus dai camion, piuttosto che berline da station wagon o persone da alani...

Di nuovo, è forse possibile in un esperimento "di laboratorio" limitato, ma è fuori senso in un'applicazione reale 24/7.

Traiettoria del target

La traiettoria del target "classica" non è altro che la sua posizione (nell'immagine o nello spazio) sviluppata nel tempo. Il fattore cruciale per avere una traiettoria efficace, è avere un tracking (inseguimento) efficace e di lungo termine del target stesso. Chiaramente, questo è di nuovo fortissimamente dipendente dalla complessità della scena: più la scena è affollata e/o piena di ostacoli, meno efficace e duraturo sarà il tracking del singolo target; di conseguenza, la sua traiettoria sarà più corta o, peggio, sbagliata.

D'altro canto, una traiettoria può essere anche la semplice direzione di passaggio attraverso una linea, quindi molto localizzata e senza la necessità di un tracking lungo.

In realtà, nell'attuale stato dell'arte della video analisi, per traiettoria si intende qualcosa di molto più ampio e non ancora facilmente realizzabile al momento. La traiettoria di un target è un vettore di più feature, tra le quali possono esserci posizione e direzione, ma anche tutte le stesse feature che possono essere utilizzate per la classificazione di un target. L'evoluzione di queste feature nel tempo rappresenta la traiettoria del target, ed essa stessa è un'informazione molto potente per classificare gli oggetti, in base anche alla loro evoluzione e comportamento. Ne parleremo tra qualche anno..!

Forma del target

Non è concettualmente impossibile, per ogni target rilevato, definire quale forma abbia basandosi su template primitivi (rettangolo, quadrato, cerchio, ellisse, ..). Più complesso, ma anche qui non impossibile, definire a priori delle forme specifiche (un carrello, una sedia, una valigia, ..) e definire, per ogni target rilevato, se sia associabile o meno a una di queste forme. Il problema è che, sia nel primo che nel secondo caso, il modulo di video analisi che acquisisce in diretta i dati dovrebbe processare a priori degli algoritmi di detezione di forme primitive, o basati su classificatori pre-addestrati. Questi algoritmi sono ancora parecchio pesanti e onerosi in termini computazionali; per di più, la maggior parte di questi sono ancora dipendenti dalla scena specifica e dalla prospettiva, comportando di conseguenza un notevole onere di configurazione. Ci sono metodi che lavorano anche con feature indipendenti a prospettiva e rotazioni, ma sono ancora più pesanti. E' quindi davvero poco probabile che chi sostenga di poter fare riconoscimenti di forme utilizzando appliance leggere lo faccia veramente...

Altro problema è, naturalmente, il fatto che si deve poter vedere bene per intero il target, per poter stabilire con precisione la sua forma. Ciò significa che ci possiamo scordare categoricamente di ottenere questo risultato in scenari affollati o con molti ostacoli..!

Velocità del target

Questa è l'informazione dove c'è, in assoluto, più confusione. Si chiede spesso di filtrare oggetti che vadano a una certa velocità: tutto molto semplice, avendo target che vanno dritti lungo traiettorie orizzontali alla camera, come si vede in molti bellissimi video su YouTube. A volte, questo può essere sufficiente, ad esempio per rilevare veicoli lungo rettilinei che procedono a certe velocità in aree con restrizioni o per rilevare persone che corrono in corridoi rettilinei. Comunque, anche in questo caso è indispensabile una perfetta calibrazione dell'immagine, per poter trasformare efficacemente pixel/secondo in metri/secondo.

Ma quando questi target si muovono in direzioni non rettilinee? Quando questi target non camminano al suolo, ma volano a mezz'aria (volatili, insetti, oggetti lanciati, ..)? Quando questi target si occludono parzialmente tra loro o dietro a ostacoli e la loro posizione non è quindi stabile nell'immagine e nella sua proiezione sul piano? Quando siamo in aree affollate dove il tracking della singola persona è impossibile? Evidentemente, in questi ed altri casi, la mia bella formuletta "velocità uguale spazio fratto tempo" va a farsi benedire... (continua)

Tre paradigmi di Citel per la sistemistica informatizzata di gestione della sicurezza fisica in architettura aperta

di Nils Fredrik Fazzini – general manager Citel spa

Con il numero 3/2015 di **essecome** si è conclusa la mappatura dell'Ecosistema generato da Centrax e dal quale Centrax è a sua volta alimentato. Centrax è il PSIM di Citel e la sua mappatura completa è stata pubblicata in un e-book di Securindex (<http://www.securindex.com/library/e-books>), ripreso e distribuito in 6 puntate della rivista.

Era la prima volta che un Ecosistema (evocato spesso dai produttori di sistemi informatizzati) di un sistema informatico della sicurezza fisica veniva spiegato, nei suoi aspetti pratici e nei suoi effetti virtuosi, ad una platea vasta come può essere quella di una piattaforma di settore come Securindex. Ed erano quindi sorprendenti i numeri record di aperture effettuate dai lettori sul portale Securindex nelle diverse puntate.

Il termine Ecosistema era stato evocato in passato da molti produttori di soluzioni di sicurezza, dando forse per scontato che tutti sapessero cosa volesse dire la sua applicazione alla tecnologia, ad un catalogo prodotti, ad un'azienda. Ed era evidentemente arrivato il momento che un addetto ai lavori spiegasse finalmente il senso pratico e dimostrabile di un concetto che suonava così positivo e costruttivo.

Per Citel è stata un'occasione per aiutare i lettori a percepire gli aspetti meno evidenti della propria attività di produttore di sistemi informatizzati, tanto impegnativi e determinanti quanto poco riconoscibili: il continuo, pluriennale impegno di un laboratorio di sviluppo software, hardware, middleware, mobile, ora esteso anche all'IOT, per l'integrazione di apparati di terzi, dando così all'utenza nuove funzionalità

interoperanti e sinergiche. E con questo, dando *contenuti di concretezza al valore astratto dell'apertura architeturale* del sistema, da sempre sostenuta da Citel e oggi pretesa dall'utenza in termini sempre più selettivi, nelle prestazioni e nella sostenibilità.

Chi ha letto qualche puntata della serie sull'Ecosistema Centrax ha potuto scoprire, tra l'altro, come nasce un sistema informatico degno di questo nome: con processi sinergici multilaterali, con il contributo determinante di utenti, fornitori, partner e anche di concorrenti. Perché *il sistema informatico della sicurezza fisica – il PSIM – non nasce nel PC di un programmatore*, ma da un'accumulazione progressiva di conoscenze e soluzioni a fronte di bisogni, interessi, vincoli che si incrociano e si contrappongono, per poi convergere nel tempo in esperienze e soluzioni.

L'ambito in cui tutto questo accade è viceversa un Ecosistema con il produttore del PSIM al centro, in un ruolo creativo e costruttivo solo se animato da una visione condivisa dalle comunità (utenti, partner), dalla padronanza di tecnologie e sistemistica e, last but not least, dalla capacità di auto-finanziare progetti informatici di respiro pluriennale.

Dal SISIF al PSIM

Citel ha sempre seguito la stampa tecnica USA (senza mai trovarvi particolari spunti innovativi), finché un giorno non è apparso improvvisamente (e provvidenzialmente) l'acronimo PSIM, il perfetto equivalente del SISIF, l'acronimo che Citel usava dal 2009 in ambito bancario per dare un nome a quello



che negli anni si stava connotando sempre di più come un vero e proprio “Sistema Informatico della Sicurezza Fisica”.

Il termine PSIM ha prontamente rimpiazzato il SISIF nel lessico di Citel che, oltretutto, ne condivideva anche il paradigma dei 7 requisiti fissati da IMS Research per chi avesse voluto attribuirsi l’etichetta di “PSIM vendor”. Qualifica che la classifica USA di IMS del 2013 attribuiva a *Corporation* a tutti gli effetti, accreditate ciascuna di centinaia di milioni di dollari di ricavi e storie aziendali più che decennali:

1. NICE Systems;
2. VidSys;
3. Proximex;
4. CNL Software;
5. Verint Systems.

Una classifica significativa di società indipendenti che confermava il fatto che il PSIM non potesse che nascere dalla grande utenza con investimenti elevati e con fornitori strutturati.

Il problema dell’ambiguità e degli opportunismi

La formulazione di 7 requisiti in forma particolarmente sintetica era necessaria per ottenere una rapida adesione da parte di una platea USA e internazionale ampia e variegata: e l’adesione al paradigma è stata infatti immediata. Peccato che la sinteticità si presti ora alla strumentalizzazione opportunistica, facendo

passare per PSIM quelli che sono solo dei software applicativi di supervisione, trascurando il fatto che un Sistema Informatico è una infrastruttura di gestione aziendale mentre un supervisore di eventi di sicurezza è soltanto uno strumento software che di quella infrastruttura è solo una parte.

Ne è conferma la chiosa alla classifica di IMS da parte di Niall Jenkins, responsabile di IHS (casa madre di IMS) per il mercato della sicurezza fisica, che cancella ogni dubbio con la considerazione che “il mercato PSIM presenta delle barriere di ingresso piuttosto alte poiché si colloca in un settore che esige il tipo di risorse di cui possono disporre solo quei fornitori di soluzioni che dispongono delle professionalità per sviluppare, personalizzare e realizzare progetti complessi”. (<http://www.securityinfowatch.com>)

Quello che, invece, è importante osservare riguarda la questione della scalabilità di un PSIM dall’alto verso il basso, con la circolazione delle esperienze tra gli utenti, perché è presso i grandi utenti strutturati che di norma vengono concepiti i processi ottimizzati di gestione. E’ questo accumulo di esperienze incorporato nel sistema informatico della sicurezza che viene di norma trasferito alle fasce di utenza minori, in forma di processi gestionali completi, efficienti, compliant al livello dei grandi utenti che hanno contribuito a concepirli.

Citel è parte in causa in questo contesto, nel senso che ha impiegato ben più di un decennio per ottenere

un PSIM come Centrax in un fortunato rapporto, più simbiotico che di fornitura con la grande utenza italiana, soprattutto la più visionaria, innovativa ed esigente. Ora che per l’informatica è caduto il rispetto reverenziale e che si diffonde l’informazione su nuovi modelli gestionali informatizzati, è naturale che si instauri tra produttori un processo imitativo che innesci una competizione che può non tener conto dei valori effettivi dietro la facciata. Se oggi i rischi di confusione intorno al termine PSIM sono meno immanenti per i grandi utenti, dove la cultura informatica e metodi di progettazione sono presenti anche nella sicurezza fisica, il rischio per l’utente di minori dimensioni è quello di fermarsi a una superficie che mostra una grafica suggestiva ed effetti speciali che portano a pensare che dietro di essi ci sia tutto quello che serve in termini di processi gestionali; mentre i valori espressivi sono utili solo se sono asserviti all’ergonomia e solo se poggiano su solide basi sistemiche, processi intelligenti, supporto competente, in una proiezione pluriennale, come bene aveva precisato Niall Jenkins di IMS Research.

Quello per la fascia media è un rischio latente, particolarmente insidioso nel settore della sicurezza fisica perché, se i processi di un sistema informatico di contabilità, di produzione, di magazzino, sono scadenti o incompleti lo si vede dai risultati, anche loro scadenti o incompleti; è diverso il caso della sicurezza fisica, che è un valore impalpabile e probabilistico, e che oltretutto si manifesta in un contesto in cui le procedure informatizzate non hanno una storia consolidata. Da qui l’idea di Citel che le ambiguità in questione possano essere risolte con la combinazione di **tre paradigmi oggettivi**:

- il PSIM innanzitutto, a sostegno dell’idea di un

sistema informatico dipartimentale allo stesso livello degli altri sistemi dipartimentali specializzati e tecnicamente autonomi o facenti parte di un ERP aziendale;

- l’Ecosistema in quanto terreno di coltura di sinergie tra esperienze e distillato naturale di soluzioni intelligenti, di validità generale e settoriale;
- la Telegestione professionale come combinazione di requisiti tecnico-architettonici, quelli di cui meno si parla e che possono nascondere falle inaccettabili.

I tre paradigmi e il sequel dell’Ecosistema

Per affrontare le peculiarità della sicurezza fisica ai fini della sua corretta informatizzazione, compresi i particolari rischi di ambiguità legati alla peculiarità del settore, Citel ha adottato la combinazione dei tre paradigmi progettuali e gestionali consolidandola come base concettuale per soluzioni di sistema al passo con i tempi. Quindi aperte, multifunzionali, sostenibili, basate sulle buone pratiche e sulla compliance.

I tre paradigmi:

- l’**Ecosistema dinamico** come insieme di comunità naturalmente sinergiche ma con un dinamismo accelerato dagli stimoli dell’organizzazione che lo ha generato;
- l’**Open PSIM**, con i suoi 7 requisiti integrati da una descrizione più completa, sempre neutra, ma basata sull’esperienza applicativa dell’utenza italiana e quindi particolarmente focalizzata sull’open architecture, la multifunzionalità, la multimedialità;
- la **Telegestione professionale**, quella che si ottiene solo a condizione che l’infrastruttura informatica rispetti criteri tecnici che garantiscano non solo le funzionalità ma la dependability della filiera e dei processi di elaborazione.



CAME apre le porte di EXPO Milano 2015 con XVia

a cura della Redazione

Came, gruppo riconosciuto in Italia e nel mondo nel settore della home & building automation, e interlocutore globale nel controllo della casa e nel mondo dell'urbanistica e dell'alta sicurezza, presenta il sistema di controllo accessi progettato per gestire i passaggi pedonali di **Expo Milano 2015**.

L'innovativo modello di controllo accessi consente la sorveglianza, il comando e la regolazione dei dispositivi di automazione degli ingressi pedonali e veicolari, dei parcheggi, dei padiglioni e delle altre infrastrutture del sito espositivo per gestire l'entrata di visitatori e operatori.

Si stima, infatti, che nei sei mesi dell'evento, **circa 140 mila persone varcheranno ogni giorno i cancelli del sito espositivo**: è come se una città delle dimensioni di Monza o Brescia si riversasse quotidianamente su un'area grande come 150 campi da calcio. Mentre **ogni notte, dall'una alle sei e mezza, circa 400 mezzi e 4mila persone**, addette al rifornimento di merci e alle pulizie, **oltrepasseranno i varchi veicolari** del sito espositivo. Il sistema di controllo accessi deve anche gestire picchi di 250mila persone al giorno, il 60% delle quali è atteso nelle prime due ore di apertura dell'Esposizione Universale.

La soluzione proposta da Came si basa su un sistema totalmente nuovo, in grado di dialogare con le tecnologie di controllo, sicurezza, sorveglianza e connettività più efficienti presenti oggi sul mercato. Gli accessi perimetrali del sito espositivo sono controllati da 230 tornelli automatici, 20 dei quali sono stati appositamente progettati per gestire l'ingresso dei visitatori diversamente abili. La fornitura si completa con l'integrazione di automazioni per cancelli scorrevoli, barriere automatiche stradali e con 40 dissuasori per



la protezione e la selezione delle entrate perimetrali di passaggi carrai. Il sistema integrato di controllo accessi può essere monitorato anche attraverso 70 dispositivi palmari.

Fulcro della piattaforma tecnologica sviluppata da Came è **XVia**, il nuovo tornello a tripode dotato di testa di lettura progettato ad hoc per Expo Milano 2015, in grado di gestire la grande complessità di dati e di variabili connesse alla lettura di tutti i tipi di titoli d'ingresso, all'elevato numero di periferiche e di visitatori che accedono nello stesso momento



all'Esposizione Universale.

Lo stesso nome del prodotto - **XVia** - che si ispira al 2015, anno dell'Expo identificato come XV, esprime il concetto di Via di accesso al nuovo percorso di innovazione che Came sta intraprendendo, orientato a proporre soluzioni tecnologiche all'avanguardia al servizio della vita quotidiana delle persone, delle imprese, dei grandi progetti.

Il tornello "intelligente", parte integrante del sistema di controllo accessi e del sistema di ticketing di Came, è in grado di leggere biglietti in formato cartaceo, QR Code, RFID o NFC che consentono ai visitatori e agli espositori di accedere anche da mobile, utilizzando smartphone e tablet.

Pensato per essere integrato in grandi progetti di controllo accessi, **XVia** coniuga innovazione tecnologica e minuziosa ricerca estetica. Il design ricercato, lo stile minimale e la struttura compatta permettono al tornello di inserirsi in modo armonico e discreto nella più varia tipologia di ambienti. La costante connessione alla rete Ethernet consente, invece, di controllare in tempo reale di tutte le funzionalità dell'impianto.

Studiato per interfacciarsi con le tecnologie di tutti i partner di Expo Milano 2015, ciascun tornello è stato predisposto con un dispositivo per la lettura

biometrica finalizzato ad elevare il livello di sicurezza come nel caso di autorizzazione all'ingresso per personale abilitato o di servizio. Il design di **XVia** è stato studiato anche per comunicare con i visitatori, attraverso segnalazioni luminose e sonore, rendendo più rapida la fase di accesso, riducendo code e lunghe attese. Gli indicatori direzionali luminosi garantiscono sicurezza e facilità di passaggio nei contesti in cui i flussi sono elevati: la segnalazione luminosa consente, infatti, di comprendere in modo immediato quando è possibile transitare.

Il tripode è dotato della funzionalità di pre-rotazione che viene attivata non appena convalidato il titolo d'accesso, facilitando così il passaggio dell'utente. In caso di particolari esigenze o qualora sia necessario liberare immediatamente il passaggio, **XVia** dispone della funzione di caduta braccio; quando l'emergenza sarà rientrata, è possibile attivare, anche da remoto, il riarmo automatico.

Completa la soluzione un sistema sinottico di controllo in grado di gestire le automazioni presenti sulla piattaforma di Expo Milano 2015. Il programma è installato presso il MOC (Main Operation Centre) dell'Esposizione Universale e viene utilizzato per monitorare in tempo reale e in modo centralizzato



lo stato di tornelli, dissuasori, barriere e cancelli scorrevoli installati presso il sito espositivo. Il sistema, connesso alle automazioni Came, consente di gestire in maniera centralizzata le configurazioni dei sistemi ed eventuali complessità e imprevisti legati alla gestione dei titoli d'ingresso con l'obiettivo di migliorare il servizio, facilitare il flusso di entrata e ridurre i tempi di attesa.

Came S.p.A.

Came S.p.A., tra i leader riconosciuti in Italia e nel mondo nel settore della home & building automation, si presenta come interlocutore globale nel controllo della casa e nel mondo dell'urbanistica e dell'alta sicurezza al quale offre soluzioni integrate per la regolamentazione e il monitoraggio dei flussi e degli accessi.

Il gruppo, rappresentato dal marchio Came Safety&Comfort, progetta, produce e commercializza

con i marchi Came, Bpt, Domino LED e GO Italia soluzioni di automazione per ingressi, sistemi domotici e di sicurezza antintrusione, videocitofonia, termoregolazione e illuminazione a LED, e porte e portoni sezionali per ambienti residenziali e industriali; attraverso i brand delle società Urbaco, Parkare offre inoltre soluzioni per l'urbanistica e per i grandi progetti, sistemi per la gestione di parcheggi automatici a pagamento, per il controllo accessi e la protezione di ambienti collettivi come spazi pubblici, piazze e strade. Di proprietà della famiglia Menuzzo, Came S.p.A. è una realtà fortemente legata alle proprie radici italiane. Presente sul mercato con 480 tra filiali e distributori in 118 Paesi del mondo, ha sede a Dosson di Casier in provincia di Treviso e possiede stabilimenti produttivi a Treviso, Sesto al Reghena (PN), Avignone (Francia) e Barcellona (spagna). L'azienda conta 1.370 collaboratori e ha registrato un fatturato di 230 milioni di euro nel 2014.

Came è un'azienda certificata "100% Qualità Originale Italiana" dall'Istituto Tutela Prodotti Italiani (ITPI). Un riconoscimento che ha premiato la scelta del gruppo di progettare italiano, di non delocalizzare l'assemblaggio e di avvalersi di fornitori esterni, con i quali ha instaurato un rapporto di fiducia reciproca in oltre 40 anni di attività.

Came, grazie alle proprie soluzioni innovative per il controllo accessi, è stata scelta come partner tecnologico da Expo Milano 2015.

