essecome
security&safety
04
DUEMILATREDICI
ANNO XXXIII - I
PERIODICO DI INFORMAZIONE SU TECNOLOGIE, APPLICAZIONI E PROBLEMATICHE DELLA SICUREZZA

in collaborazione con

UNIVERSITÀ DEGLI STUDI DI GENOVA

con il patrocinio di:

COMUNE DI GENOVA

REGIONE LIGURIA

CPEXPO®

COMMUNITY PROTECTION

29/30/31 OCTOBER 2013 FIERA DI GENOVA

International Conference and Exhibition

Per approfondire il tema della protezione delle comunità e dei cittadini, ponendo in risalto il ruolo fondamentale del funzionamento sicuro e efficiente delle infrastrutture critiche e le loro interconnessioni.

Per il confronto costruttivo internazionale tra Politica, Istituzioni e Ricerca, grande Committenza e Industria.

Per analizzare un settore economico in costante espansione, per capire la sua evoluzione e fornire una "visione integrata" su rischi, minacce e soluzioni.

Per favorire l'accesso a nuovi mercati internazionali, le partnership pubblico-private e per stimolare l'avvio di nuovi modelli di sviluppo sostenibili.

Per creare una piattaforma stabile dedicata a favorire l'incontro tra domanda e offerta, integrata da specifici servizi di assistenza, in un mercato ricco di molteplici opportunità.

50 Seminari|3 Sessioni Plenarie|Area demo|3 giorni di expo-conference

www.cpexpo.it

SISTEMI DI SICUREZZA INTEGRATI

VIDEOTREND

dahua

technolife
tecnologie per la vita

EYEON

Telecamere HD-SDI. Telecamere IP Megapixel. Videoregistratori di Rete. Speed Dome. Monitor LCD. Telecamere Analogiche. Videoregistratori Digitali. Video Wall. Armadi Rack. Fibre E Convertitori Ottici. Switch Di Rete. Fibre Ottiche. Accessoristica Professionale. Matrici Video. Custodie. Illuminatori IR. Gruppi di Continuità. Sistemi Di Connessione Wi-Fi. Sistemi antintrusione. Sistemi domotici.

www.videotrend.net

DISTRIBUTORI AUTORIZZATI

Distributore Piemonte
Doppler Srl
www.doppleronline.it

Distributore Como
Sicurtel Snc
www.sicurtel.com

Distributore Monza e Brianza
DSA Brianza Srl
www.dsabrianza.com

Distributore Milano Nord Ovest
Tecnocity Srl
www.tecnocitysrl.it

Distributore Milano Nord Est
Nibra Srl
www.nibra.it

Distributore Brescia e Bergamo
Com.pac. Srl
www.compacsrl.com

Distributore
Padova, Verona, Rovigo
B&B Tecnosystems Sas
www.bebtecnosystems.com

Distributore
Trentino Alto Adige
Pamitron Srl
www.pamitron.com

Distributore Toscana
AST Srl
www.astweb.net

Distributore Abruzzo
2B Automazioni e sicurezza
www.2bautomazioni.com

Distributore Roma e provincia
Checkpoint Srl
www.checkpointroma.com

Distributore Puglia
Digital System Srl
www.digitalsystemsrl.it

Distributore Campania
Vitekna Srl
www.vitekna.it

Distributore
Palermo, Agrigento e Trapani
Decibel Srl
www.decibelpro.it

www.eyeon.it

I 4 topic della sicurezza secondo gli analisti internazionali

In un mercato sempre più globalizzato succede spesso di riscontrare che scenari e tendenze rilevati nel mondo dagli analisti si manifestino prima o poi anche in Europa e in Italia. Non è quindi una perdita di tempo seguire i report che arrivano numerosi in redazione, dai quali si possono trarre indicazioni importanti su cosa succederà anche a casa nostra. Abbiamo fatto una selezione dei 4 temi più frequentati nel 2013, in base al numero di press release pervenuti, alla reputazione delle fonti e alla rilevanza per il nostro mercato.