Segui Came anche sul sito www.came.com e sui profili LinkedIn, Twitter e Facebook.

CAME
safety&comfort

CONTATTI - CAME S.P.A.
Via Martiri della Libertà, 15
31030 Dosson di Casier (TV)
Tel. +39 0422 4940
Fax +39 0422 4941

intersec

January 17 – 19, 2016

Dubai, UAE

www.intersecexpo.com

BOOK YOUR
STAND NOW!

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

Avigilon: intelligence e video analisi, il futuro della videosorveglianza

in colloquio con Corrado Grandin, Avigilon Regional Sales Manager Italy & Malta a cura della Redazione

Quali sono le linee guida di Avigilon per lo sviluppo delle applicazioni di Intelligence nella videosorveglianza?

In Avigilon crediamo che le attività di monitoraggio non possano prescindere dall'Intelligence, dal momento che l'incorporazione della video analisi nella sorveglianza può permettere la prevenzione di un incidente invece della gestione delle sue conseguenze. Questo perché la security deve avere un ruolo proattivo nella protezione delle persone, delle strutture e dei beni e non solamente di risposta a un evento, con un approccio solamente di tipo 'forense'.

Questi cinque punti riassumono ciò che, secondo noi, si dovrebbe ottenere dalla video analisi:

1. Le applicazioni di analisi devono comprendere le funzionalità di 'intelligence' per poter utilizzare il video non solamente in tempo reale, ma anche successivamente;
2. L'analisi dovrebbe cambiare il modello di costo del monitoraggio, aumentare la produttività degli operatori e rendere, in conclusione, la protezione più accessibile per un maggior numero di utenti;
3. Per ottenere una 'visione olistica' che consenta di reagire in tempo reale agli incidenti, l'analisi deve fornire l'intelligence già incorporata in un sistema integrato di sorveglianza end-to-end, senza doverla aggiungere alla camera come un 'accessorio';
4. La video analisi non deve richiedere all'utente alcun sforzo aggiuntivo, deve operare in modo autonomo;
5. La video analisi deve aiutare l'utente ad assicurare la sua attività nel futuro, come fonte intelligente di dati per ridurre i costi, aumentare la produttività e i guadagni, ridurre i rischi.

Quali sono i principali mercati verticali in Italia per Avigilon?

Le soluzioni di Avigilon sono ideali per ogni tipologia



di mercato verticale, ma Retail, Amministrazioni Pubbliche, Security aziendale, Impianti Sportivi e Trasporti sono quelli sui quali siamo maggiormente concentrati.

Quali sono i prodotti che avete presentato per il 2015/2016?

Il nostro successo e la nostra crescita sono dovuti ai nostri prodotti innovativi, all'eccellente servizio clienti e alla ricerca di espansione geografica e verticale.

Adesso siamo concentrati a promuovere questi nuovi prodotti ma altri stanno arrivando nel prossimo futuro

- 7K HD Pro camera
- HD Pro with self-learning analytics
- HD Multisensor
- ACC ES HD Video Recorder

7K HD Pro

- Le nuove camera Avigilon HD Pro 6K e 7K catturano 'best-in-class' i dettagli delle immagini in grandi aree di monitoraggio, consentendo la massima gamma di opzioni. La 7K è la nostra linea ancora più potente e innovativa di camere ad alta definizione
- Ma l'alta definizione va oltre la camera, le altre parti del sistema devono assicurare la scalabilità, la decodifica e la larghezza di banda necessaria per gestire immagini HD
- La nostra tecnologia brevettata High Definition Stream Management (HDSM) riduce drasticamente la larghezza di banda del server-client e i requisiti per lo storage, ottimizza l'utilizzo delle risorse informatiche del cliente e offre una grande scalabilità senza penalizzare la risoluzione
- Questo consente di integrare senza soluzione di continuità le nostre nuove telecamere 7K nei sistemi Avigilon preesistenti senza dover fare alcun upgrade dell'infrastruttura, proteggendo l'investimento e fornendo un basso TCO

HD Pro con self-learning video analytics

- Tecnologia di video analisi self-learning incorporata
- 5K è la camera a sensore singolo a più alta definizione prodotta con analisi self-learning
- Copertura di grandi aree con possibilità simultanea di zoomare sui dettagli, accoppiata ad un accurato rilevamento degli oggetti
- Tecnologia HDSM 2.0 con compressione H.264 per la massima chiarezza dell'immagine, minima larghezza di banda e di necessità di storage

- Tecnologia LightCatcher™ per un'eccezionale resa dei colori nell'immagine

Avigilon Control Center Edge Solution (ES) High Definition (HD) Recorder

- Registra localmente, monitora centralmente, gestisce da remoto
- Secondo una recente ricerca globale di Forbes, la maggior parte delle organizzazioni (58% degli intervistati) controlla con la videosorveglianza meno della metà dei propri asset di valore
- Secondo la stessa ricerca, degli intervistati che utilizzano la videosorveglianza, la maggioranza (66%) ha detto che meno della metà dei siti o delle strutture dove la videosorveglianza è in funzione, è controllata attivamente da personale di sicurezza specializzato
- L'Avigilon Control Center (ACC) Edge Solution (ES) High Definition (HD) Recorder ingloba tecnologie di base di Avigilon in un dispositivo compatto per memorizzare in modo intelligente i video HD, eliminando i problemi di larghezza di banda per il monitoraggio centralizzato dei siti remoti
- Chiave di accesso alle prestazioni dell'ACC ES HD Recorder, il software ACC è dotato della tecnologia Avigilon brevettata High Definition Stream Management™ (HDSM), che fornisce la larghezza di banda efficiente e la gestione dello storage, consentendo agli utenti di visualizzare anche le telecamere a massima risoluzione su una connessione remota. Quando è accoppiato con le telecamere di Avigilon HD con analisi self-learning, la soluzione offre regole e gli allarmi per consentire risposte proattive agli incidenti.



ekey e il mercato globale dei sistemi fingerprint: ottime prospettive di ulteriore crescita

a cura della Redazione

È stata pubblicata a giugno la ricerca di mercato di **Marketsandmarkets** sul mercato globale dei sensori fingerprint, con una panoramica delle tecnologie e dei campi di applicazione delle soluzioni fingerprint. Secondo il report americano, il mercato mondiale dei sensori per scansione delle impronte digitali crescerà fino al 2020 ad un tasso annuo medio del 17%.

ekey, attiva da oltre 16 anni in questo settore, tra i protagonisti mondiali e N. 1 in Europa delle soluzioni per l'accesso ad impronta, sta quotidianamente rispondendo alle esigenze e al trend di una continua maggior diffusione della tecnologia fingerprint in sempre più numerosi aspetti della nostra vita quotidiana. Anche in ekey lo sviluppo dell'azienda continua a procedere a ritmo costante e sostenuto, con una forte crescita del fatturato registrato anche quest'anno.

L'impronta digitale è personale, non trasferibile e non riproducibile, costituisce il metodo più sicuro e, allo stesso tempo, più comodo per accedere alla propria abitazione. La leadership di ekey si basa sulla ricerca fondamentale, settore al quale ekey si dedica sin dalle sue origini, nonché sulle funzionalità intelligenti dei prodotti quali, ad esempio, la funzione d'apprendimento del software, il doppio algoritmo di confronto di proprietà ekey, e il filtro per la ricostruzione delle linee papillari, che conferiscono ai prodotti ekey un'imbattibile capacità di rilevamento. Con il sensore a radiofrequenza autopulente, è escluso che rimangano immagini latenti sul sensore. Una serie di brevetti nazionali ed internazionali assicurano il know-how di ekey.

Tecnologia fingerprint evoluta per una sicurezza totale

ekey ha messo a punto un algoritmo proprietario molto potente per il rilevamento delle impronte digitali. Si tratta della tecnologia di base della ekey, che viene impiegata nelle soluzioni standard ekey, nei moduli embedded nonché in numerose altre applicazioni. Un'intensa attività



nel campo della ricerca fondamentale, nell'ambito del rilevamento e del trattamento delle immagini, assicurano una posizione all'avanguardia nella tecnologia, garantita a lungo termine. Per raggiungere un'alta performance di rilevamento, ekey ha sviluppato una serie di ulteriori procedimenti, che sono stati implementati nell'algoritmo ekey.

Algoritmo basato sulle minuzie

ekey usa il rilevamento delle minuzie, procedimento che trasforma le particolarità delle impronte, come ad es. punti singolari, terminazioni delle linee, biforcazioni ecc. in un codice numerico binario inconfondibile.

L'algoritmo ekey è caratterizzato da due componenti principali, il Feature Extractor e il Matcher.

Feature Extractor

Le immagini dell'impronta rilevate dal sensore sono sfocate, hanno un cattivo contrasto e contengono errori e difetti. L'algoritmo sviluppato da ekey ricorre a misure estremamente potenti per migliorare la qualità delle immagini.



Matcher

Il motore di rilevamento di per sé lavora con estrema velocità e affidabilità. Grazie all'esperienza pluriennale e all'ampia ricerca in questo campo, l'algoritmo ekey è caratterizzato da una sicurezza superiore abbinata al massimo comfort. La tecnologia di base può trovare impiego sia in piccoli che in grandi banche dati.

Tecnologia dei sensori

L'algoritmo concepito da ekey può essere abbinato ad una serie di sensori diversi.

Software intelligente

Il software intelligente ad ogni suo uso impara, riconosce la crescita delle dita di bambini, nonché i cambiamenti di abitudini e piccole ferite degli utenti.

Una politica della qualità rigorosamente perseguita

L'elevato standard qualitativo e la longevità dei prodotti, connessi all'ampio ventaglio di servizi offerto da ekey, come, per esempio, la garanzia di 5 anni su tutti i prodotti ekey, un attento supporto tecnico alla clientela e la possibilità di update dei prodotti per un lungo periodo di tempo, hanno valso a ekey la posizione all'avanguardia nel campo della tecnologia fingerprint.

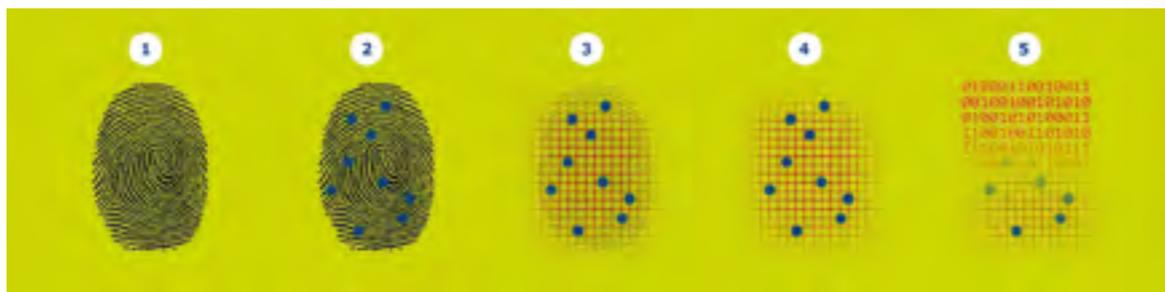
L'estensione volontaria della garanzia a 5 anni è stata introdotta nel 2014, come conseguenza di una politica aziendale che, sin dalle origini, attribuisce la massima importanza alla sicurezza e alla qualità, e riguarda tutti i sistemi di controllo d'accesso ekey.

Usabilità e versatilità dei prodotti come basi della filosofia ekey

Per i suoi sistemi, ekey ha messo a punto diverse modalità di funzionamento e di programmazione, che dipendono dalle esigenze particolari dei clienti e delle relative applicazioni. ekey rivolge un'importanza particolare all'usabilità e intuitività dei suoi prodotti. Per questo motivo abbiamo messo a punto diversi sistemi tecnici di base, in funzione dei requisiti dei nostri clienti.

ekey adminfinger

La soluzione essenziale ed economica. Mediante un dito amministratore definito, è possibile memorizzare le autorizzazioni all'accesso direttamente sul lettore d'impronte digitali. Grazie alla scelta di uno o più dita amministratrici, si possono salvare i diritti d'accesso direttamente sul lettore d'impronte.



ekey home app

L'innovativa e comoda soluzione per amministrare il proprio lettore d'impronte ekey. Con estrema facilità è possibile impostare sullo smartphone o tablet tutte le funzioni del sistema di controllo degli accessi con il lettore d'impronte ekey. In più, è possibile aprire la porta di casa anche tramite l'app. Disponibile per Apple iOS e Google Android.

ekey classic

Il sistema collaudato, facile da utilizzare. Nella centralina di comando integra, incassata nella porta, si gestiscono comodamente tutte le impostazioni e diritti d'accesso.

Nel **settore OEM**, ekey conta tra i suoi clienti molti **produttori di porte, di sistemi di chiusura, maniglie e citofoni**, che sviluppano soluzioni di design high-end con lettori ekey integrati. Dato che le porte sono continuamente sottoposte a movimenti, a volte intensi o violenti, tutta la nostra gamma porte è stata sviluppata per queste specifiche esigenze e dall'inizio controllata da un Istituto accreditato. Efficacia, versatilità e funzionalità di integrazione sono le basi del successo della ekey con i partner OEM.

Grandi gruppi internazionali hanno scelto ekey come fornitore della tecnologia fingerprint.

ekey ha anche stretto delle alleanze con molti produttori leader di **sistemi avanzati della domotica**, sviluppando interfacce per l'integrazione dei lettori d'impronte ekey in molti marchi di home automation (Gira Home, AMX, Savant, Control4, Crestron, Beckhoff...). I driver trasmettono un pacchetto dati al sistema domotico, i lettori di impronte possono quindi determinare alcune azioni oppure richiamare impostazioni di atmosfera personalizzate.

La gamma delle soluzioni ekey si rivolge sia a clienti privati che a aziende e enti pubblici, proponendo **le soluzioni stand-alone ekey home**, per un singolo accesso (porta/cancello/allarme), **le soluzioni ekey multi**, che permettono di gestire fino a 4 lettori d'impronte, e **i sistemi ekey net** (controllo d'accesso con software di gestione per impianti di qualsiasi dimensione), per aziende e case di alta gamma.

Vantaggi delle soluzioni ekey, l'esperto del riconoscimento dell'impronta digitale:

- Algoritmo proprietario di riconoscimento
- Intensa attività nel campo della ricerca fondamentale, stretta cooperazione con istituti di ricerca esterni
- Posizione all'avanguardia nella tecnologia grazie alla funzione di apprendimento del software, il doppio algoritmo di confronto, e il filtro per la ricostruzione delle linee papillari
- Oltre 1 milione di utenti soddisfatti
- Numerosi brevetti e modelli d'utilità nell'ambito del riconoscimento delle impronte digitali e del trattamento delle immagini
- Sensore autopulente (non lascia immagini latenti sul sensore) per la massima sicurezza
- Ineguagliabile per riconoscimento e comfort
- Fornitore di fiducia della tecnologia fingerprint di grandi gruppi internazionali
- Sistema certificato di gestione qualità conforme a ISO 9001:2008
- Test di resistenza a fattori ambientali e a temperature estreme
- A prova di vibrazioni e di shock

Continui sviluppi tecnologici sono il garante per il successo comune!

Prodotti ekey: la sicurezza della qualità.

CONTATTI - EKEY
www.ekey.net
italia@ekey.net
 Tel. +39 04 7192 2712

The Next Big Thing



ALL-OVER-IP

THE FASTEST GROWING IP-FOCUSED NETWORKING EVENT IN RUSSIA



IT INFRASTRUCTURE & NETWORKS
 VIDEO SURVEILLANCE, VSAAS
 IP SECURITY
 STORAGE, ANALYTICS, BIG DATA
 CLOUD & VIRTUALIZATION
 IDENTITY MANAGEMENT
 AND ACCESS CONTROL
 INTELLIGENT BUILDING
 INTEGRATED SECURITY SOLUTIONS

190 GLOBAL AND RUSSIAN BRANDS
 5000 KEY LOCAL
 CUSTOMERS & PARTNERS
 CEO SUMMIT
 GLOBAL KEYNOTE THEATRE
 IT & CLOUD LAB
 SMART & SAFE CITY
 INTELLIGENT VIDEO 2.0
 MACHINE VISION

8

ALL-OVER-IP
 Russia
 18-19.11.2015

Groteck
www.all-over-ip.ru

Dahua presenta le nuove telecamere di rete della serie Eco-Savvy 2.0

a cura della Redazione

Dahua Technology, produttore e fornitore di prodotti di videosorveglianza professionale e VIDEOTREND, distributore ufficiale per l'Italia, presentano la nuova serie di telecamere IP "Eco-Savvy 2.0".

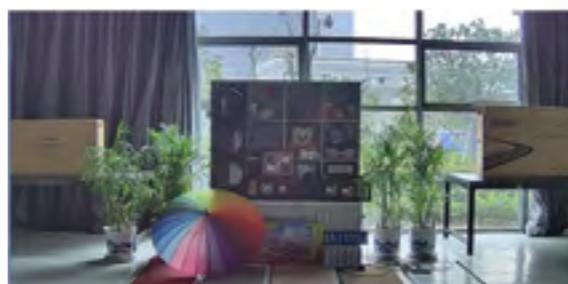
Questa nuova serie offre nuove impressionanti caratteristiche tecniche nella videosorveglianza, pur mantenendo e rispettando il concetto di risparmio energetico nel suo DNA, grazie al nuovo processore Ambarella S2LM. Le telecamere sono dotate di un sensore CMOS a scansione progressiva con risoluzione

di 4MP che offre immagini di alta qualità a 20fps. Grazie a questo si ottiene un'immagine due volte più chiara rispetto a quella di una tradizionale telecamera 1080p (2MP). La serie Eco-Savvy dispone di una vasta gamma di funzioni evolute, tra cui il face detection e la video analisi con funzioni attraversamento linea e/o area. Queste caratteristiche fanno sì che gli utenti abbiano la possibilità di usufruire di una video analisi più precisa e, dunque, di avere una maggiore efficienza nel livello di sicurezza del sistema.

WDR



WDR off



WDR on

Intelligent Video Surveillance



Alarm



Normal



La nuova serie adotta anche la tecnologia WDR per l'ottimizzazione delle immagini e sono dotate di triplo stream video. Il wide dynamic range (120dB) assicura che le telecamere possano offrire significative prestazioni sia nelle riprese in controluce, sia in quelle effettuate nelle aree con scarsa illuminazione, due delle situazioni tradizionalmente più difficili per le telecamere di sorveglianza. Dahua ha inoltre introdotto miglioramenti nei fotosensori. Il sensore di luce a infrarossi consente alla telecamera di commutare le modalità giorno/notte in modo dinamico e automatico, in funzione delle necessità ed in base ai livelli di illuminazione. Tutti questi miglioramenti sono progettati per fornire agli utilizzatori della nuova serie Eco-Savvy 2.0, una impareggiabile facilità d'uso unita a prestazioni eccezionali.

La nuova serie è certificata IP67 e IK10 anti-vandalo,

per garantire sempre un perfetto funzionamento anche nelle condizioni più difficili. Cosa c'è di più? Tutti i modelli della serie Eco-Savvy 2.0 funzionano a temperature comprese tra i -40°C e +60°C, garantendo la certezza che le telecamere Dahua continueranno a funzionare anche negli ambienti e nelle condizioni più difficili. Le dimensioni compatte della serie Eco-Savvy 2.0 le rendono ideali in gran parte delle applicazioni su larga scala come scuole, alberghi, negozi, uffici e industrie.

Caratteristiche principali

- 4M@20fps; 3M@25/30fps
- Triple stream video
- Analisi video integrata
- WDR (Wide Dynamic Range) reale sino a 120dB
- Massima distanza IR 50 metri
- Protezioni IP67 e IK10



L'attenzione di Saet verso progettisti e installatori a tutela del cliente finale

a colloquio con Davide Crosetto, membro CdA di Saet Italia srl e A.U. di Tervis srl
a cura della Redazione

L'attenzione che SAET dedica ai progettisti e agli installatori si esprime anche attraverso incontri sul territorio, per dare informazioni e approfondimenti sull'evoluzione tecnologica e gli aspetti normativi. Quali sono i presupposti di questo impegno e quali sono i vostri programmi per il futuro?

Dal 1965, quando è nata la Saet, ci siamo sempre confrontati con un aspetto per noi fondamentale: portare avanti la Cultura della Sicurezza. Questa nostra missione la decliniamo a tutti i livelli e quello dei progettisti è un anello fondamentale della catena distributiva prevista nel modello Saet. E' ovvio che 40 anni fa gli strumenti a disposizione erano completamente diversi, ma non bisogna fare l'errore di credere che non vi sia più nulla da imparare. Se negli anni '70 per l'installatore ed il progettista erano necessarie delle competenze di tipo elettrotecnico, negli anni 90 è diventato indispensabile aggiungere competenze di natura elettronica. Se prima "bastava" sapere come funziona un relè, da un certo punto in avanti è stato necessario capire anche come funziona una linea seriale. Ben inteso che come funziona un relè bisogna continuare a saperlo anche adesso. Oggi si devono aggiungere competenze di tipo informatico, dato che il cosiddetto IoT (Internet of Things) coinvolgerà in modo sempre più pesante il settore. Noi cerchiamo di essere pronti per soddisfare queste nuove esigenze formative. La tecnologia è una commodity ed è destinata ad appiattare tutte le prestazioni: oggi la differenza la fa l'esperienza di consumo, a tutti i livelli: dal distributore al progettista, all'installatore e fino all'utente finale. Noi investiamo non solo nel prodotto ma anche in tutti quei servizi che possono rendere l'esperienza di acquisto dei nostri prodotti assolutamente perfetta.

Nest, la società di domotica acquistata da Google nel 2014 per 3,2 miliardi di dollari, ha lanciato nelle scorse settimane una video camera, offerta on-line a 199 dollari e servizio gratuito di storage delle immagini su cloud per 30 giorni (vedi www.securindex.com <http://www.tuttoandroid.net>). Dal vostro punto di vista, come evolverà il mercato della sicurezza residenziale? Quali saranno gli spazi e le modalità di proposta per le soluzioni tradizionali, con l'impianto progettato e installato da operatori specializzati?

Giudichiamo in modo assolutamente positivo l'ingresso nel mercato da parte di colossi di questo calibro. In un mercato dove meno del 15% degli immobili sono dotati di un "qualche" sistema di sicurezza, non ci preoccupa affatto l'ingresso di nuovi players. La sicurezza va concepita come un processo senza fine. La piccola telecamera acquistata su e-bay non rappresenta impianti "tradizionali" venduti in meno, ma venduti in più domani. Non si torna indietro rispetto al livello di sicurezza percepita raggiunto e tutti ne abbiamo bisogno: altrimenti nemmeno chiuderemo la porta di casa, mentre risulta che tutti lo facciamo. E' chiaro che oggi la tecnologia offre delle soluzioni "entry level" che ieri non esistevano. Questo tuttavia avvantaggia l'installatore tradizionale in quanto si trova a confrontarsi con un utente finale che ha già palesato la sua esigenza e che domani vorrà qualcosa di più che una semplice telecamera stand alone. Di sicuro, chi ha acquistato un sistema "completo" è in grado di capire quali sono i limiti di una soluzione compatta "all-in-one" e, in particolare, di giudicare la loro inadeguatezza rispetto alle proprie esigenze. Non



si deve tuttavia parlare di "nicchie del mercato" ma, piuttosto, di percorsi che il consumatore oggi può fare per arrivare a soddisfare in pieno le proprie esigenze.

Di fronte a queste evoluzioni del mercato, quale sarà l'impatto delle norme a tutela dei consumatori, ad esempio a proposito dell'adeguatezza delle soluzioni adottate per la messa in sicurezza dell'abitazione?

Dal punto di vista pratico, il concetto di "funzionamento inadeguato", introdotto nelle norme a tutela dei consumatori, si risolve con uno scritto, una sorta di accettazione da parte dei clienti finali dei limiti tecnici di un prodotto di sicurezza. In pratica deve essere l'utilizzatore che dichiara l'adeguatezza al rischio di quanto acquistato. Non può e non deve essere l'installatore il quale, solo in seconda battuta, una volta definito il rischio (possibilità per danno), proporrà una soluzione adeguata. Tuttavia, questo quadro avvalorerà ancora di più il fatto che un sistema di sicurezza vada

progettato e realizzato con l'ausilio di un professionista. Le competenze richieste non possono essere solo di natura elettronica e informatica ma anche, senza voler esasperare il concetto, di criminologia e, in definitiva, di "psicologia del furto".

La differenza sostanziale tra calcolare il "rischio incendio" e il "rischio furto" sta proprio in questo. Il calcolo del carico di incendio e del relativo rischio è presto fatto, avendo i dati in ingresso. Diversamente, nel calcolo del rischio furto va tenuto presente che non esiste la casualità ma abbiamo a che fare con una "mente negativa", che cercherà il modo per introdursi nella rete, prendere il controllo dei vostri NVR, centralizzare le immagini della sala riunioni verso un server esterno e vendere le informazioni raccolte ad un vostro concorrente. Forse fantascienza, ma non troppo. Quello che voglio dire è che un professionista è e rimarrà sempre il tassello fondamentale nel processo di offerta e installazione di un sistema di sicurezza.

L'ecosistema HomeControl+ Pyronix: controllo via IP per il XXI secolo

a cura della Redazione

I progressi nelle tecnologie della comunicazione hanno aperto un mondo di interconnettività per i sistemi di sicurezza tradizionali. In questo contesto si inserisce l'ecosistema HomeControl+. Tale sistema innovativo riunisce in sé quattro tecnologie chiave: tecnologia cloud, antifurto e domotica, streaming video, smartphone.

L'ecosistema HomeControl+ è compatibile con una serie di accessori come: il premiato sistema wireless Enforcer 32WE-APP e il pannello di controllo ibrido PCX 46-APP, entrambi dotati di moduli di comunicazione GPRS o LAN; le telecamere HomeControl+ LAN/WIFI esterne (XCAM/S) e interne (ICAM/PT); l'APP HomeControl+ per smartphone iOS e Android; e l'infrastruttura PyronixCloud. Tutti gli elementi utilizzano una rete IP cablata o wireless, garantendo flessibilità e facilità d'uso per utenti e installatori, in ambienti domestici o commerciali di piccole dimensioni.

Per apprezzare appieno la tecnologia di questo ecosistema è importante conoscerne i componenti chiave.

Per iniziare, PyronixCloud rappresenta un'infrastruttura gateway online sicura e criptata, che collega tutti gli elementi del sistema all'utente e all'installatore. PyronixCloud consente le autorizzazioni di password e utente tra i componenti di sicurezza (Enforcer 32W-APP e PCX46-APP) e i componenti video (telecamere XCAM/S e ICAM/PT) nelle app HomeControl+. Gli utenti possono quindi vedere lo streaming video live sui loro smartphone e controllare in remoto il loro sistema di sicurezza da qualsiasi luogo del mondo. Grazie al cloud, gli installatori possono accedere a distanza ai sistemi, per attività



di programmazione e assistenza in remoto.

PyronixCloud integra due interfacce utente: una è dedicata all'utente finale e consente di gestire autonomamente sistemi di furto, sistemi video, abbonamento a cloud, notifiche push e smartphone; la seconda è dedicata agli installatori e consente di gestire un ampio numero di sistemi video e furto, abbonamenti, notifiche push e utenti. In questo modo, oltre ad essere un'interfaccia di gestione online e un gateway per le comunicazioni, PyronixCloud rappresenta uno strumento unico per gli installatori, che possono così offrire assistenza ai loro clienti. Inoltre, tramite il cloud gli installatori italiani potranno personalizzare l'app HomeControl+ con il loro logo. Questo è un altro esempio di come Pyronix studi soluzioni ponendo sempre l'installatore in primo piano. La seconda parte dell'ecosistema è l'app HomeControl+ disponibile in due versioni: Android e iOS. L'APP consente il controllo remoto del sistema di antifurto e la trasmissione dello streaming live del video ripreso dalle telecamere. Di fatto, l'APP trasforma lo smartphone dell'utente in una tastiera



touch. Gli utenti possono inserire/disinserire i loro sistemi, visualizzare lo stato del sistema, escludere sensori, interrogare la memoria di eventi e attivare dispositivi remoti come luci, irrigatori e cancelli, utilizzando fino a 30 uscite di domotica programmabili. Se la facilità d'uso e d'installazione sono importanti, il fulcro dell'ecosistema rimane la sicurezza: nello sviluppo di prodotti che sfruttano gli ultimi ritrovati della tecnologia in termini di protezione e crittografia, Pyronix si impegna a mantenere il proprio ethos. Le comunicazioni tra APP e cloud sono protette da un protocollo di crittografia SSL a 128 bit, mentre le comunicazioni tra app e impianto sono protette da crittografia AES a 256 bit. L'APP HomeControl+ e il cloud sono inoltre dotati di opzioni di sicurezza aggiuntive, come una protezione con password a due livelli. Inoltre, le informazioni sensibili relative all'utente non vengono raccolte né salvate su PyronixCloud. L'ultimo elemento dell'ecosistema HomeControl+ è

l'apparecchio fisico montato presso i locali dell'utente. I componenti disponibili sono la centrale wireless bidirezionale Enforcer 32WE-APP, la centrale ibrida PCX46-APP e l'ultima novità della gamma, ovvero le telecamere HomeControl+. Le centrali possono comunicare con PyronixCloud attraverso i loro moduli di comunicazione GPRS o LAN, mentre le telecamere comunicano tramite le interfacce LAN e WIFI integrate. Queste telecamere IP sono facili da installare nella rete e non richiedono la programmazione del router situato presso i locali dell'utente. Pyronix continua a creare prodotti in grado di soddisfare le necessità e le richieste del mercato, realizzando opzioni innovative per gli installatori. Essere sulla cresta dell'onda è cruciale per Pyronix. La capacità di integrare le nuove tecnologie nei propri prodotti caratterizza l'azienda britannica fin dai suoi inizi nel 1986. L'ecosistema HomeControl+ è l'ultima innovazione che ridefinisce gli standard dei tradizionali sistemi antintrusione.



CONTATTI - PYRONIX
www.pyronix.com
Tel. +44 (0)1709 700 100

Kaba 'Food Defence': più sicurezza nella produzione alimentare

a colloquio con l' Ing. Luca Negrini, Country Manager di Kaba Italia
a cura della Redazione

Quale è il ruolo della security nella certificazione per lo Standard IFS Food V6?

In questo settore di mercato, la Security deve avere un ruolo proattivo. Infatti tutti i processi, per avere una "defense" del prodotto, devono passare anche per l'implementazione di procedure di security indirizzate a vari ambiti:

- ai visitatori del sito, al fine di non permettere la loro promiscuità con le zone produttive dove essi non sarebbero sicuramente attrezzati di tutti i vari DPI o comunque permetterne l'accesso solo dopo che tali DPI sono stati espletati, chiaramente con un controllo sulle tempistiche in cui i visitatori possono accedere e/o permanere nei siti;
- verso i contractor e, in generale, i fornitori, i cui flussi di accesso devono esser controllati e soprattutto tracciati, in modo da poter dimostrare la reale efficienza della protezione;
- i propri dipendenti, che in base ai livelli organizzativi, possono o meno accedere a dati e zone o reparti produttivi;
- infine supportare la produzione contro gli attacchi dall'esterno, implementando procedure e sistemi di monitoraggio che, in tempo reale, mandino in allarme il plant produttivo e/o di stoccaggio in caso di rischi di intrusioni esterne.

Perché è importante per un'azienda del settore alimentare definire un piano strutturato e integrato di Safety/Security? Quindi quale impatto ha oggi la Security nei processi produttivi delle aziende del settore alimentare?

E' molto importante in primo luogo per poter definire

le procedure da attuare nello svolgimento del lavoro quotidiano, in modo da renderlo estremamente più rapido ed efficiente, salvaguardando al contempo Safety & Security.

Di estrema importanza è poi la tracciatura di ciò che avviene, in modo da supportare l'azienda con dati ed evidenze precise in caso di una qualunque contestazione.

È chiaro che in questo contesto le problematiche legate alla Safety & Security si fondono in modo determinante. Occorre infatti parlare di sicurezza a "380" gradi cioè tesa nel tempo grazie ai processi di Safety & Security alla prevenzione più che alla semplice difesa, portando quindi un reale ROI all'azienda.

Le soluzioni Kaba, come aiutano ad adempiere ai requisiti previsti dalla certificazione IFS?

Certezza sulle responsabilità, ottimizzazione dei processi, miglioramento della misurazione e capacità di analisi, sono solo alcuni dei benefit per le aziende che adotteranno una sicurezza più strutturata, in linea con questi standard.

Direi che quelli citati sono i principali benefici di una soluzione di Safety & Security integrata.

Kaba aggiunge a questo altri vantaggi per il cliente:

- assoluta ed indiscussa leadership tecnologica nel campo della Security Fisica e del Work Force Management (WFM): siamo in grado di realizzare progetti trasversali che coinvolgono nella "difesa" le due aree principali di un'azienda, HR e Security;
- garanzia dell'investimento per il cliente grazie sia alla forza del nostro Brand ma, oggi molto più importante, grazie alla nostre ampia capacità



finanziaria ed organizzativa. Siamo presenti non solo in tutta Italia, ma in tutto il mondo per supportare il roll-out di progetti anche oltre i nostri confini. Nel prossimo futuro, grazie alla fusione con Dorma in pianificazione, diventeremo il terzo Gruppo al mondo nella Security fisica e Work Force Management;

- grande esperienza e referenze, grazie alla certificazione Golden Partner di SAP, in impianti di grande e media dimensione nell'ambito industriale per la sicurezza, per il WFM e per le soluzioni di Production Plan and Management.

La manutenzione periodica dei sistemi tecnici di sicurezza inoltre, è molto rilevante per le normative in materia di prodotti alimentari.

Come espresso in precedenza, la tracciatura di quanto avviene è, come in tutte le certificazioni, di vitale importanza: deve esser precisa, molto dettagliata e con grande profondità storica. Di conseguenza, gli impianti devono esser continuamente controllati per non subire mai blocchi che portino alla mancanza di storicizzazione degli eventi oltre che, chiaramente, al controllo. Inoltre, ormai è d'obbligo parlare di 'manutenzione evolutiva'. Visti i continui aggiornamenti procedurali e tecnologici, il progetto non può più nascere e finire ma deve continuamente evolversi sia sul piano dei processi che su quello delle tecnologie che, oltretutto, tendono ad una obsolescenza oggi molto più rapida che in passato. Ecco perché, attualmente, un progetto che vive di una manutenzione evolutiva costa assai meno nel tempo, rispetto ad un progetto che nasce, non

viene più mantenuto e poi arriva ad un punto in cui deve esser completamente ricostruito.

Quale sensibilità ritiene ci sia su questi temi e come si stanno muovendo le aziende del settore?

Sul discorso in sé del Food Defense esiste ormai una grande sensibilità sul mercato. Abbiamo notato, visitando molti nostri clienti con soluzioni di sicurezza Kaba e che operano nel settore alimentare, che manca spesso il "LINK" tra la Food Defense, che viene vista più come un progetto legato alla Qualità, e la difesa fisica dei plant.

Solo parlando con loro di questi aspetti si sono accorti come in effetti fosse importante inserire la parte "security" nel processo di Food Defense.

La ragione principale della nostra campagna è proprio quella di sollecitare il "LINK" tra il concetto tipicamente qualitativo di Food Defence con quello della "Difesa Fisica" (Safety&Security) del plant produttivo e di stoccaggio.

CONTATTI - KABA
www.kaba.it/ifs-food
info.it@kaba.com
Tel. +39 051 4178311

La videosorveglianza più evoluta entra nel mondo DIAS con SUNELL

a cura della Redazione

DIAS, punto di riferimento per le più qualificate aziende di distribuzione di prodotti e sistemi di sicurezza professionale, ha recentemente siglato una partnership commerciale per la distribuzione esclusiva in Italia dei prodotti SUNELL, società leader nel mercato della videosorveglianza.

Questo importante accordo consente a DIAS di offrire, tramite la rete dei propri distributori, una gamma completa per la videosorveglianza più evoluta, dalle telecamere analogiche a 1000 linee alle soluzioni over IP, sia entry level che professionali, fino agli NVR di ultima generazione. Prodotti eccellenti caratterizzati da un ottimo rapporto prezzo-prestazioni, in grado di farsi apprezzare da molte fasce di utenti in numerosi contesti. Andiamo dunque a conoscere nel dettaglio alcuni dei prodotti che appartengono a questa straordinaria gamma.

Telecamera Bullet SN-IPR54/40AKDN

Partiamo dalla telecamera Bullet SN-IPR54/40AKDN. Dotata di un sensore APTINA CMOS da 1/2,5" con 2592 x 1920 pixel effettivi (5 MegaPixel), questa nuova telecamera è in grado di produrre immagini a colori fino a 0.5 Lux di illuminazione e grazie alla sua dotazione di LED IR ad alta potenza (14 LED IR SuperFlux e 3 LED IR Giant) riesce a garantire una visione monocromatica in totale assenza di luce fino a 50 metri di distanza. Il protocollo IP ONVIF 2.2 Profilo S la rende compatibile non solo con gli NVR della serie SUNELL, ma anche con la maggior parte dei software di gestione VMS (Video Management System) presenti sul mercato. L'ottica Varifocale DC IRIS da 3.3-12mm con correzione IR ne permette l'utilizzo in qualsiasi tipologia di scena, rendendo



estremamente semplici le regolazioni tramite comode viti esterne alla telecamera stessa; un'uscita CVBS integrata garantisce la possibilità di verificare queste regolazioni su un semplicissimo monitor analogico. Questa telecamera dispone inoltre di uno slot per l'inserimento di una scheda SDHC che, garantendo la possibilità di effettuare una registrazione locale di immagini o filmati di allarme, la rende un sistema completo e autonomo, in grado di funzionare anche solo alimentata a 12VCC o tramite un cavo Cat5e o Cat6 dotato di alimentazione PoE 802.3af Class 3 avendo un consumo massimo di 12W. Tutte queste caratteristiche rendono la telecamera Bullet SN-IPR54/40AKDN di SUNELL una soluzione ideale per la visione ad altissima risoluzione sia durante il giorno sia durante la notte.

CARATTERISTICHE

- Telecamera Bullet IP 5 Mpixel
- Sensore Sony Aptina da 1/2,5" CMOS
- Pixel effettivi 2592x1920@10fps, 2048x1536@20fps, 1920x1080p@25fps
- True Day/Night ICR

- Ottica Varifocale 3.3÷12mm con regolazioni ZOOM e FOCUS dall'esterno
- 14 LED IR SuperFlux e 3 LED IR Giant con portata 50 metri
- Movimento della staffa su 3 assi
- BNC di servizio per la taratura
- Ingresso e uscita Audio
- Slot Micro SD a bordo
- Alimentazione 12VCC – PoE
- Grado di protezione IP66

Telecamera Mini Speed Dome 3 Mpixel SN-IPS56/30CDR

Un design unico e la straordinaria affidabilità dei prodotti SUNELL portano all'attenzione degli operatori più qualificati questa questa nuovissima telecamera compatta, che entrerà in gamma nei mesi. Dotata di un processore Ambarella e di un sensore Day/Night IRC da 3 MegaPixel CMOS, equipaggiata con un'ottica Zoom Motorizzata 12X e due potenti illuminatori a LED IR integrati nella sua forma sferica, questa nuova Mini Speed Dome permette di ottenere immagini chiare e definite in modalità monocromatica fino a 60 metri di distanza nella più profonda oscurità. L'alimentazione integrata PoE e la capacità di fornire uno stream standard ONVIF 2.4 Profilo S rendono la telecamera SN-IPS56/30CDR adatta a qualsiasi applicazione, non solo tramite la nuova linea di NVR integrati di SUNELL, ma anche mediante l'utilizzo di una vasta gamma di Software VMS o di sistemi NAS dedicati alla registrazione di flussi video di sicurezza. SUNELL fornisce anche tutti gli accessori progettati per realizzare una semplice e veloce installazione dei prodotti. La Nuova Mini Speed Dome SN-IPS56/30CDR si avvale dunque di tutta la gamma di staffe e box di interfaccia che



permettono agli installatori specializzati di poter eseguire velocemente il montaggio a parete, a palo, sugli spigoli degli edifici o in modalità pendente da soffitto, con risultati estremamente soddisfacenti sia dal punto di vista funzionale sia dal punto di vista estetico.