Il sorpasso relativo. Secondo i report di settore la videosorveglianza in rete avrebbe finalmente messo la freccia di sorpasso nei confronti di quella analogica. Diciamo "finalmente" perché, considerando da quanto tempo se ne parla, verrebbe quasi da stupirsi che ci siano ancora in giro produttori di sistemi analogici. In realtà secondo IMS Research (IHS), il sorpasso avverrà soltanto in termini di fatturato e non di numero di pezzi venduti, perché ampie fasce di utenti rimarranno legati ancora a lungo all'analogico. Una recente ricerca aveva rivelato che nel mercato consumer USA i pezzi analogici avevano addirittura ri-superato quelli digitali, perché costano meno e sono più facili da installare; nell'immenso mercato di sostituzione del mondo bancario e delle PA, che per primi si erano dotati di TVCC, i sistemi in rete vengono presi in considerazione esclusivamente per i nuovi impianti. È dunque sorpasso, ma soltanto relativo!

Integrazione ante litteram. Per anni si è parlato grossolanamente di "integrazione" e di "interoperabilità" tra sistemi eterogenei, prima di scoprire che sono modalità identificate da un termine e da una tecnologia ben precisi e con un mercato specifico che, secondo Frost & Sullivan, sta crescendo a due cifre nel mondo.
PSIM è l'acronimo di Physical Security Informations Management, una famiglia di middleware che consentono, per l'appunto, di integrare, coordinare e ottimizzare sottosistemi diversi (videosorveglianza, antintrusione,

controllo accessi, antincendio, energia, clima, etc.) per facilitarne la gestione da parte dell'utente. Infrastrutture critiche, banche, retail, logistica, oil & gas sono tra gli utenti naturali di soluzioni PSIM che vedono (finalmente) aziende italiane con livelli di esperienza e di competenza secondi a nessuno.

SaaS, VsaaS o AcaaS? Sembrano giochi di parole ma indicano le direttrici dello sviluppo della sicurezza nel futuro. Security as a Service ma anche Software as a Service, Videosurveillance as a Service, Access control as a Service sono le "nuove" modalità di vendita che arrivano al traino delle truppe ICT sbarcate nella sicurezza fisica. Quest'anno sembrano andar di moda le acquisizioni di società specializzate in VsaaS cloud based e non c'è report che non preveda crescite iperboliche di questo segmento nei prossimi anni. Nel loro piccolo, gli istituti di vigilanza italiani offrono impianti di allarme in comodato da almeno 30 anni anticipando anche in questo caso la definizione ma, per l'appunto, sono stati e sono ancora troppo piccoli per fare tendenza…

Unitevi e certificatevi. Secondo gli analisti, uno dei principali ostacoli all'integrazione dei sistemi di controllo accessi e antintrusione deriva dalla mancanza di protocolli condivisi tra i principali produttori mondiali, come invece è avvenuto nella videosorveglianza in particolare con Onvif. È facile immaginare che prima o poi qualcosa si muoverà, data l'importanza degli interessi in gioco. Su scala diversa, il problema si pone tuttora con l'unificazione delle certificazioni di prodotto in ambito europeo. Malgrado i proclami lanciati lo scorso anno dal commissario UE all'industria (il nostro Antonio Tajani), la certificazione unica europea appare ancora come un miraggio per i nostri produttori, costretti a moltiplicare prove, costi e tempi per quanti sono i paesi in cui intendono penetrare. Non sarebbe il caso che, almeno per una volta, si riesca seriamente "fare sistema" tra le associazioni, gli enti di certificazione e le nostre autorità governative preposte per rimuovere questo anacronistico ostacolo per l'export, che appare sempre più l'unico, vero toccasana per la nostra industria?

Sommario

News

SCENARI

6 Euralarm, il libro bianco della sicurezza europea

13 Il punto della situazione secondo Assosicurezza

16 Chi forma i formatori? - 2ª puntata

INTERVISTA

18 La formazione secondo il CFS di HESA

20 La formazione secondo Gazzoli Engineering

AZIENDE

24 NO LIMITS! Come imprimere energia a tutto il mercato

SCENARI

28 Infrastrutture critiche, il centro dell'attenzione

AZIENDE

32 Infrastrutture Critiche, PSIM per il DLGS 61

SCENARI

38 Nasce l'Osservatorio di Eurispes sulla Sicurezza

EVENTI

43 Gli eventi di CPExpo

Technologies

INTERVISTA

47 Ermes Elettronica a CPEXPO per la sicurezza delle comunità

CASE HISTORY

50 GS250 di Paradox: una protezione a regola d'arte

ZOOM PRODOTTO

54 Da Venitem un nuovo alimentatore switching

CASE HISTORY

56 FLIR-Aimetis Symphony™ una migliore protezione perimetrale a costi ridotti

INTERVISTA

59 Communication network quali prospettive?

62 JVC, ritorno dal futuro

Money

INTERVISTA

64 SIA acquista Emmecom ed entra nella sicurezza

SCENARI

67 Accessibilità e controllo: valutare il livello di esposizione a crimini predatori

People

AZIENDE
71 Oil & Gas, il terreno della sicurezza globale

SCENARI
74 Stride la vampa…!