CARATTERISTICHE

- Telecamera Speed Dome IP 3 Mpixel
- DSP Ambarella e sensore CMOS 3 Mpixel
- True Day/Night ICR
- Ottica ZOOM 12x
- 2 LED IR ad alta potenza con portata 60 metri
- Slot Micro SD a bordo
- Alimentazione 12VCC – PoE
- Grado di protezione IP66

NVR Serie SN-NVR10 compatto



Il nuovo NVR Serie SN-NVR10 compatto di SUNELL rappresenta la soluzione ideale per piccoli negozi e abitazioni di prestigio. Questo prodotto coniuga infatti la tecnologia più evoluta con un design discreto ed elegante che lo rende adatto anche agli ambienti più ricercati.

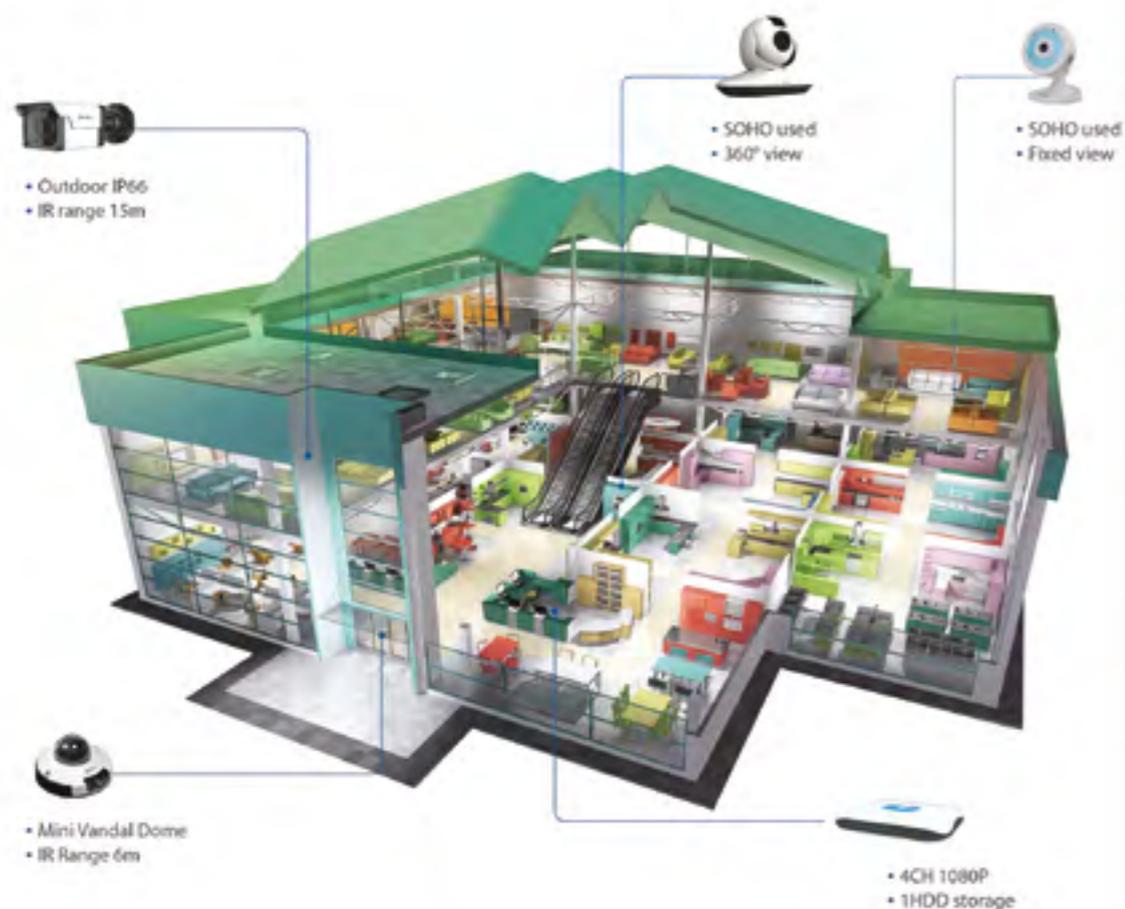
Questo nuovo NVR è in grado di registrare fino a quattro telecamere con risoluzione 1080P Full HD ad esso collegate, fornendo alimentazione tramite la tecnologia PoE (Power Over Ethernet) direttamente sull'unico cavo di rete; esso è infatti dotato di uno Switch PoE integrato a quattro porte con standard 802.3af in grado di erogare potenza sufficiente per qualsiasi telecamera del range SUNELL. Grazie all'uscita video in formato VGA o HDMI, alle funzionalità di configurazione e acquisizione automatica delle telecamere ad esso collegate, alla gestione tramite mouse e alla grande capacità degli Hard Disk inseribili all'interno del sistema,

l'NVR compatto di SUNELL garantisce un'altissima qualità di registrazione e visualizzazione, con tempi di installazione realmente ridotti al minimo.

A corredo di questo prodotto sono disponibili diversi tipi di telecamere adatte a qualsiasi utilizzo ed una suite di software di gestione per PC o dispositivi mobili (iOS e Android).

CARATTERISTICHE

- NVR compatto da 4 canali Full HD@ 4.5 Mbps per canale
- Registrazione e riproduzione in tempo reale anche in modalità QUAD
- Switch integrato PoE da 4 porte standard 802.3af
- Uscita VGA o HDMI
- Configurazione automatica
- Gestione tramite mouse
- Singolo Alimentatore 230VAC/48VCC incluso



CONTATTI - DIAS
www.dias.it
 Tel. +39 02 3803 6901

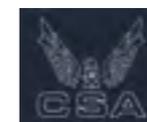
Security for Retail

78 Cash-management, parte dall'Italia la leadership di Gunnebo nel Retail

a colloquio con Marco Depaoli, Retail Business Director Region South Europe di Gunnebo
 a cura di Raffaello Juvara

80 Intelligent Article Surveillance: Adidas innova con le soluzioni intelligenti RFID-ready di Nedap

a cura della Redazione



Cash-management, parte dall'Italia la leadership di Gunnebo nel Retail

a colloquio con Marco Depaoli, Retail Business Director Region South Europe di Gunnebo a cura di Raffaello Juvara

Ingegnere Depaoli, lei è stato recentemente nominato da Gunnebo Retail Business Director Region South Europe. Oltre al riconoscimento per le sue competenze, quale strategia del gruppo indica questa nomina?

Prima di tutto vorrei ringraziare tutti i dipendenti di Gunnebo Italia che hanno contribuito alla mia nomina permettendo all'Italia di assumere la responsabilità del Business Retail per la Spagna, il Portogallo e naturalmente per l'Italia. È il riconoscimento per i risultati ottenuti in termini di crescita profittabile della Divisione Retail in Italia e, in particolare, nelle soluzioni di cash management. La strategia del gruppo è di esportare l'esperienza di successo e la competenza italiana anche negli altri paesi, con la focalizzazione sulle soluzioni di trattamento denaro.

I sistemi di cash-management si stanno diffondendo in tutte le tipologie di PDV, dai supermercati ai negozi di prossimità. Quali sono le principali esigenze espresse dai gestori?

Occorre precisare che Gunnebo intende per soluzioni di cash management quelle che trattano il denaro a partire dal punto cassa sino al back office, per arrivare alla sala conta e all'accredito diretto del denaro in banca. Sicuramente, la soluzione di cash handling a ciclo chiuso (trattamento denaro sia sul punto cassa che sul back office) è quella che offre più vantaggi per il retailer, ed è la più idonea e performante nell'implementare il cash management. Le esigenze espresse dai gestori sono diverse in funzione del format del PDV e della zona geografica dove il PDV è localizzato. Riassumo le più importanti: riduzione



costi attraverso la semplificazione e la velocizzazione del processo del cash partendo dal PDV sino alla sala conta, recupero di efficienza sul PDV e sul trasporto valori, incremento della sicurezza con eliminazione delle rapine ed accredito diretto del contante in banca. La soluzione di cash management introduce nel PDV una notevole innovazione sul processo del contante, e permette al retailer di rientrare sull'investimento in tempi brevi.



Quali sono le proposte di Gunnebo per il 2015, sia per i grandi retailer che per i piccoli negozi?

Le soluzioni di Gunnebo permettono di soddisfare le esigenze e le aspettative di tutti i format di PDV: ipermercato, superstore, supermercato, hard discount, cash & carry, catene specializzate, negozio di prossimità e singolo negozio. Tutte le soluzioni possono operare in versione stand-alone oppure in rete, utilizzando un pacchetto software che permette di collegare tra di loro tutte le macchine anche differenti, in funzione del format del PDV. Questo pacchetto software rende disponibile in tempo reale ogni transazione e ogni tipo di report per il retailer (sia sul singolo PDV che a livello di sede centrale), per il trasporto valori e per la banca. Lo stesso pacchetto pure include e supporta l'attività di help desk e di assistenza remota.

SaaS, ovvero security as a service: ritiene che questa modalità, che arriva nella sicurezza provenendo dal mondo IT, abbia possibilità di applicazione anche nel campo della gestione del denaro nella distribuzione, includendo anche altri attori, come CIT e banche? Parlerei di cash handling a ciclo aperto (trattamento del denaro solo sul back office) 'as a service' dove nel servizio sono incluse le macchine di back office con relativa installazione e manutenzione. Inizialmente

questo concetto è stato proposto da alcune società di trasporto valori e da alcune banche. Questo approccio al mercato vincola il retailer a siglare contratti pluriannuali ed al tempo stesso impone al fornitore del servizio elevati investimenti per l'acquisto delle macchine con rientri non sempre nei tempi desiderati e con notevoli costi manutentivi. La tendenza è di modificare l'offerta iniziale offrendo un servizio che non includa più le macchine. Vorrei infine sottolineare che la soluzione di cash handling a ciclo aperto implementa solo parzialmente il cash management e di conseguenza offre minori vantaggi al retailer.

Quali sono le prospettive per l'integrazione intersistemica nei PDV, dal punto di osservazione multinazionale che ha Gunnebo?

Gunnebo propone una offerta multi soluzione per il PDV: sicurezza fisica, sicurezza elettronica, cancellotti e cash management. Gunnebo è leader di mercato nella sicurezza fisica e nel cash management a ciclo chiuso. Non ci sono problemi per eseguire l'integrazione di queste soluzioni nel PDV, che aumentano ulteriormente il valore ed il vantaggio per il retailer.



CONTATTI - GUNNEBO
www.gunnebo.it
Tel. +39 02 267101

Intelligent Article Surveillance: Adidas innova con le soluzioni intelligenti RFID-ready di Nedap

a cura della Redazione

L'ESIGENZA

Adidas, multinazionale tedesca, specializzata nella produzione e distribuzione di articoli sportivi per dilettanti e professionisti, con oltre 2000 punti vendita nel mondo, continua il piano di espansione retail globale attraverso negozi monomarca in grado di raccontare la filosofia e lo stile del brand grazie al design, ai colori, alle collaborazioni artistiche e all'innovazione tecnologica. Proprio dalla volontà di fornire esperienze uniche e sempre nuove ai propri clienti nasce l'esigenza di uniformare l'immagine dei nuovi concept store, standardizzando i sistemi di protezione attraverso soluzioni EAS innovative e future-oriented, in grado di integrarsi perfettamente al design dei punti vendita senza intaccarne il look&feel.

La recente apertura del nuovo Flagship Store Adidas Originals a Milano, quinto nel mondo dopo Londra, Berlino, Shangai e Seoul, ha visto la collaborazione di **Nedap Italy** per la fornitura di sistemi EAS di nuova generazione RFID-ready, confermando la partnership tra i due brand anche sul mercato italiano.

LA SOLUZIONE

Per la protezione del **nuovo flagship store di Milano**, Adidas ha scelto la nuova soluzione Nedap !Sense per la Sorveglianza Intelligente degli Articoli (IAS), con installazione delle antenne RFID-ready i45 all'ingresso. **!Sense** è il primo e unico sistema IAS sul mercato, completamente scalabile e IP based, che aiuta i retailer a prevenire le perdite in modo efficace, permettendo di integrare l'EAS nella rete di sicurezza esistente e raccogliere dati di immediato valore pratico direttamente dai punti vendita, 7 giorni su 7 e 24 ore su 24, in tutto il mondo. Tramite i sensori intelligenti



integrati nelle antenne i45, la piattaforma !Sense raccoglie informazioni su allarmi RF ed RFID, metal detector, borse schermate e contapersone. Il design avanzato dei sistemi i45, con pannelli pubblicitari integrati, contribuisce a creare un ambiente invitante e accogliente, mantenendo l'ingresso al punto vendita privo di ingombri e garantendo al contempo prestazioni di rilevazione ottimali. Supportando due tecnologie (RF e RFID), le antenne i45 permettono di colmare il divario tra la tecnologia attuale e futura: grazie al modulo RFID clip-in integrato, i retailer possono migrare in qualunque momento da una tecnologia all'altra, senza dover intervenire sul sistema installato o sul design del punto vendita.

Gestita interamente via software, la piattaforma !Sense consente di connettere facilmente i sistemi EAS al gestionale del retailer e ad ogni dispositivo network based che comunica tramite i protocolli supportati, come le telecamere di videosorveglianza. La connettività dà informazioni in tempo reale sulle prestazioni dei sistemi e i potenziali rischi per la



sicurezza attraverso la dashboard in-store, collocata nella centrale Renos di ogni antenna. Il sistema di reporting centralizzato Retail Analytics, disponibile via web o come app per smartphone e tablet, consente di monitorare e confrontare nel lungo periodo tutti i punti vendita connessi attraverso report di facile utilizzo che rendono più visibili e controllabili le cause alla base delle perdite e delle differenze inventariali.

Con la Teleassistenza i sistemi vengono monitorati da un team di tecnici dedicato tramite un'interfaccia di monitoring, attiva 24 ore su 24, che ne consente la gestione e la manutenzione da remoto, permettendo una maggiore efficienza e un notevole risparmio economico poiché i costi e i fastidi degli interventi on-site sono azzerati. I disattivi intelligenti, connessi on-line e integrati nel banco cassa, prevengono i falsi allarmi grazie a performance di rilevazione e disattivazione superiori (fino a 30 cm) e, disattivando le etichette solo nel momento in cui vengono rilevate, consentono di ridurre i consumi energetici e snelliscono le operazioni di cassa. Infine, etichette adesive e rigide testate al 100% garantiscono la più elevata qualità di rilevazione e consentono di ottenere la massima resa dal sistema EAS installato.

I VANTAGGI

“Per l'importante opening del nuovo flagship store Adidas Originals a Milano, parte di un più ampio programma di espansione retail che prevede l'apertura di 30 monomarca nei principali centri culturali e di tendenza del mondo, Adidas necessitava di un partner tecnologico in grado di mantenere gli stessi elevati standard qualitativi garantiti in tutte le aree retail internazionali e assicurare un servizio preciso e puntuale unitamente alla massima versatilità e flessibilità delle soluzioni di protezione installate. La scelta è caduta nuovamente sull'expertise e il service esclusivo di Nedap”, afferma **Federico Saini, Profit Protection Manager South Europe di Adidas Group**. “L'estetica, il design avanzato e la tecnologia innovativa delle soluzioni Nedap incontrano la nostra esigenza di creare spazi multifunzionali capaci di fornire ai nostri clienti esperienze sempre nuove ed entusiasmanti. Le antenne i45 si integrano perfettamente nel design del punto vendita e, oltre a garantire performance di rilevazione ottimali, ci consentono la massima scalabilità, potendo essere facilmente upgrate a tecnologia RFID qualora necessario. I pannelli pubblicitari integrati attraggono l'attenzione dei clienti aumentando l'esposizione del

brand. Grazie alla dashboard in locale e al sistema di reporting centralizzato, abbiamo la possibilità non solo di raccogliere informazioni dai sistemi connessi all'interno del singolo negozio, ma di ottenere una panoramica in tempo reale su tutti gli aspetti che influenzano la gestione dei punti vendita a livello globale: ciò consente di identificare più facilmente eventuali problemi e intervenire tempestivamente sulle minacce alla sicurezza, prendendo i provvedimenti opportuni per eliminare le perdite e aumentare i profitti".

"La conferma di Nedap Italy come partner tecnologico in ambito EAS da parte di Adidas Group ci riempie di soddisfazione", afferma **Mauro Barosi, Managing Director di Nedap Italy Retail**. "Il nuovo flagship store Adidas Originals, inaugurato la scorsa primavera in C.so Como a Milano, si configura come un'eccellenza nel nostro portfolio, non solo per la rilevanza del punto vendita e del brand, ma anche perché è il primo store italiano a implementare la nostra nuova

soluzione **IAS !Sense** completa, con antenne i45 ibride che supportano sia la tecnologia RF che RFID. L'applicazione sul campo di soluzioni pionieristiche di Sorveglianza Intelligente degli Articoli, che permettono di ottenere dati in tempo reale da tutti i sistemi connessi grazie a piattaforme di gestione in-store o centralizzate, frutto d'ingenti investimenti in ricerca e sviluppo, ci consente non solo di osservare come le nuove tecnologie vengano efficacemente impiegate dai nostri clienti per migliorare le proprie performance, ma anche di studiare insieme nuove applicazioni in un'ottica di innovazione continua. Lo spirito future-oriented e l'attenzione al design ed alle performance dei sistemi di protezione espressa dal management Adidas si riflettono a pieno nell'avanguardia tecnologica delle soluzioni adottate. Ci auguriamo fortemente di continuare la nostra collaborazione con Adidas per fornire in futuro soluzioni sempre più innovative, user-friendly e customizzate".

Informazioni su Adidas

Con più di 53.731 dipendenti in oltre 160 paesi, Adidas produce circa 660 milioni di unità di prodotto ogni anno, generando vendite per 14,5 miliardi di euro (dati 2014). La storia di ciascun marchio del gruppo trae origine dalla grande passione per lo sport e uno stile di vita attivo. Tutti i brand Adidas si completano l'un l'altro per aiutare atleti, dilettanti o professionisti, a dare il meglio di sé e a sentirsi perfettamente a proprio agio grazie a prodotti innovativi e distintivi. Con dedizione, impegno e spirito di squadra, Adidas innova costantemente perseguendo l'obiettivo di essere il leader globale nell'industria degli articoli sportivi.

Informazioni su Nedap

Nedap crea tecnologie intelligenti ad alto valore aggiunto, con un impatto concreto sul progresso sociale. Le soluzioni Nedap sono mirate alla risoluzione delle grandi problematiche globali: cibo a sufficienza per una popolazione in continua crescita, acqua potabile nelle zone che ne sono prive, sistemi intelligenti per il risparmio energetico. Ecco come Nedap interpreta la sua mission di creare "tecnologia che fa la differenza". Nedap, fondata in Olanda nel 1929 e quotata alla Borsa Euronext dal 1949, impiega oltre 730 dipendenti ed è presente in tutto il mondo con filiali e partner certificati. Nedap aiuta i retailer a ridurre in maniera permanente le differenze inventariali, ottimizzare i livelli di stock e semplificare la gestione delle catene retail. In altre parole, Nedap rende più profittevoli i punti vendita.



CONTATTI - NEDAP
www.nedapretail.it
Tel. +39 02 2670 8493

La manutenzione dei presidi antincendio, una sicurezza da certificare contro le frodi

a colloquio con Federico Pasqui, Responsabile Area Sistemi di Gestione ICIM SpA
a cura della Redazione

La manutenzione dei presidi antincendio, un comparto dalle dimensioni ragguardevoli dal punto di vista economico e di estrema importanza per la sicurezza delle persone, sta affrontando un percorso contro le frodi, sempre più diffuse. Qual è la posizione di ICIM al riguardo e quali sono le iniziative poste in essere?

La normativa italiana è molto chiara e severa riguardo alla prevenzione e alla sicurezza antincendio: i decreti legislativi e le norme nazionali hanno contribuito a costruire un unico "sistema" che parte dalle caratteristiche delle strutture e degli impianti e coinvolge varie figure – committenti, tecnici, responsabili sicurezza, manutentori, ecc. – al fine di garantire una complessiva gestione del rischio d'incendio che, seguendo criteri oggettivi e processi condivisi, sia efficace, economica e "sicura". Siamo dunque alla presenza di un quadro normativo che, seppur ancora migliorabile, non lascia spazio a "interpretazioni". Mancare di rigore nella manutenzione dei presidi fondamentali quali gli estintori, le reti idranti o le porte resistenti al fuoco si traduce in un vero e proprio attentato alla sicurezza delle persone. E la parola "frode" è tanto più appropriata dal momento che il danno si estende anche al bilancio di tutte quelle aziende del comparto che lavorano secondo le regole. ICIM - quale ente di certificazione di terza parte che lavora da anni nel settore e ne conosce appieno le problematiche - ha messo a punto uno strumento che va direttamente al cuore del problema: uno schema per la certificazione della manutenzione antincendio che è volontario e va ad affiancare i controlli previsti dagli Organi



dello Stato, segnalando l'efficienza e la correttezza degli operatori. La certificazione del servizio di manutenzione ha l'obiettivo di verificare che la manutenzione di estintori, idranti, porte tagliafuoco sia eseguita secondo criteri «di qualità» definiti. Le verifiche presso le aziende di manutenzione riguardano:

- le attrezzature per l'erogazione del servizio;
- i documenti e l'adeguatezza delle procedure operative;
- le registrazioni e la tracciabilità degli interventi;
- la gestione dei ricambi e del materiale di consumo (es. liquidi e polveri estinguenti);
- la verifica dello smaltimento dei rifiuti generati dai servizi di manutenzione;
- il bilancio tra materiali utilizzati e smaltiti, ecc.

Vengono presi in considerazione anche gli eventuali reclami dei clienti, un indice di controllo non trascurabile della qualità degli interventi.

ICIM utilizza, inoltre, un tool innovativo: un QR Code che non può essere contraffatto e che conferma la veridicità del marchio di certificazione riportato sul cartellino di manutenzione. Il codice, criptato e univoco, garantisce che il cartellino è attivo e originale. Abbiamo già certificato diverse aziende, (per un elenco dettagliato <http://www.icim.it>) Oltre alla certificazione del servizio di manutenzione, ICIM ha sviluppato vari schemi di certificazione per i prodotti antincendio (tra queste maniglie e cerniere di sicurezza per chiusure tagliafuoco, regolatori di chiusure e serrature meccaniche ecc.) ed è da anni tra gli organismi di certificazione di riferimento del settore a livello europeo, anche in ottemperanza all'applicazione delle direttive europee sui materiali da costruzione.

La provenienza geografica dei prodotti finiti e dei componenti si è dimostrata un fattore critico per la qualità dei presidi antincendio. In che modo la certificazione PPG, sviluppata da ICIM, garantisce gli standard qualitativi?

Nel nostro Paese "l'industria del falso" prospera e la certificazione di prodotto è oggi fondamentale anche nel settore antincendio, e più specificatamente, degli estintori, dove la contraffazione può avere conseguenze nefaste per la sicurezza delle persone nonché per il conto economico delle imprese. Lasciando agli organi proposti la lotta attiva alla contraffazione, ICIM può dare alle aziende un supporto oggettivo con la certificazione volontaria PPG, Prodotto di Provenienza Garantita, che unisce controllo sul campo e smart technology per dimostrare che il prodotto, impianto o servizio è stato realizzato e assemblato in Italia o in un paese dell'Unione Europea, con componentistica europea o italiana. Nel caso degli estintori, il prodotto viene dapprima verificato per la conformità, applicando il regolamento a tutti i singoli componenti (serbatoio, valvola, estinguente). In seguito, ancora una volta ci viene in aiuto la tecnologia che ICIM ha sviluppato

proprio per racchiudere tutti i dettagli riferiti alla certificazione: codifichiamo e crittografiamo tutte le informazioni relative al prodotto in un QR Code - stampato con delle tecniche che non consentono la falsificazione - che mostra la corrispondenza delle informazioni con quanto realmente dichiarato sul prodotto certificato da ICIM. Gli utenti tramite l'app dedicata - *QRTIFY™*, disponibile su *Apple Store*, *Google Play* e *Windows Store* e scaricabile su qualsiasi dispositivo mobile - possono conoscere di persona le informazioni contenute nel momento in cui il quadrato in bianco e nero che timbra ogni prodotto prende vita. La durata della certificazione è annuale per un'azienda di produzione di componenti e triennale per le aziende che gestiscono un prodotto finito: tutte hanno così la possibilità di proteggere il proprio marchio. Per i committenti, è una garanzia dell'originalità della merce acquistata. Abbiamo rilasciato il primo marchio PPG in Italia proprio agli estintori della Universo, un'azienda storica dell'antincendio nel nostro Paese.



Come è possibile informare l'utente finale del livello qualitativo reale dei presidi antincendio che si trovano installati nei luoghi in cui ne è prevista la presenza a tutela della sua sicurezza? È possibile coinvolgere l'utente finale nella survey del rispetto delle norme da parte dei gestori/responsabili dei luoghi "obbligati", ovvero dei fornitori? Quale ruolo possono giocare gli operatori professionali certificati?

E difficile pensare che l'utente finale possa essere direttamente informato del reale livello qualitativo

dei presidi antincendio installati negli uffici pubblici e privati, scuole, ospedali e, in generale, in tutte le situazioni in cui la legge prevede una tutela antincendio; in quest'ottica sarebbe molto interessante promuovere e favorire iniziative di formazione in materia di antincendio e di sicurezza fin dalle scuole primarie, così come avviene in molti paesi dove, anche per ragioni storiche, è più diffusa la "cultura antincendio". Ma è un processo culturale lungo e articolato. Riteniamo invece estremamente positivo lo sviluppo delle nuove norme per la certificazione professionale di figure chiave, quali gli addetti del settore antincendio, che offrono criteri oggettivi per poter affidare la manutenzione degli impianti a operatori qualificati. Quando la certificazione professionale degli addetti entrerà negli appalti per le gare di affidamento dei servizi di manutenzione, in particolare da parte dei grandi soggetti pubblici, si alzeranno automaticamente i livelli di tutela degli utenti finali. Nel settore, la prima figura professionale a essere riconosciuta è quella dei posatori e manutentori di chiusure resistenti al fuoco e/o per il controllo del fumo, che ora possono certificarsi secondo la UNI 11473-3, una norma che completa e integra la legislazione in materia antincendio e che è stata sviluppata per disciplinare le figure professionali non regolamentate.



ESTINTORE

I professionisti dell'antincendio sono, infatti, tra coloro che non hanno una figura definita a livello legislativo. Al momento rilasciata in Italia esclusivamente da ICIM, primo organismo di certificazione accreditato da Accredia, la certificazione UNI 11473-3 è volontaria e sarà presto affiancata dalle certificazioni professionali per i manutentori di estintori e crediamo in futuro anche di altri dispositivi quali le reti idranti, i dispositivi di evacuazione fumi, ecc. L'adeguata manutenzione non può prescindere da una corretta qualificazione degli operatori, e queste norme contribuiscono a definire criteri oggettivi per certificare gli operatori competenti.

CONTATTI - ICIM
www.icim.it
Tel. +39 02 725341

securindex.com

Il primo portale italiano per la security

Cultura e Formazione

87 I racconti della Sicurezza - 2

di Giulia Lazzeri - tratto dalla rivista "EHF-Sicurezza per la cultura", organo ufficiale della Fondazione Enzo Hruby, anno XXII, n.1 dicembre 2012-marzo 2013

88 Una borsa di studio per il miglior studente del progetto Campus Came nel ricordo di Paolo Tura

a cura di Raffaello Juvara

89 essecome, il "giochino" di Paolo nel ricordo di Valerio

a colloquio con Valerio Tura

91 100 studenti e 20 insegnanti coinvolti nel primo anno di Campus Came

a colloquio con Elisa Menuzzo, Vice Presidente Came S.p.A.

CAME
safety&comfort

FONDAZIONE
ENZO HRUBY

FONDAZIONE
LHS
LEADERSHIP IN HEALTH & SAFETY

e GazzoliEngineering

I racconti della Sicurezza - 2

Il furto della Gioconda

di Giulia Lazzeri - tratto dalla rivista "EHF-Sicurezza per la cultura", organo ufficiale della Fondazione Enzo Hruby, anno XXII, n.1 dicembre 2012-marzo 2013

È il 1911: Marie Curie vince il Premio Nobel per la Chimica e in Germania Kandinskij fonda il movimento del "cavaliere azzurro". Intanto la Francia occupa Fez, in Marocco, e al Louvre viene rubata la *Gioconda*. Il 21 agosto Parigi si sveglia soffocata dall'afa. Alle 8 il copista Louis Bérout, mentre prepara cavalletto e tavolozza nella Salle Carrée del Louvre, fa scattare l'allarme: è sparita la *Gioconda*! Parte la caccia al ladro e sulle prime pagine dei giornali si fanno strada le supposizioni più disparate, arrivando a sospettare del furto persino l'impero tedesco. In Europa sono gli anni del processo alla cultura e il centro del dissenso è Parigi, dove Filippo Tommaso Marinetti ha da poco pubblicato il Manifesto del Futurismo. Sull'onda della contestazione, Guillaume Apollinaire dichiara di voler distruggere i capolavori dei musei per far posto all'arte nuova. Non si può certo criticare la Gendarmerie che, ai primi di settembre, arresta il poeta per il furto della *Gioconda*, considerando anche l'accusa a suo carico relativa all'acquisto di alcune sculture arcaiche trafugate dal Louvre, servite forse all'amico Pablo Picasso come modello per le *Demoiselles d'Avignon*. Dopo poco, la polizia è però costretta a rilasciarlo e per i due anni successivi torna a brancolare nel buio. Nel dicembre 1913 l'antiquario fiorentino Alfredo Geri riceve una lettera dove è scritto: «ho la *Gioconda* e intendo restituirla», firmata Léonard. L'antiquario avverte il direttore degli Uffizi e con lui si reca all'appuntamento all'albergo "Tripoli Italia", dove ricompare il capolavoro perduto. L'autore del furto, che in cambio della restituzione chiede una ricompensa in denaro, si rivela l'ex impiegato del Louvre Vincenzo Peruggia, imbianchino originario di Luino, in provincia di Varese. Trascinato in tribunale,



dove viene condannato a un anno e 15 giorni di reclusione, Peruggia sostiene di aver rubato la *Gioconda* per motivi patriottici, ignaro che il dipinto fosse stato portato olttralpe da Leonardo stesso negli ultimi anni della sua vita. La dinamica del furto è di una semplicità allarmante: passata la notte in uno sgabuzzino del Louvre, all'alba del 21 agosto, giorno di chiusura del museo, Peruggia preleva il quadro, si allontana da una porta di servizio e, con la *Gioconda* sotto la giacca, sale su un taxi e si dilegua nelle nebbie di Parigi. Successivamente, prima di portarla a Firenze nel 1913, custodirà la tela in una valigia con doppio fondo nella sua stanza parigina in rue de l'Hôpital Saint-Louis. Capolavoro sublime circondato dal mistero, la *Gioconda* ci osserva da dietro il cristallo della sua teca ipertecnologica con microclima costante. Testimone inconsapevole di oltre 500 anni di storia, è stata idolatrata, sfollata durante guerre e rivoluzioni, rubata, sfregiata e schernita. Pensiamo solo a Duchamp che le ha imposto barba e baffi o a Dalí che si è ritratto come *Gioconda*. Eppure non ha mai smesso di sorridere.

Una borsa di studio per il miglior studente del progetto Campus Came in nome di Paolo Tura

a cura di Raffaello Juvara

Il prossimo 3 novembre ricorrerà il quinto anniversario della scomparsa di **Paolo Tura**, che aveva fondato nel 1981 la rivista **essecome**, riconosciuta negli anni come una delle testate di riferimento per gli operatori della sicurezza fisica.

Con questa idea, Paolo si assunse un ruolo di divulgatore di competenze e di informazioni in un settore che si stava appena formando in quegli anni, con la passione che gli apparteneva e un'approfondita conoscenza dell'argomento "sicurezza" che derivava dalle esperienze acquisite quando aveva girato per il mondo come direttore commerciale della CISA.

Paolo ha così contribuito alla crescita anche identitaria del settore, trasmettendo agli addetti ai lavori l'idea che fosse necessario far nascere una specifica "cultura della sicurezza" da divulgare nella società, con la convinzione che questo avrebbe favorito anche la loro crescita economica. Per questo motivo, il figlio

Valerio ha deciso di ricordare Paolo istituendo una borsa di studio a suo nome, da assegnare nel 2015 al miglior studente di **Campus Came**, il più significativo progetto di formazione professionale avviato in Italia nella scuola pubblica nel settore della sicurezza.

La premiazione avverrà proprio il 3 novembre, giorno di apertura della 18ª edizione di **Sicurezza**, presso lo stand di **essecome** (pad. 22, stand M17-N20) nell'ambito della tavola rotonda sul tema della Formazione professionale e responsabilità degli installatori. Nell'intervista che segue, **Valerio Tura** descrive i presupposti del premio a nome di Paolo, del quale traccia un ritratto in parte inedito, che farà piacere leggere ai tanti amici che lo ricordano sempre con affetto. **Elisa Menuzzo**, vicepresidente di Came Group SpA, illustra il progetto **Campus Came** e gli obiettivi che il gruppo trevisano, leader nell'automazione degli edifici, si pone per favorire l'ingresso di giovani nel mondo del lavoro nella sicurezza.



essecome, il "giochino" di Paolo nel ricordo di Valerio

a colloquio con Valerio Tura

Quando è stato pubblicato il primo numero di essecome in febbraio 1981, la sicurezza tecnologica era riservata a una fascia ristretta di utilizzatori e l'esperienza delle figure professionali coinvolte era ancora in via di consolidamento. Che cosa aveva spinto allora Paolo a dar vita a una testata specializzata di settore?

Dopo una quindicina d'anni come dirigente commerciale e amministratore in diverse aziende, in Italia e all'estero, mio padre era stato chiamato alla CISA, come direttore commerciale, dove rimase fino al 1980. In quella posizione si occupò molto della penetrazione internazionale dell'azienda e dei suoi prodotti. Ebbe modo di continuare a viaggiare, sempre di più, in Europa, ma anche nelle Americhe, in Oriente, in Africa. Ciò gli diede modo di ampliare ulteriormente i suoi orizzonti, di confrontarsi con altre realtà produttive, con altri mercati, con approcci diversi e più attuali ai temi della sicurezza. Visitava con frequenza fiere ed esposizioni, ma soprattutto teneva le antenne sempre ben pronte (lui usava la metafora "i miei baffi da gatto"...) a ricevere stimoli, spunti, idee, a metabolizzarli e utilizzare tutto ciò per migliorare le strategie produttive e commerciali della CISA. L'azienda, che fino ad allora aveva prodotto principalmente lucchetti, chiavi e serrature, via via si propose sul mercato anche con prodotti più innovativi. Ricordo ad esempio quanta attenzione Paolo dedicò all'inserimento nel mercato nazionale e internazionale di prodotti quali i maniglioni anti-panico, ma anche la sua costante preoccupazione di guardare avanti, di pensare al futuro, intuendo il potenziale che nel settore della sicurezza avrebbe avuto lo sviluppo delle tecnologie elettroniche ed informatiche, cosa non del tutto scontata, né acquisita, negli anni Settanta e Ottanta. Parallelamente all'attività professionale, nel corso della sua vita Paolo aveva però anche sempre coltivato una



vivace passione per la scrittura e per la carta stampata: fin da giovane scriveva brevi racconti, essenzialmente per sé, per la famiglia e per gli amici, ma forse un giorno ne farò pubblicare una piccola antologia. Io gli dicevo che aveva il "morbo di Gutenberg"...!

Quando lasciò la CISA, fu quindi quasi naturale per Paolo, che non sapeva stare con le mani in mano, decidere di creare qualcosa di cui avvertiva la necessità, cioè una rivista, un periodico specializzato destinato ai professionisti che in vario modo operavano nel settore della sicurezza che, allora, era ancora ai primi passi.

Quali erano le motivazioni principali che lo hanno spinto ad assumersi un impegno così gravoso?

Paolo intuiva che in Italia era necessario far crescere una consapevolezza che vedeva ancora abbastanza debole, che occorreva una sorta di "cultura della sicurezza". Intuiva che ciò sarebbe stato facilitato facendo circolare puntualmente notizie, informazioni, esempi e confronti internazionali, commenti, interviste, contributi tecnici, analisi commerciali e industriali, presentazioni di nuovi prodotti, ritrovati tecnici, applicazioni specifiche di tecnologie sviluppate in altri ambiti. Intuiva che ciò sarebbe stato possibile se

gli addetti del settore, cioè imprenditori, installatori, commercianti, progettisti e tecnici di vario genere, utenti di prodotti e servizi, operatori delle forze dell'ordine, della vigilanza, dell'antincendio e così via, avessero potuto contare su uno strumento agile, comodo, facilmente disponibile, adatto alle loro esigenze. Intuiva che il settore della sicurezza, in generale, avrebbe avuto nei decenni a seguire una crescita di un certo rilievo, e che quanti operavano in quel mondo dovessero attrezzarsi ed essere preparati.

Nacque così **essecome**, quello che Paolo chiamava scherzosamente "il mio giochino"...

Alla luce di quanto accaduto nei trentacinque anni successivi, forse la realtà dei fatti ha mostrato la giustezza delle sue intuizioni.

Paolo riteneva dunque che la divulgazione della conoscenza, non solo nelle tecnologie, avrebbe favorito la crescita del settore. Quali sono state le iniziative più importanti alle quali ha partecipato?

Nel corso del tempo lo sguardo di **essecome** si è allargato, così come il ventaglio delle attività, anche non strettamente legate al periodico: libri, annuari e pubblicazioni collaterali di varia natura, e poi convegni, seminari e corsi, ma anche iniziative rivolte specificamente alla formazione degli operatori.

Se da un lato alcuni dei suoi principali oggetti d'interesse furono sempre le fiere internazionali specializzate del settore della sicurezza, che lui vedeva come luoghi di confronto, oltre che d'incontro e di promozione, dall'altro Paolo ebbe sin da subito ben presente la necessità di intrattenere un dialogo costante con le associazioni imprenditoriali, professionali e tecniche, cercando di stimolarle a rendersi protagoniste trainanti in questo processo di "formazione permanente" e di aggiornamento. Non credo sia il caso di ricordare alcuna iniziativa specifica, anche perché sono state molto numerose. Ricordo però con molta chiarezza la sua costante attenzione a questi aspetti. Un suo pensiero ricorrente era che, in Italia, gli operatori del settore dovevano aprirsi al mondo, e dovevano capire che avevano da colmare una sorta di gap che li distanziava dagli equivalenti stranieri, sotto ogni profilo: industriale, tecnico, commerciale, ma soprattutto "culturale". Il superamento di questo gap fu uno degli obiettivi che Paolo perseguì con maggior determinazione.

Possiamo quindi considerare il Premio intitolato a Paolo, che quest'anno verrà attribuito al miglior



studente del progetto Campus CAME, come una prosecuzione concreta del suo impegno per lo sviluppo della cultura del settore?

Certamente. Sono molto lieto che l'attuale direzione di **essecome** e un'azienda importante come **Came** abbiano accolto favorevolmente la mia proposta di creare un Premio ispirato al ricordo di Paolo e intitolato al suo nome, dando avvio all'iniziativa quest'anno, nel quinto anniversario della sua scomparsa, e in occasione della fiera a Milano, alla quale partecipò sempre regolarmente. Spero che questo piccolo contributo serva in qualche modo ad accrescere l'attenzione sulla necessità di sviluppare incessantemente la ricerca e la cultura specifica, in un territorio come quello della sicurezza. Si tratta di un terreno, come quasi tutti i campi del sapere tecnico e industriale, nel quale i processi innovativi non possono mai fermarsi. Paolo diceva spesso che chi non va avanti e sta fermo finisce fatalmente per rimanere indietro, e che quando si raggiunge un obiettivo occorre immediatamente iniziare a lavorare per focalizzare l'obiettivo successivo, più avanzato. Ciò è reso oggi ancor più evidente dal fatto che la realtà attuale si evolve e si trasforma con grande rapidità, spesso maggiore rispetto alla rapidità con cui si sviluppa la nostra stessa capacità di comprenderla. E' evidente che la ricerca e l'innovazione non possono che essere alimentati dalla formazione, in particolar modo dei più giovani, di quanti saranno protagonisti del domani e del dopodomani.