Security Services

EVENTI
77 Federsicurezza e il default della vigilanza privata

SCENARI
81 Vigilanza, la parola alle guardie giurate

Fiere

FIERE
83 Wise, la porta per il mercato polacco
85 Kenya, un mercato da scoprire
87 CPSE 2013: Shenzhen calling
90 Sicherheits Expo München supera tutte le aspettative
91 Calendario Fiere

REDAZIONALI TECNOLOGIE
92-93-94

in copertina...

"NO LIMITS" è forza, idee e strumenti necessari a tutti gli operatori della Sicurezza per essere sempre più preparati e vincenti.
Qui possono cogliere molti aspetti a favore della loro attività: cavalcare l'ECOSISTEMA, arricchire la formazione con un metodo OPEN, attuare un GENTLEMAN BUSINESS AGREEMENT per far crescere la propria Azienda con Milestone Systems.
Milestone Systems è sviluppatore globale di software per la gestione di video IP su piattaforma aperta.
La piattaforma XProtect offre potenti funzioni di sorveglianza, è facile da usare, solida e collaudata in migliaia di installazioni presso clienti di tutto il mondo.
Garantendo la più ampia scelta del settore per hardware di rete e integrazione con altri sistemi, XProtect offre soluzioni ottimali per introdurre le applicazioni video nelle aziende — gestendo i rischi, proteggendo persone e beni, ottimizzando processi e riducendo i costi. Il software Milestone è distribuito attraverso partner autorizzati e certificati.

Euralarm, il libro bianco della sicurezza europea

a cura di Raffaello Juvara

Nella scorsa primavera Euralarm ha presentato un libro bianco con le proposte dell'associazione per la competitività dell'industria europea della security e la sicurezza dei cittadini, indicando le priorità politiche e un'agenda programmatica per il triennio 2013-2015. Nel documento sono espressi i principi che Euralarm considera fondamentali per il futuro del settore, in particolare per quanto riguarda il sostegno al comparto nella competizione a livello mondiale e il processo di unificazione delle certificazioni a livello comunitario. Un tema, quest'ultimo, di estrema importanza per i nostri produttori, che devono guardare ai mercati oltre confine per compensare la stagnazione di quello interno, e hanno quindi particolare bisogno che vengano abbattute le barriere protezionistiche che sopravvivono tuttora sotto forma di certificazioni nazionali a difesa di taluni mercati europei, come ha denunciato il vice presidente di ASSOSICUREZZA Renato Cavalleri nell'intervista che pubblichiamo nelle pagine seguenti. Il tema, peraltro, risulta recepito dal governo comunitario, che già nel 2012 aveva annunciato un programma per l'unificazione delle certificazioni (vedi nel numero di Essecome di agosto 2012 l'intervista al commissario europeo per l'industria Antonio Tajani) ma, al momento, i riscontri sul campo sono ancora di là da venire.
Si capirà nel prossimo futuro se l'azione lobbistica condotta dai sostenitori dell'unificazione riuscirà a prevalere nei confronti dei poteri avversi, forse individuabili in taluni enti di certificazione e in talune aziende operanti nei mercati locali più ricchi, magari associate a Euralarm stessa. All'assemblea di ANIE Sicurezza del 20 giugno il vice presidente di Euralarm, Enzo Peduzzi, ha illustrato agli operatori italiani le linee guida del libro bianco di cui, stante la rilevanza, pubblicheremo il testo integrale tradotto in italiano in tre puntate, a partire da questo numero. Il pdf dell'originale in lingua inglese è postato in www.securindex.com/library.