100 studenti e 20 insegnanti coinvolti nel primo anno di Campus Came

a colloquio con Elisa Menuzzo, Vice Presidente Came S.p.A.

Come si è concluso il primo anno di attività di Campus Came?

Il primo anno di attività del progetto di formazione ideato da Came per diffondere la cultura dell'automazione e della domotica e formare personale altamente specializzato è stato davvero soddisfacente. Nell'anno scolastico 2014/2015 Campus Came è partito in cinque istituti tecnici presenti sul territorio nazionale, coinvolgendo un centinaio di ragazzi del quarto anno e una ventina di insegnanti. Nello specifico, il progetto è stato attivato nelle scuole di Vittorio Veneto, Pordenone, Magenta, Bologna e Verona, selezionate in base al prestigio riconosciuto sul territorio.

Con l'anno scolastico 2015/2016, Campus Came verrà esteso in altri cinque istituti superiori in Piemonte, Trentino Alto Adige, Liguria, Toscana e Lazio. Devo dire che ad oggi abbiamo riscontrato un interesse molto alto sia da parte dei ragazzi che dei professori coinvolti nel progetto, che hanno accolto con grande entusiasmo la nostra nuova proposta formativa.

Quali sono i criteri adottati per valutare il rendimento degli studenti e stabilire la graduatoria?

Al termine del percorso formativo costituito da 20 ore di lezione in aula, ai ragazzi vengono somministrati due questionari. Il primo consiste in un test tecnico volto a misurare l'apprendimento di ciò che è stato spiegato in aula sia attraverso lezioni di teoria che con lezioni pratiche svolte con l'utilizzo di pannelli didattici realizzati ad hoc da Came e consegnati a ogni singolo istituto. Il secondo è un test psicologico di valutazione del potenziale che misura abilità quali



la capacità di iniziativa, il problem solving e la facilità di apprendimento. I punteggi dei due test vengono sommati e lo studente che per ogni istituto raggiunge il punteggio più alto viene scelto per accedere al secondo step del progetto.

Quali sono gli incentivi previsti per gli studenti migliori?

Agli studenti selezionati viene offerta la possibilità di recarsi una settimana in azienda per completare il percorso di formazione sui sistemi di home automation e di partecipare a una settimana di stage presso uno degli installatori autorizzati Came.

Quali saranno le prossime tappe di sviluppo del progetto, a partire dal prossimo anno scolastico?

A partire dal prossimo anno scolastico, verranno

inseriti nel progetto altre cinque istituti professionali selezionati. Come primo step ai docenti delle scuole coinvolte verranno insegnati i principi della domotica e dei sistemi integrati. Gli insegnanti parteciperanno poi a una sessione di formazione di due giorni organizzata in azienda in cui verrà spiegato loro l'argomento che a loro volta affronteranno in classe con gli studenti durante l'anno.

Campus Came

Campus Came è il progetto di formazione ideato da Came e rivolto a tutti gli studenti degli Istituti

Superiori italiani. L'obiettivo è quello di diffondere la cultura dell'automazione e della domotica, formando gli installatori di domani sulle tante innovazioni tecnologiche in corso. Negli istituti che aderiscono al progetto, Came entra in aula per insegnare ai ragazzi le novità dal mondo dell'automazione e dell'home automation, offrendo materiale didattico e sottoponendo gli allievi a un test di valutazione finale. I migliori studenti proseguono il percorso formativo con uno stage in una delle sedi Came e poi presso un installatore.



Interfonia, chiamate di soccorso e diffusione sonora Over IP per campeggi, parchi e aree di intrattenimento

SICUREZZA Milano-RHO
3/5 Nov. 2015 - Stand D19 - E10

Sipac Padova
18/19 Nov. 2015

ermes

Via Treviso, 36 - 31020 San Vendemiano (TV) - tel. +39 0438 308470 - email: ermes@ermes-cctv.com - web: www.ermes-cctv.com

Come cambia la sicurezza in banca - 4

La gestione del cash in MPS

a colloquio con Guido Giorgetti, responsabile settore physical cash di MPS Banca a cura della Redazione

Il sistema bancario italiano ha reagito alle criticità emerse negli anni scorsi nel trasporto valori introducendo modalità di monitoraggio continuo del contante nelle diverse fasi della logistica. Può descriverci le soluzioni adottate da MPS in partnership con BASE?

Da alcuni anni, MPS ha implementato e incrementato numerosi sistemi informatizzati per tenere sotto controllo tutte le fasi del ciclo di vita del "proprio" contante, sia sotto il profilo della logistica che di quello relativo ai vari processi di lavorazione puntando, in particolare, a sistematizzare un processo unico in tutta la nostra rete italiana per garantire certezza, rapidità delle informazioni e sicurezza, nel pieno rispetto delle vigenti normative imposte da Banca d'Italia.

Una delle ultime soluzioni ingegnerizzate insieme a **BA.SE Service** del Gruppo Battistolli, partner decennale della Banca, è stata la soluzione **SICURPos**: un sistema di tracking in tempo reale delle operazioni presso lo sportello, unito a un processo in simultanea di autenticazione del soggetto operante.

Il sistema prevede una prima fase di autenticazione dell'operatore (GpG), che si presenta in filiale o presso un nostro cliente GDO per svolgere le operazioni di prelievo o consegna dei valori, grazie ad una tecnologia innovativa: un badge biometrico riportante foto, logo dell'istituto e matricola della guardia giurata, che si attiva grazie al passaggio dell'impronta digitale su un apposito sensore situato all'interno del badge stesso. Una prima, grande innovazione con un brevetto operante in 75 paesi nel mondo.

Il badge viene poi avvicinato al POS e, dopo un'interrogazione verso l'anagrafica online delle GpG,



è il POS stesso che indica nel display le operazioni autorizzate e accompagna l'operatore nello svolgimento delle singole operazioni (consegna/ritiro), richiedendo la cattura del codice a barre di ogni singolo plico, cassetto o sacco.

Le operazioni sono tutte registrate online in tempo reale e, solo dopo averle correttamente censite, il POS restituisce uno scontrino attestante il corretto svolgimento dell'intero iter operativo.

Viene così creata una situazione di contraddittorio in tempo reale tra banca e fornitore, che velocizza la registrazione dei dati, facilita sia la misurazione dei

KPI che il processo di fatturazione e innalza il livello di sicurezza.

Aggiungiamo che tale soluzione, di proprietà della banca, ci permette anche la totale autonomia nella scelta dei corrispondenti, agli operatori dei quali viene richiesto solamente di avere con sé l'apposito tesserino di riconoscimento fornito dal nostro partner BASE, che provvede anche a mettere a disposizione l'intera architettura HW e SW, che non richiede alcun tipo di interfacciamento con le strutture IT della Banca.

Una soluzione auto-consistente, molto semplice nell'utilizzo e strategica per le nostre attività di controllo e monitoraggio del servizio.

I sistemi di sicurezza fisica delle filiali, in particolare i software di gestione centralizzata, sono coinvolti in queste modalità di monitoraggio del contante?

Assolutamente sì. Questa domanda consente di parlare di una soluzione di monitoraggio in tempo reale del denaro contante presso le Sale Conta, che stiamo sviluppando sempre insieme a BA.SE. Si tratta della soluzione **SICURBank**, un armadio per caveau con un sistema a bordo di videoregistrazione interna e di apertura/chiusura controllato tramite elettroserrature, gestibile dalla banca anche da remoto. Il sistema permette di monitorare, grazie alla gestione centralizzata dell'armadio, ogni operazione di apertura, chiusura e deposito delle banconote all'interno dello stesso.

Il sistema ci consente, inoltre, di essere certi delle operazioni che vengono effettuate per il trattamento e il ricovero del "nostro" denaro, dando la possibilità di inibire l'apertura, e quindi l'accesso ai valori, secondo la nostra discrezionalità. Tale soluzione, centralizzata presso una Control Room, è un esempio ulteriore dell'attenzione che la banca riserva a tutti i processi relativi al denaro contante, a cui si aggiungono i sistemi di trattamento automatizzato in filiale (TARM) e gli ATM multifunzione. Tutti questi sistemi sono dotati di sensoristica collegata alla nostra architettura di gestione centralizzata, in modo che ogni fase del processo di gestione del cash ci possa fornire quante più informazioni possibile, in tempi rapidissimi e in assoluta sicurezza. Altre piattaforme software sviluppate partendo dai nostri sistemi di contabilità interna e aventi per oggetto sempre il cash, ci

consentono oggi di proporre soluzioni automatizzate di casseforti intelligenti per la GDO, con il servizio di accredito immediato sul conto corrente dell'esercente. In un prossimo futuro, potremo gestire a livello centralizzato, su un unico portale interno, le movimentazioni di denaro corrente che avvengono nella nostra rete in Italia ogni giorno, considerando anche gli aspetti ad esse correlati, come gli assegni, i titoli, i documenti in bianco, i valori di vario genere, verbali di rendicontazione e anomalie, ecc.

Qual è la vostra vision in merito alle prospettive future del contante, a livello globale e interno alla Banca MPS ?

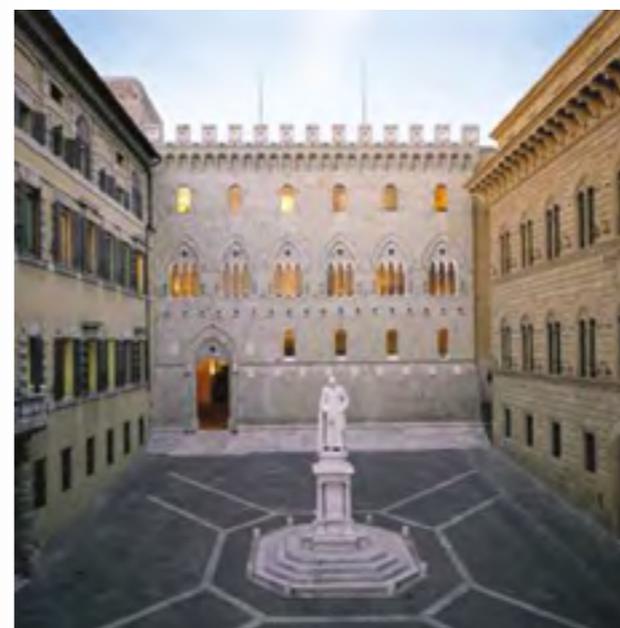
Banca MPS sta valutando molto attentamente un nuovo modello nell'approccio alla gestione del contante, fermo restando che le prospettive di diminuzione nell'utilizzo del cash non si sono ancora concretizzate in modo significativo, malgrado le numerose iniziative adottate al riguardo. Cercheremo di adottare modelli flessibili e leggeri, in modo che la circolazione del contante avvenga attraverso canali innovativi, in grado di offrire maggiori servizi alla clientela in un arco temporale più ampio rispetto all'orario canonico di apertura della filiale. Stiamo valutando in queste settimane interessanti prospettive relative a nuovi canali tecnologici e nuovi strumenti, che potranno rendere la gestione del cash più economica, pur non limitando la disponibilità verso la clientela che vorrà farne ancora uso. Stiamo parlando di intensificare i servizi offerti sui terminali ATM, di ampliare il concetto di 'banca aperta' con postazioni self service e di incrementare la capillarità sul territorio attraverso partnership con altri operatori.

I nuovi servizi "cashless" aumenteranno sempre di più e questo comporterà inevitabilmente una flessione nella circolazione del contante che, comunque, non segue una relazione direttamente proporzionale dal momento che, anche senza considerare i fattori di tipo macro economico, sono molti gli elementi che possono influenzare la clientela a richiedere un utilizzo più o meno elevato di denaro contante.

Come Banca, cercheremo tuttavia di rispondere al meglio in entrambi gli scenari, modulando i nostri servizi su soluzioni molto flessibili e guidate da criteri di continua e incessante ottimizzazione dei processi operativi.



La Banca



Cenni storici

La Banca Monte dei Paschi di Siena, sorta nel 1472, rappresenta oggi una delle principali banche nazionali. E' a capo di un Gruppo di rilevanti dimensioni, che si colloca ai primi posti in termini di quote di mercato nei diversi comparti.

Ideale erede delle tradizioni mercantili e bancarie senesi del Medioevo, il Monte fu fondato nel 1472, per volere della Repubblica di Siena. Il carattere pubblicistico del Monte trovò conferma con la riforma del 1624, che dotò l'Istituto di progredite strutture bancarie. Con l'occasione il Granduca mediceo concesse ai depositanti la garanzia statale mediante il vincolo delle rendite dei pascoli demaniali della Maremma ("i Paschi", da cui prese il nome la Banca). Su questo fondamento il Monte dei Paschi fu in grado di consolidare ed intensificare la propria attività tra il Seicento e il Settecento. Vennero così create le basi della cospicua espansione avviata all'indomani dell'unità nazionale, e più ancora affermatasi nel XX secolo.

Nel 1995, con Decreto del Ministro del Tesoro, l'azienda bancaria è stata conferita in Banca Monte dei Paschi di Siena costituita nella forma di società per azioni. La Banca Monte dei Paschi di Siena opera, anche tramite proprie controllate, nei diversi segmenti dell'attività bancaria e finanziaria, da quella tradizionale, al credito speciale, all'asset management, alla bancassurance, all'investment banking.

Il Monte ha una spiccata vocazione retail (famiglie e piccole e medie imprese) che contribuisce a renderla "banca di riferimento" in tutte le aree nelle quali insediata. A partire dal giugno 1999, Banca Monte dei Paschi è quotata presso il Mercato Telematico Azionario della Borsa Italiana e fa parte, da settembre '99, dell'Indice più rappresentativo del mercato, il FTSE Mib.

L'ANAC entra in scena per gli appalti pubblici dei servizi di vigilanza

a cura di GpG (Gossip particolare Giurato)

La Gazzetta Ufficiale n.186 del 12 agosto 2015 ha pubblicato la Determina del 22 luglio 2015 dell'Autorità Nazionale Anti Corruzione (ANAC) con le "Linee guida per l'affidamento del servizio di vigilanza privata", a firma del Presidente Raffaele Cantone.

Un provvedimento caricato di un'aspettativa salvifica dagli istituti di vigilanza, speranzosi di veder risolti dall'Autorità i problemi creati da se stessi appena caduta Tulpswood, cioè da quando sono venute meno protezioni e costrizioni del TULPS mod. 1931.

Esaminando in controluce i cinque punti presi in considerazione dall'ANAC, relativi ad altrettante situazioni "attenzionate" nel tempo dalle Autorità territoriali di controllo (prefetture, questure, magistratura) in quanto potenziali focolai di illegalità, si ricava un edificante quadretto, nel quale le furbizie escogitate da un gran numero di operatori del settore per "fregare" di volta in volta clienti, dipendenti, concorrenti, fisco, INPS, o anche tutti insieme, in molti casi si sono alla lunga ritorte contro i "furbetti" stessi, non prima di aver devastato il mercato e danneggiato irreparabilmente le (poche) aziende serie.

Vediamo i punti di attenzione selezionati dall'ANAC:

1. Distinzione tra i servizi di vigilanza privata e i servizi di guardiania e custodia. Da quando è partito il fenomeno del "portierato" oltre 20 anni fa, non è parso vero agli istituti di vigilanza di poter mettere in piedi aziende ombra e cooperative fasulle con le quali poter fare tutto quello che non potevano fare come titolari di licenza di PS (per esempio: lavorare fuori



provincia, scansare regolamenti di servizio, abbattere CCNL ecc). In molti casi queste "armi non convenzionali" sono state usate contro concorrenti anche lontani, non essendoci bisogno di licenza di PS, oppure per poter "estrarre" dagli istituti di vigilanza originari i clienti più interessanti, lasciando ai curatori le costose GpG e i debiti troppo pesanti. Basterebbe poter analizzare in filigrana i soggetti che si sono mossi e tuttora si muovono nella "area grigia" del portierato per comprendere chi abbia prodotto quella confusione tra i servizi di vigilanza privata e i servizi di guardiania e custodia, confusione che ora si chiede all'ANAC di chiarire;

2. Corretta individuazione dei requisiti di partecipazione da fissare nel bando di gara, con particolare riguardo alla sussistenza della licenza prefettizia e alla sua territorialità. In parte è un corollario del punto 1, visti i casi di "guastatori" del portierato mandati all'assalto di piazze per le quali l'istituto di vigilanza mandante era privo di autorizzazione; per altra parte, sarebbe quasi ovvio che partecipi a una gara per servizi di vigilanza solamente chi è in possesso del requisito essenziale della licenza di PS, ovvero che sia nelle condizioni di poterla ottenere prima dell'inizio dell'attività. Evidentemente, si sono mossi in troppi per partecipare a gare senza aver neanche l'ombra della licenza prefettizia necessaria per operare in quel territorio o, in qualche caso, neppure i presupposti per poterla ottenere;

3. Determinazione della formula per individuare l'offerta economicamente più vantaggiosa (OEPV), tutelando le PMI. E' abbastanza curioso che vengano coinvolte le stazioni appaltanti pubbliche che indicano gare al massimo ribasso in tempi di spending review e di patti di stabilità. Finchè trovano samaritani che fanno prezzi sotto-costò pur di non perdere l'appalto oppure gangster con licenza benedetti dalle "competenti" autorità di controllo, perché dovrebbero spendere più quattrini dei contribuenti?

4. Ribassi eccessivi che potrebbero essere correlati ad irregolarità nel rispetto degli obblighi derivanti dall'applicazione del CCNL. Questo è il punto dei "sepolcri imbiancati". Chi ha fatto o sta facendo prezzi stracciati nelle gare indette da enti pubblici per il servizio di vigilanza? Gli istituti di vigilanza italiani, mica quelli marziani e nemmeno quelli europei, che si tengono a debita distanza dalla carneficina auto-distruttrice scoppiata dopo la scomparsa delle tariffe minime, imposta dalla sentenza della Corte di Giustizia Europea alla fine del 2007. Il prezzo di un servizio fatto praticamente di sola manodopera, ha un limite

invalicabile nella corsa al ribasso, costituito dai costi obbligatori della manodopera stessa. Il superamento di quel limite è possibile solo eludendo contratti di lavoro, contributi, tasse, formazione, regolamenti ecc, oppure truffando i clienti oppure facendo altro di peggio. Il che spiega l'interesse dell'ANAC per l'argomento. Ne dovremmo vedere delle belle...!

5. Modalità di attuazione del "cambio di appalto". Un argomento vastissimo e impervio, come dimostra il fatto stesso che l'ANAC se ne debba occupare, dopo anni che i contratti di lavoro nazionali e provinciali provano a regolamentarlo. Punto uno: tutela dei livelli occupazionali. Dal punto di vista "quantitativo" del mercato del lavoro, un cambio di appalto non modifica il saldo dei lavoratori occupati, anche se il subentrante impiega personale nuovo. Punto due: tutela dei lavoratori dell'azienda cessante. E' difficile per chiunque fare offerte economicamente migliorative per servizi di sola manodopera, se si devono utilizzare lavoratori con diritti contrattuali acquisti molto onerosi. Punto tre: interesse della stazione appaltante. Se il suo obiettivo in sede di gara è quello di risparmiare, non può che tifare per un subentrante che "ignori" i vincoli di assunzione del personale del cessante. Altrimenti, dove risparmia? E la libertà d'impresa dei concorrenti dove la mettiamo? Come detto, è un argomento difficile, che rimarrà probabilmente sullo sfondo a lungo.

Conclusione: Il "deus ex-machina" dell'ANAC dovrebbe guardare veramente dentro al sistema per individuare e possibilmente estirpare le anomalie che hanno finora ritardato il percorso verso la "normalità" di un comparto bloccato per decenni da una legge anacronistica, il Tulps del 1931. Un comparto relativamente piccolo, con 2,8 miliardi di euro di fatturato con 45.000 addetti, ma di forte rilevanza sociale, che deve poter contribuire pienamente e dignitosamente alla sicurezza partecipata nel momento in cui il paese intero potrebbe averne più bisogno.

A Sicurezza 2015 saranno protagonisti i market leader e le soluzioni verticali

a cura della Redazione

Continua il cammino verso SICUREZZA 2015 con ritorni importanti e un'ampia e ricca offerta orientata a tecnologie su misura per contesti specifici. Un format che continua a crescere e in tre edizioni – 2015, 2017 e 2019 – punta a diventare evento di riferimento del Bacino del Mediterraneo.



Importanti **riconferme**, **ritorni** di brand che mancavano da qualche anno, **nuovi focus tematici** che guardano al futuro prossimo del mercato e aprono interessanti opportunità di business: **SICUREZZA 2015** (a Fiera Milano dal **3 al 5 novembre**), quando mancano due mesi all'inizio della manifestazione, si conferma appuntamento di riferimento per i professionisti della security e dell'antincendio, **unico evento internazionale in calendario nel secondo semestre di quest'anno**.

La prima edizione negli anni dispari propone un format sempre più orientato alle soluzioni, in linea con le richieste degli espositori e di tutte le realtà del settore, destinato a potenziarsi anche nelle prossime edizioni, nel 2017 e nel 2019. Intanto, si stanno formalizzando a ritmo serrato le adesioni: si conferma forte la **videosorveglianza**, ma è sempre più rappresentativa l'offerta di soluzioni e prodotti per **sicurezza passiva** – in particolare i **serraturieri** - e **controllo accessi**, tra i settori con il maggior numero di espositori.

Notevole, inoltre, la presenza di **market leader**, che hanno scelto la manifestazione perché in contatto con i loro mercati di riferimento e potenziale via di sbocco verso nuove opportunità commerciali.

Ma **SICUREZZA 2015** non offrirà soltanto un panorama completo di tecnologie e soluzioni attraverso la proposta diretta dei più grandi produttori italiani e internazionali, ma proporrà anche **iniziative verticali** dedicate a un mondo di applicazioni in continua crescita, per guidare l'operatore in visita verso la scelta più adatta alle sue esigenze e indirizzarlo a comprendere le potenzialità delle tecnologie proposte.

LE INIZIATIVE ESPOSITIVE

L'EVOLUZIONE DELLE SOLUZIONI PER IL RETAIL
È specificamente dedicato alle soluzioni di security per il commercio e la grande distribuzione **Security for Retail Show** (pad. 22), appuntamento realizzato per la prima volta da **SICUREZZA** in collaborazione con **essecome/securindex.com**.

Rivolta ai professionisti del retail in cerca di strumenti per mettere in protezione la propria attività, l'area favorirà il confronto su queste problematiche e proporrà soluzioni

CREATE
SECURITY
MAKE
BUSINESS

3-5
NOVEMBRE
2015

FIERA
MILANO
(RHO)

RISPARMIA
TEMPO
E DENARO!

Registrati e acquista
il biglietto al **50%**
SU

www.sicurezza.it

SICUREZZA

Biennale Internazionale di Security & Fire Prevention

INTERNATIONAL NETWORK



www.exposec.it



www.fisp.it

Follow us on



Official Partner

su misura per ogni tipologia di punto vendita, riunendo in un unico contesto tecnologie e soluzioni verticali dedicate. Oltre a mostrare proposte integrate su misura e nuove idee per coniugare la sicurezza all'accoglienza del cliente nei punti vendita, questo spazio attraverso **talkshow, tavole rotonde e workshop a cura di essecome/securindex.com**, offrirà 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.

ICT E SECURITY SEMPRE PIU' INTEGRATI

Per offrire una visione privilegiata sull'anima sempre più digitale del settore, **SICUREZZA**, in collaborazione con **Digitalic**, ripropone il **Cyber Security Village** (pad. 24). In un mondo in cui uno strumento di sicurezza è spesso un dispositivo digitale collegato ad una rete, in comunicazione con server, hard disk e collegato a Internet, servono nuove competenze e nuove soluzioni per proteggere adeguatamente gli strumenti di sorveglianza e i dati che questi registrano. Il Village di Digitalic offrirà **esempi concreti della sempre maggiore integrazione tra ICT e security** e proporrà soluzioni all'avanguardia in campi diversi, dalla registrazione su hard disk e memorie, alla protezione delle reti. Da cablaggi sicuri a memorie in grado di difendersi da tentativi di furto di dati, fino ai software e ai sistemi di difesa del patrimonio aziendale, saranno numerose e interessanti le tecnologie di

ultima generazione presentate all'interno di quest'area dedicata alla sicurezza digitale.

L'INTELLIGENZA E LA SICUREZZA DELLE COSE

Interessante area verticale sarà quella dedicata a **IoT: l'intelligenza e la sicurezza delle cose** (pad. 24): con l'avvento della "quarta rivoluzione industriale" le "cose" diventano smart e dialogano tra loro e tutto – dalle infrastrutture al mondo industriale, fino ai singoli – è ormai collegato a un dispositivo digitale e ad una rete. In questo contesto il tema della sicurezza diventa prioritario: non solo infatti sicurezza fisica e logica convergono, ma la security in ogni ambito diventa elemento chiave per garantire protezione, monitoraggio costante, ma anche efficienza e miglioramento delle performance. L'area IoT, con l'intento di gettare uno sguardo al futuro del mercato, **riunirà aziende che già oggi stanno concretamente lavorando per risolvere le problematiche di security che vanno affrontate alla luce della sempre maggiore diffusione di device e prodotti intelligenti**. Ad arricchire l'area di contenuti, sono in programma un convegno, realizzato da Digitalic, che coinvolgerà i **massimi esperti di IoT e di sicurezza** e workshop tecnici che illustreranno case history e opportunità future.

QUANDO LA SICUREZZA VOLA ALTO

Per la prima volta sarà ospitata in manifestazione **SICUREZZA Drone Expo** (pad.22), iniziativa



interamente dedicata all'utilizzo degli APR (Aeromobili a Pilotaggio Remoto) per le attività di security e safety. Organizzato dalla società Mediarkè di Roma, che già da un paio di anni promuove altri eventi professionali nel settore, l'evento si articolerà in una collettiva all'interno dei padiglioni di **SICUREZZA 2015**, cui parteciperanno le più importanti aziende italiane ed estere specializzate nella produzione o nei servizi con gli Aeromobili a Pilotaggio Remoto. Non mancheranno le scuole di volo APR, che proporranno i loro corsi per la formazione dei futuri piloti di droni. In collaborazione con la testata S News sono previsti anche due convegni sull'utilizzo degli APR per le attività di security e safety. Una vera e propria "flight area" consentirà infine di effettuare voli dimostrativi di droni multirotori. Una iniziativa che guarda al futuro della security, ambito in cui anche questo tipo di tecnologia trova ormai sempre maggiore applicazione, dalla sorveglianza dei flussi migratori nel Mediterraneo al controllo di infrastrutture critiche e grandi eventi, dalla tutela del patrimonio artistico al monitoraggio di frane e incendi boschivi. A queste attività, presto se ne affiancheranno altre, come l'intervento d'emergenza in caso di disastri e catastrofi naturali, il controllo dall'alto di situazioni critiche, fino addirittura al trasporto di medicinali in aree isolate.

PROFESSIONALITÀ IN "PIAZZA" TRA BUSINESS E CONVIVIALITÀ

Tra i progetti espositivi, torna a **SICUREZZA** l'Ecosystem Village (pad. 24), **isola dedicata ai partner di Milestone Systems**: uno spazio, ma anche una "piazza" e un bar in cui incontrarsi, scambiarsi opinioni e toccare con mano novità tecnologiche, condividendo

formazione tecnica e momenti di scambio in un'unica area, pensata per unire convivialità e professionalità, incontri informali e business, prodotti e possibili idee progettuali.

SOLUZIONI, FORMAZIONE E VALORIZZAZIONE DELLE STRATEGIE VINCENTI

Applicazioni e soluzioni innovative saranno protagoniste grazie alla **Solutions Gallery** (pad. 24) a cura di Ethos Media, grazie a una "mostra - premio" che darà visibilità, in un'area espositiva dedicata, alle soluzioni messe in campo per risolvere i problemi concreti dei committenti, in diversi mercati verticali, permettendo ai visitatori di votare le soluzioni ritenute più efficaci. Solutions Gallery sarà un viaggio oltre il prodotto, tra l'eccellenza delle tecnologie applicate e integrate.

FORMAZIONE E INFORMAZIONE

A completare l'offerta, numerose opportunità di formazione di qualità. Sarà dedicata agli installatori la Ethos Academy, che offrirà formazione tecnica, normativa, gestionale e manageriale. Non mancheranno le proposte delle più importanti associazioni e di editori trade, orientate all'aggiornamento normativo nei diversi comparti, all'analisi di mercato e ai trend del momento. A questo si aggiungeranno le dimostrazioni e i convegni promossi dalle aziende espositrici. Qualità e innovazione, nuove soluzioni, formazione e spazi sempre più interattivi per confrontare e valorizzare idee e professionalità: i visitatori di **SICUREZZA** troveranno tutto questo dal **3 al 5 novembre 2015 a Fiera Milano**.

DA NON DIMENTICARE

Risparmia tempo e denaro

Per acquistare il proprio biglietto al 50% e accedere direttamente in fiera senza code è già possibile preregistrarsi su www.sicurezza.it.

Scopri le Convenzioni viaggio

Ventana Group, agenzia viaggi ufficiale di Fiera Milano (tel: +39 02 45402049; fax: +39 02 45402045; e-mail: fieramilano@ventanagroup.it) è a disposizione di espositori e visitatori per costruire pacchetti su misura. In particolare, grazie a un accordo con Trenitalia, sono disponibili pacchetti a prezzi speciali, che includono il viaggio in treno A/R e pernottamenti in hotel 4*. Per info www.sicurezza.it/it/come-arrivare

Seguici! SICUREZZA è sempre più Social

Sicurezza è anche su twitter e LinkedIn. Segui la nuova showcase di LinkedIn al link <https://www.linkedin.com/company/sicurezza-milano>.

Domotica, IoT, Smart Building, LED, Efficienza Energetica a Home and Building 2015

a cura della Redazione

Si avvicina la settima edizione di **Home and Building - Mostra Convegno della Domotica e delle Building Technologies**, l'appuntamento annuale più atteso riservato agli specialisti di sistemi e componenti per l'automazione domestica e degli edifici in programma a Verona il 27 e 28 ottobre.

Home and Building è l'unico evento verticale in Italia dedicato agli operatori che vogliono avere una panoramica completa sulle tendenze del settore, comprendere il mercato di domotica, smart home, edificio intelligente, conoscere nuovi prodotti e applicazioni, entrare in contatto con le eccellenze, avviare progetti e business.

Anche questa edizione sarà ricca di novità e di iniziative studiate, come di consueto, con la collaborazione dei partner scientifici più qualificati e con le associazioni di riferimento del settore.

Tra le tematiche in evidenza segnaliamo il tema dell'Internet of Things che, applicato alle mura domestiche, comprende l'insieme delle tecnologie che mettono in rete gli oggetti di utilizzo quotidiano per scambiare informazioni con altri oggetti e persone. In programma momenti di approfondimento con personalità di spicco del settore, che introdurranno le più innovative tecnologie della IoT applicata al building, con importanti benefici nella gestione energetica e in quella degli stessi impianti.

Altro tema di grande interesse è lo Smart Building. Saranno presentati approfondimenti e case history di successo relativi alle migliori tecnologie ICT e di automazione che possono contribuire al risparmio energetico e alla sostenibilità ambientale.

Anche i LED saranno tra i protagonisti dell'edizione 2015, grazie all'evento verticale **mcT LED - Mostra**

Convegno dei Sistemi di Illuminazione a LED, in programma il 28 ottobre, che vedrà l'organizzazione in parallelo di momenti congressuali dedicati. L'attenzione sarà puntata sui LED e sull'efficienza energetica, sulla smart lighting e sull'integrazione con i sistemi domotici. Il programma della giornata comprende questo e molto altro per tracciare lo stato dell'arte della tecnologia, offrire scambi di esperienze e best practice di assoluto rilievo.

La **domotica** svolge anche un'importante funzione sociale ed etica, visto che la tecnologia intelligente permette un radicale miglioramento della qualità della vita di persone in età avanzata o affette da disabilità. Un tema sempre di attualità in un Paese come il nostro, in cui il 21% della popolazione supera i 65 anni di età. In questo ambito, si parlerà di "**soluzioni domotiche a uso sociale**", con focus sulle migliori soluzioni in risposta ai bisogni e alle diverse esigenze abitative e per migliorare la fruizione degli spazi domestici.

Per massimizzare le sinergie e le opportunità, la due giorni di Verona godrà inoltre della concomitanza di **SAVE** - Mostra Convegno Automazione, Strumentazione, Sensori, e di **mcTER** - Mostra Convegno Applicazioni di Cogenerazione, evento di grande successo e dedicato alle tematiche dell'efficienza energetica, di grande interesse anche per il settore building. **Home and Building** (Veronafiere, 27-28 ottobre), organizzata da EIOM, si configura come un'autorevole vetrina internazionale sulle novità tecnologiche del mercato, un appuntamento riservato ai più importanti player del settore e a tutti gli operatori qualificati - quali progettisti, integratori di sistema, prescrittori, impiantisti, distributori, imprese edili, e molti altri ancora.

L'evento verticale di riferimento per progettisti, studi tecnici, installatori qualificati

HOME AND BUILDING

Mostra Convegno della Domotica e delle Building Technologies.

Fiera di Verona
27-28 ottobre 2015



- ✓ Soluzioni e tecnologie per domotica e home automation
- ✓ Soluzioni e tecnologie per building automation
- ✓ Efficienza energetica
- ✓ Componentistica elettrica e materiale d'installazione
- ✓ Sistemi bus / Interfacciamento
- ✓ Gestione e controllo consumi, accessi, reti, clima
- ✓ Gestione e controllo elettrodomestici, illuminazione
- ✓ Automazione porte, cancelli, serrande, videocitofonia
- ✓ Sistemi antintrusione e antifurto
- ✓ Home audio / video
- ✓ Controllo carichi / sistemi UPS

Il miglior rapporto qualità/prezzo

- Stand preallestiti
- Workshop tecnici
- Incontri verticali



www.expoHB.eu

Benvenuti a ShenZhen, la capitale della sicurezza in Cina

a cura della Redazione

CPSE 2015 vi invita a partecipare alla più importante fiera internazionale della sicurezza!

La 15° edizione di CPSE si terrà quest'anno dal 29 ottobre al 1° novembre nella città di ShenZhen, diventata ormai la capitale della sicurezza, che di certo susciterà anche questa volta l'attenzione di tutto il mondo.

Dopo 25 anni di impegno e crescita, CPSE è la più grande esposizione internazionale del settore, ma vuole avere sempre più successo. Rimanendo l'unica manifestazione certificata dall'UFI in Cina, questa edizione occuperà una superficie di 110.000 metri quadrati e, secondo le statistiche, il 96% degli espositori del 2013 ha già deciso di partecipare anche quest'anno alla manifestazione, ormai diventata la piattaforma preferita per presentare le nuove tecnologie e i nuovi prodotti. Fino a questo momento, CPSE ha attirato più di 1500 espositori da oltre 30 paesi, fra

i quali 55 tra le 500 società più famose del mondo. Sono previsti oltre 120.000 visitatori professionali che parteciperanno, visiteranno e compreranno i più avanzati prodotti per la sicurezza, cercando le migliori opportunità commerciali. CPSE, in quanto principale fiera internazionale della sicurezza, è considerata un appuntamento indispensabile per gli esperti, anche per il ruolo guida e l'influenza che esercita a livello globale nel settore. Si prevede che verranno esposti i prodotti più completi e le migliori soluzioni di tutte le grandi aziende della sicurezza, che presenteranno tecnologie e prodotti video, sistemi di controllo accessi e di allarme antifurto, citofoni remoti, apparecchi intelligenti per la casa, sistemi di controllo di parcheggio. Inoltre, diventeranno il focus di CPSE di quest'anno i prodotti e le tecnologie antincendio, i sistemi antifalsificazione, le applicazioni per la polizia, i sistemi intelligenti per il



THE WORLD'S BIGGEST SECURITY TRADESHOW
110,000m² 1,500 Exhibitors 130,000 Visitors 6,000 Booths

CPSE 2015

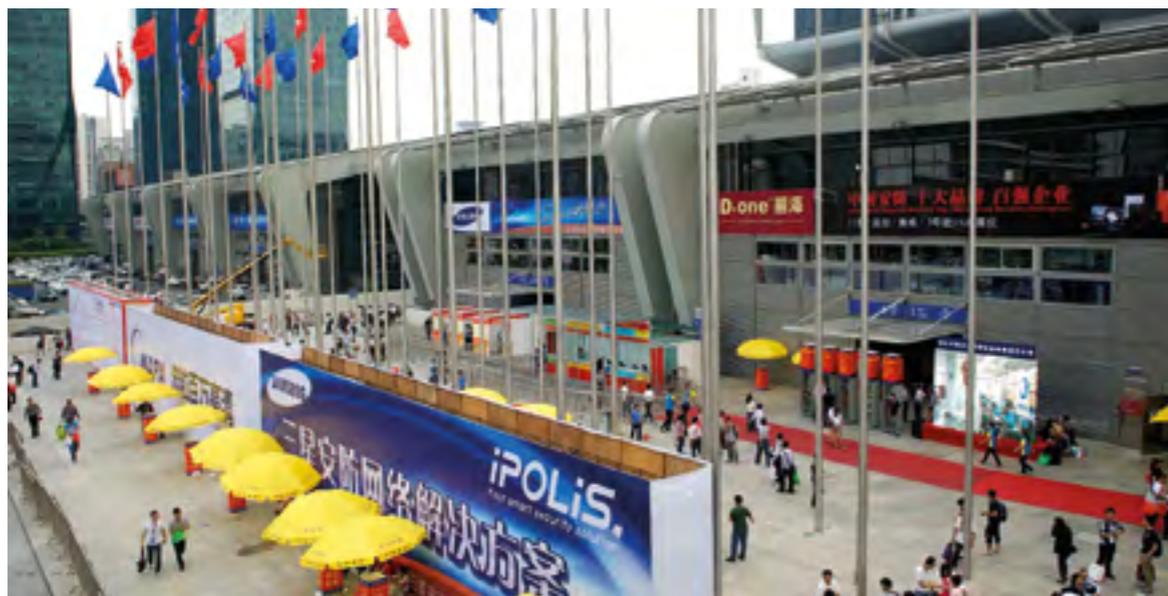
THE 15TH CHINA PUBLIC SECURITY EXPO
Oct 29 - Nov 1, 2015 | SHENZHEN CHINA
www.cpse.com.cn

The CPSE Golden Excellence Award 2015
CPS Forum 2015 - The 13th China Public Security Forum
The Public Security Academic Forum



Exhibitor partial list





traffico, la sicurezza informatica, l'analisi intelligente, la sicurezza della rete e l'antiterrorismo.

Durante i quattro giorni di esposizione, avranno luogo una serie di eventi, come il 13° forum della sicurezza di Samsung. CPSE non sarà, quindi, solo una piattaforma di prodotti e servizi: gli organizzatori si aspettano che, attraverso queste attività, diventi anche un appuntamento indispensabile per scambiare le innovazioni tecnologiche e conoscere le nuove tendenze del campo della sicurezza, promuovendo il commercio e lo scambio tra la Cina e il resto del mondo. "CPSE è un ottimo veicolo per conoscersi e scambiare informazioni. In quanto sponsor principali dell'evento, vogliamo dimostrare al mondo il livello dei nostri prodotti per la sicurezza" ha affermato Jin

Shengzhi, direttore generale della Samsung di Tianjin. Arriveranno a CPSE diverse delegazioni da tutti i paesi del mondo, fra cui Germania, Brasile e Arabia Saudita. Con la rapida crescita dell'industria della sicurezza in Cina, il mercato cinese continuerà a attirare l'attenzione dei partecipanti stranieri e dei clienti professionali, con grandi opportunità commerciali nel mondo. ShenZhan interpreta da sempre un ruolo importante nell'industria della sicurezza e il mercato cinese, il più importante del mondo, offrirà delle opportunità agli espositori a CPSE, che diventerà una bella partenza per la collaborazione internazionale.

Benvenuti a CPSE 2015! Per avere più informazioni, si prega di visitare il sito ufficiale www.cpse.com.cn



Abbonati!
6 numeri a soli 60€

Nuove Mini Dome Dahua: 4K Ultra HD Network IR serie Eco-Savvy 2.0.

DAHUA TECHNOLOGY CO LTD

(+39) 0362 1791300

www.dahuasecurity.com



Nuove ed importanti caratteristiche tecniche e massimo risparmio energetico oggi possibile, grazie al nuovo processore Ambarella S2LM. Hanno un sensore CMOS con risoluzione 4K (3840x2160 pixels) per immagini di altissima qualità, 4 volte più dettagliate delle tradizionali telecamere 1080p (2MP). Hanno una vasta gamma di funzioni evolute, tra cui la video analisi integrata la tecnologia WDR, wide dynamic range, che assicura ottime prestazioni nelle riprese in controluce e con scarsa illuminazione, due delle situazioni più difficili per le telecamere di sorveglianza.

Un nuovo sensore evoluto commuta le modalità day/night in modo dinamico e accurato, in funzione delle necessità ed in base ai livelli di illuminazione.

Sono certificate IP67 e IK10 anti-vandalo e lavorano a temperature comprese tra i -40°C e +60°C. Le dimensioni compatte le rendono ideali in tutte le applicazioni: scuole, alberghi, negozi, uffici, industrie e centri commerciali.

DIAS presenta il nuovo rivelatore NV35MR di PARADOX.

DIAS SRL

(+39) 02 38036901

www.dias.it



Il nuovo rivelatore passivo d'infrarossi a effetto tenda NV35MR di PARADOX distribuito da DIAS è ideale per protezione di porte e finestre. E' progettato per essere installato sia all'esterno sia all'interno e offre una rilevazione precisa, un'elevata immunità ai falsi allarmi e agli animali domestici e un'altissima affidabilità. Per uso esterno, fornisce un rilevamento di qualità superiore pur rimanendo immune a piccoli uccelli, cani e gatti, mentre in modalità per utilizzo interno fornisce un raggio ampio e un rilevamento maggiore. Il rivelatore NV35MR offre una protezione a tenda (fascio ottico da 0,5m a 5m) che consente il movimento in prossimità della porta o della finestra protette senza generare falsi allarmi.

Caratteristiche: Super Pet immunity con ottica geometrica per aumentare l'immunità agli animali; funzione antimascheramento; doppio rivelatore controllato da Full Authority Digital Electronics Control (FADEC); protezione antirimozione e antiapertura; funzione antistrisciamento; conforme EN 50131-2-2 Grado 2 Classe IV.

BNC a crimpare o a compressione. ELAN ha la soluzione.

ELAN SRL

(+39) 071 7304258

www.elan.an.it



BNC a crimpare o BNC a compressione? Questa è una domanda che molti installatori si fanno costantemente.

In molti prediligono il BNC a compressione, formato da sole 2 componenti, con il quale è possibile risparmiare tempo e fatica. Questo tipo di BNC infatti richiede una sola crimpatura con il pin centrale fisso. Un po' come avere un piede taglia 43 e indossare scarpe taglia 45: se consideriamo un segnale HD digitale il problema si presenta col tempo. Il **BNC a crimpare ELAN**, invece, fa in modo che il pin e il conduttore diventino una sola cosa con la crimpatura. Calzano a pennello. Tagliato lo schermo in eccesso, infilata e crimpata la ferrula, tutto rimane solido e stabile. L'utilizzo di una pinza **crimpatrice ELAN** con **connettori dorati ELAN** su **cavi coassiali ELAN** garantisce piena efficienza e affidabilità. Impiegare 30 sec. in più per crimpare il connettore fa in modo che, fatto il lavoro, non si debba tornare dal cliente, dopo un po' di tempo, per sostituire un connettore a compressione!

Tastiera numerica keypad integra 2.0.

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



Con la tastiera numerica keypad, il N. 1 in Europa nelle soluzioni per l'accesso ad impronta presenta un prodotto che amplia la gamma di lettori d'impronte digitali. Si possono programmare fino a **99 differenti sequenze di numeri** formate da 4 a 8 cifre. Il relè separato garantisce la sicurezza anti-manomissione, a differenza di molte altre tastiere a codici. Il keypad può essere montato **nella porta** durante la produzione, **oppure nel muro** con l'apposito set ad incasso. È compatibile con tutti i dispositivi di apertura elettronici, serrature motorizzate e cilindri wireless. ekey offre una **garanzia di 5 anni su tutta la gamma di produzione**. Prima che un prodotto ekey venga immesso sul mercato, viene sottoposto a approfonditi controlli: resistenza a fattori ambientali e temperature estreme, vibrazioni e shock, impermeabilità all'acqua e molt'altro ancora.

SHORT FACTS: touchpad: 51,7 x 97,1 x 5,6 mm; temperatura d'utilizzo: da -25° C a +70° C; idoneo all'uso esterno, IP 54; 2 LED di stato; cavi staccabili per un facile plug&play; dimensioni della fresatura identiche al lettore integra.

Chiamate di emergenza per prevenzione incendi nei campeggi.

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



ERMES produce una gamma di Help Point su rete LAN per chiamate di emergenza, con il solo audio o con l'audio ed il video, che si adattano perfettamente alle esigenze che si presentano nei campeggi, villaggi e strutture turistiche in generale, come previsto dalla "Regola tecnica di prevenzione incendi" emessa dal Ministero degli Interni con il Decreto del 28 febbraio 2014 ed alla successiva circolare emessa dal Dipartimento dei Vigili del Fuoco del 12 settembre 2014. Queste colonnine SOS sfruttano un qualsiasi collegamento di rete, anche preesistente e condiviso con altri servizi, per consentire ad un utente in difficoltà di contattare in modo semplice, rapido ed efficiente il personale addetto alla gestione delle emergenze. L'affidabilità dei singoli apparati e dell'intero sistema è una delle caratteristiche di maggior importanza da sottolineare in quanto assicura, anche grazie alle funzioni di autodiagnosi, la sicurezza di tali aree. Il collegamento Over IP di questi apparati consente una elevatissima flessibilità potendo utilizzare tradizionali reti LAN su rame, collegamenti wireless o qualsiasi altro tipo di collegamento dati che sia già disponibile o che si voglia implementare.

Nuova serie CIR1200: le telecamere analogiche di alta qualità.

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



Nell'ambito della videosorveglianza analogica, Fracarro propone la nuova serie CIR1200 che si caratterizza per l'eccezionale qualità video e per la grande praticità d'uso. Dotata del nuovo sensore 1/3" CMOS Sony IMX238 che, combinato con il DSP ISP8520 garantisce un'altissima risoluzione fino a 1200TVL, la serie CIR1200 dispone anche della funzione Day&Night con filtro ICR meccanico, per assicurare riprese notturne sempre precise e colori brillanti durante il giorno. Le telecamere sono proposte in tre versioni: oltre alla grandangolare da 3,6mm, sono disponibili anche due varifocali (2,8-12mm e 9-22mm), che garantiscono una grande flessibilità nella selezione dell'inquadratura, facilmente regolabile tramite le 2 viti esterne di Zoom e Focus. Anche l'installazione è molto semplice grazie al menu OSD gestibile tramite il pratico joystick integrato nel cavo video; il montaggio inoltre può essere effettuato sia a soffitto sia a parete grazie alla robusta staffa regolabile che integra il passaggio cavi. La protezione IP66 infine, consente il suo utilizzo anche in ambienti esterni.

Tornelli a tutta altezza Full-O-Stile.

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



Le barriere per il controllo degli accessi installate in aree non presidiate, all'aperto, o soggette a numerose sollecitazioni devono essere particolarmente resistenti. È per questo che in situazioni quali stadi, siti archeologici, parcheggi o stazioni dei mezzi di trasporto sono spesso usati i varchi Full-O-Stile prodotti da Gunnebo. Praticamente invalicabili, costituiscono una barriera fenomenale per i tentativi di passaggio fraudolento; allo stesso tempo sono facili da usare e consentono un flusso rapido e ordinato delle persone autorizzate. Robustissime e con ridottissime esigenze di manutenzione, sono state installate recentemente alla stazione S. Siro della linea metropolitana 5 di Milano, in corrispondenza dello stadio, proprio per la capacità di resistere alle sollecitazioni date dal passaggio delle esuberanti tifoserie.

HESA presenta le nuove centrali Serie PowerNEO di DSC.

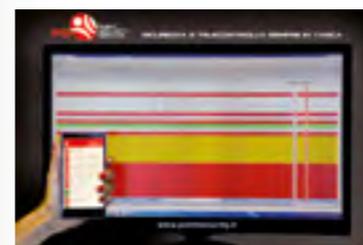
HESA SPA
 (+39) 02 380361
www.hesa.com



HESA presenta le nuove e tanto attese centrali Serie PowerNEO di DSC. Disponibili in quattro modelli da 6 e da 8 zone espandibili fino a 128 zone cablate o senza fili, con possibilità di creare da 2 a 8 aree indipendenti, queste centrali sono state progettate per coniugare la massima affidabilità ad una grande semplicità di gestione, di manutenzione e di programmazione. Caratteristica che contraddistingue le centrali Serie PowerNEO è la possibilità di verifica video degli eventi che hanno fatto scattare l'allarme grazie ad un avanzato rivelatore con telecamera a colori integrata abbinato alle centrali. Le centrali Serie PowerNEO gestiscono una linea completa di dispositivi bidirezionali senza fili, tra cui tastiere senza fili LCD a 32 caratteri con retroilluminazione, sirene interne ed esterne bidirezionali, contatti magnetici, rivelatori passivi di infrarossi, rivelatori d'urto, pulsanti di allarme panico e telecomandi a 2 e a 4 tasti programmabili. L'integrazione senza fili a 868MHz delle nuove centrali Serie PowerNEO è completamente bidirezionale.

La piattaforma di supervisione P.S.S.

POINT SECURITY SOFTWARE
 (+39) 030 2039010
www.pointsecurity.it



La piattaforma di supervisione Point Security Service (P.S.S.) è stata ideata e progettata in base alle reali esigenze degli operatori nel settore dei sistemi di sicurezza, antintrusione, rilevazione incendio, controllo accessi e tvcc. Point Security Service può essere utilizzata per i processi evoluti di manutenzione, post vendita e facility, è volta ai sistemi di building automation, per gestire una concreta e ideale area di lavoro e di processo di diversi protocolli, quali Konex, Profibus, PLC ed SDK. Il software rappresenta una nuova opportunità di crescita per le aziende legate al mondo della security&safety e della grande distribuzione. Particolare attenzione è stata dedicata allo sviluppo dell'area Saving Energy. Sono state utilizzate competenze ed esperienze degli operatori del settore, creando un focus group su scala nazionale, che ad oggi usufruisce di questo strumento per personalizzare i propri impianti, centralizzare le proprie tecnologie, utilizzando un modello di lavoro intraprendente giovane e dinamico.

Sorveglia la tua abitazione, ovunque tu sia!

PYRONIX
01709 700100
www.pyronix.com



La nuova **APP HomeControl+** è compatibile con Android e iOS per controllare la centrale Enforcer32-WE APP utilizzando lo Smartphone come tastiera wireless. L'infrastruttura Cloud (www.PyronixCloud.com) fornisce agli utenti una piattaforma semplice e sicura che consente di connettersi alla centrale da remoto tramite l'App HomeControl+. Ora l'utente può inserire/disinserire le aree, conoscere lo stato ed escludere i sensori, leggere lo storico degli eventi, attivare le uscite domotiche solo toccando il proprio smartphone. Con le Notifiche Push si possono ricevere gli aggiornamenti in tempo reale dello stato del sistema da qualsiasi luogo del mondo, utilizzando l'HomeControl+ e il PyronixCloud. A breve l'App HomeControl+ integrerà i sistemi intrusione Pyronix con la gestione del video, sempre attraverso l'infrastruttura PyronixCloud, consentendo agli utenti di verificare in tempo reale le immagini delle telecamere attraverso l'App HomeControl+, oltre al normale controllo della centrale di allarme. Con l'infrastruttura PyronixCloud l'installatore abilitato può collegarsi da remoto alla centrale per programmare e effettuare la diagnosi delle proprie installazioni.

Nuovo Sensore Volumetrico DT Saet!!! DT PLATINO.

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



Rivelatore vol. doppia tecnologia composto da sez a Microonde (MW) e sez Infrar. Passivo (PIR) per installazioni altamente professionali. Sistema GLAS (Global Ant imasking System), con Antimasch. su MW, Antimasch. Attivo su IR, e sistema ABP1 / ABP2 (anti occultamento dell'intruso). Set di resistenze DEOL di fine linea per singolo e triplo bilanciamento. Port. 18m

Sensore DT da int. con Antimasch. uscita reed - Cod. PA6060

Sensore DT da int. con Antimasch. con interfaccia seriale - Cod. PA6061

Compensazione aut. temp (-10 °C / + 55 °C); portata MW regolabile da trimmer; mod. rilevazione: AND - OR; sensib. regolabile su due liv; copertura max: 90° a 18 mt; resistenze di fine linea selezionabili e programmabili con dip Switch; assorb.: 26mA (in memoria allarme) - 12mA (in stand by); anti fluorescent digital processing; MW: 8dBm 10,525 Ghz. lente di Fresnel a 18 fasci su 4 piani con Look Down Zone, con emissione impulsata a basso impatto ambientale; blocco MW selezionabile; mem. del tipo di allarme temporizzata; installabile a parete o a soffitto con snodo Hub (optional). Col: bianco, dim. 108 x 64 x 46 mm.

La piattaforma CST contro l'insider attack dei varchi.

TSEC S.p.A.
(+39) 030 5785302
www.tsec.it



L'insider attack è uno dei rischi più significativi per i sistemi di sicurezza moderni: per contrastare questi attacchi si devono utilizzare nuove tecnologie di protezione perimetrale. Spesso gli attacchi avvengono dall'interno del perimetro protetto, sia da parte di dipendenti che di visitatori, soprattutto quando i sistemi di sicurezza devono supervisionare varchi temporizzati (bussole, uffici cassa, ecc.) o uscite di sicurezza. Con la piattaforma CST di TSEC, per la prima volta questi problemi possono essere risolti con una tecnologia completamente passiva.

Coppia sensore/magnete codificata

Il contatto riconosce il proprio magnete: la Coded Sensor Technology, esclusivo brevetto TSEC, permette di realizzare coppie di sensori e magneti codificate.

Circuito antimascheramento indipendente

Tentativi di utilizzare un magnete diverso da quello codificato causano l'apertura di un circuito di tamper 24h indipendente dal contatto primario.

Sensori passivi compatibili con tutte le centrali

I sensori CST, nonostante la loro tecnologia avanzata, si presentano alle centrali come comuni contatti passivi: compatibilità completa con ogni marca di centrale.

Conosciamo l' HDCVI?

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



Conosciamo l' HDCVI?

La tecnologia HDCVI, High Definition Composite Video Interface, sviluppata e brevettata da Dahua, permette le trasmissioni video in alta definizione su lunghe distanze ad un costo contenuto, con l'uso di cavi coassiali per trasmissioni video standard analogiche in alta definizione.

Trasmissioni a lunga distanza

Garantisce trasmissioni di alta qualità ed affidabilità. In particolare sino a 1200m a 720P, 800m a 1080P con il cavo coassiale RG6 e 800m a 720P e 500m a 1080P con il cavo coassiale RG59. Con il cavo CAT6 UTP, la distanza di trasmissione a 720P è 450m e a 1080P è 300m.

3 segnali trasmessi su un unico cavo coassiale

I segnali video, audio e controllo sono modulati insieme e trasmessi su un unico cavo coassiale.

Aggiornamento semplice e veloce

I sistemi analogici possono essere facilmente portati alla versione HDCVI a costi contenuti.

L' HDCVI sta guidando l'innovazione dell'HD in tutto il mondo ed usare i prodotti HDCVI per sostituire quelli analogici è ormai una tendenza inevitabile.

VIDEOTREND è il distributore ufficiale per l'Italia di DAHUA Technology.



n. 04 luglio-agosto 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

Simone De Titta, Nils Friedrik Fazzini, Giulia Lazzeri, Giuseppe Mastromattei, Paul Zaal

SEGRETERIA DI REDAZIONE

redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI

marketing@securindex.com

EDITORE

Secman srl
Verona - Via Bozzini 3/A
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

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

GRAFICA/IMPAGINAZIONE

Lilian Visintainer Pinheiro
contatto@lilastudio.it

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

AVIGILON

www.avigilon.com
I Romana, 60 - 61

CAME

www.came.com
56 - 58, 91 - 92, III Copertina

DAHUA

www.dahuasecurity.com
2 - 3, 66 - 67, 107, 111

EKEY BIOMETRIC SYSTEMS

www.ekey.net
62 - 64, 108

FONDAZIONE ENZO HRUBY

www.fondazionehruby.org
87, IV Copertina

HESA

www.hesa.it
19, 109

INTERSEC

www.intersecexpo.com
59

MICRONTEL S.P.A.

www.microntel.com
26 - 28

NEDAP ITALY

www.nedapretail.com
80 - 82

PYRONIX

www.pyronix.com
70 - 71, 110

SATEL

www.satel-italia.it
Copertina, 6

TECHNOAWARE S.R.L.

www.technoaware.com
48 - 52

AXITEA

www.axitea.it
20 - 22

CITEL

www.citel.it
46 - 47, 53 - 55

DIAS

www.dias.it
74 - 76, 107

ERMES

www.ermes-cctv.com
92, 108

FRACARRO

www.fracarro.it
108

HOME AND BUILDING

www.expohb.eu
102 - 103

ISEO SERRATURE

www.iseoserrature.it
23 - 25

MILESTONE SYSTEMS

www.milestonestems.com
13, 48

ONVIF

www.onvif.org
8 - 9

SAET ITALIA

www.saetitalia.it
68 - 69, 110

SICUREZZA 2015

www.sicurezza.it
98 - 101

T-SEC S.P.A.

www.tsec.it
35 - 37, 110

BANCA MPS

www.mps.it
95

CPSE

www.cpse.com.cn
104 - 106

ELAN

www.elan.an.it
II Copertina, 107

EURALARM

www.euralarm.org
10 - 15

GUNNEBO

www.gunnebo.it
43, 44 - 45, 78 - 79, 109

ICIM

www.icim.it
83 - 85

KABA

www.kaba.it
72 - 73

MIRASYS LTD

www.mirasys.com
29 - 31

POINT SECURITY SOFTWARE

www.pointsecurity.it
109

SAMSUNG

www.samsungcctv.com
32 - 34

ALL-OVER-IP 2015

www.all-over-ip.ru
65

VIDEOTREND

www.videotrend.net
2 - 3, 66 - 67, 107, 111



**LA MIGLIOR DIFESA
PER LA TUA CASA**

Sicurezza e controllo: connessi



Scopri Ermet
con Fabio Cannavaro
came.com/ermet

Came lancia le più avanzate tecnologie per garantire
sicurezza e controllo: connessi!

Sicurezza e alte prestazioni per Came hanno la stessa importanza e si fondono
insieme nella nuova generazione di centrali radio Ermet. I nuovi impianti di
sicurezza per la casa sono caratterizzati da un sistema innovativo che raccoglie
tutte le funzioni, l'affidabilità e la praticità dei prodotti antintrusione Came.
Grazie all'integrazione con la domotica di Came, queste caratteristiche sono
affiancate dalle più innovative funzioni di controllo che rendono il sistema
antintrusione parte integrante di un progetto domotico evoluto, in grado,
attraverso la tecnologia Came Connect, di essere gestito da remoto
in qualsiasi momento.



INTERNET
READY



PSTN



MESSAGGI
VOCALI



WIRELESS



SMS



DOMOTICA

CAMECONNECT
CLOUD CONNECTED TECHNOLOGY

Ermet, il miglior sistema per difendere la tua casa.
Scopri lo con Fabio Cannavaro.

Visita il sito came.com/ermet

Official Partner



MILANO 2015
FEEDING THE PLANET
ENERGY FOR LIFE



CAME
safety&comfort

securindex.com

Il primo portale italiano per la security

PREMIO H D'ORO
H

2006 • 2015

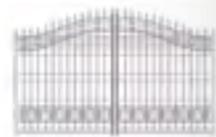


DIECI ANNI

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