LA VISION PER UN'INDUSTRIA EUROPEA DELLA SICUREZZA PIÙ COMPETITIVA E UNA SOCIETÀ PIÙ SICURA
1ª parte

INTRODUZIONE

Mentre l'Unione Europea deve affrontare una delicata situazione economica e politica, l'industria europea della sicurezza presenta un potenziale senza pari per contribuire alla ripresa e favorire la crescita economica. In questo Libro Bianco, Euralarm definisce le priorità politiche e le azioni ritenute necessarie per migliorare la forza innovativa e la competitività globale dell'industria della sicurezza in Europa e, di conseguenza, per migliorare la sicurezza di tutti i cittadini europei. La sicurezza è chiaramente un settore in cui è necessaria "più Europa" e il suo progresso dipende in primo luogo dalla condivisione, da parte degli Stati membri dell'UE e delle Autorità pubbliche competenti, del concetto che, in generale, una visione europea e internazionale sia più utile per l'interesse pubblico che fare affidamento esclusivamente sulle azioni nazionali o locali. Il riconoscimento condiviso di questo concetto è necessario e urgente. Esistono ampi presupposti giuridici per impostare le azioni politiche necessarie a livello comunitario ed Euralarm esorta i responsabili della politica ad agire rapidamente, mantenendo in primo piano gli obiettivi indicati con chiarezza, come in questo caso. È il miglior modo per fare l'interesse pubblico europeo.

Da sinistra: Martin Harvey (Section Security), Marc Chabaud (President Euralarm), Enzo Peduzzi (Chairman Section Services) e Lance Rütimann (Section Fire).

Euralarm indica tre priorità essenziali per la competitività dell'industria europeo della sicurezza e per una società sicura:

1. **Sviluppo di un mercato interno europeo reale per l'antincendio e la security.** Questa deve essere la priorità assoluta. È la condizione essenziale per consentire all'industria europea della sicurezza di esprimere il proprio potenziale a livello continentale e di poter competere con successo a livello mondiale.

Euralarm chiede :

- un quadro di normalizzazione coerente, efficiente e completo;
- uno schema di certificazione paneuropeo giuridicamente vincolante;
- la piena attuazione della Direttiva Servizi.

2. **Garanzia per tutti i cittadini di livelli più elevati di sicurezza antincendio e di security.** Al di là degli aspetti di mercato interno e di politica industriale per il settore, ci sono molteplici aree in cui vi è una chiara esigenza di interventi normativi per migliorare il livello di sicurezza dei cittadini e di sicurezza generale.

Euralarm chiede:

- lo sviluppo di standard paneuropei per attuare soluzioni condivise per le comunicazioni al pubblico e i sistemi di allerta generale;
- l'adozione di una direttiva europea sulla sicurezza antincendio per gli alberghi, al fine di garantire un livello uniforme di protezione per i viaggiatori in tutta l'Unione Europea;
- alle autorità pubbliche di prendere in considerazione le esigenze della sicurezza antincendio e della security per l'armonizzazione dei nuovi requisiti previsti dalla UE sull'efficienza energetica degli edifici.

3. **Supporto alla competitività dell,industria europea della sicurezza nel mercato globale.** Molti dei principali player europei sviluppano una quota significativa delle proprie attività al di fuori dell'Unione Europea e si trovano ad affrontare una forte concorrenza nel mercato mondiale. È di vitale importanza per un crescita competitiva delle aziende europee che il mercato mondiale della sicurezza sia aperto e accessibile.

Euralarm chiede:

- l'introduzione di una legislazione europea per delimitare la responsabilità civile delle Terze Parti. La sua assenza indebolisce la base industriale dell'Unione Europea, ostacola gli investimenti e abbassa l'utilizzo delle tecnologie innovative e dei servizi di sicurezza in Europa;
- la garanzia che le politiche commerciali dell'UE agevolino l'accesso al mercato internazionale attraverso il libero scambio il reciproco riconoscimento e la normalizzazione dei prodotti e dei servizi di sicurezza.

LE PROSPETTIVE

Parliamo del Libro Bianco

A livello UE deve venire riservato il massimo interesse pubblico per i prodotti, i sistemi e i servizi per la sicurezza antincendio e la security che assicurano la protezione delle persone e delle proprietà. In risposta alla crescente domanda di questa protezione proveniente dal nostro mercato domestico e da tutto il mondo, l'industria europea della sicurezza (security + safety) può contribuire molto alla crescita dell'economia e dell'occupazione, purché rimanga competitiva a livello globale.

La rapida evoluzione delle tecnologie digitali e delle loro applicazioni stimola sempre più l'innovazione e il miglioramento delle prestazioni dei sistemi di security e di allarme antincendio per la protezione delle persone e dei beni, mentre si sta trasformando il modo con cui i servizi di protezione civile possono venire integrati e gestiti.

La capacità delle società europee che operano nella sicurezza e, in particolare delle PMI, a rimanere competitive nei confronti di una concorrenza globale sempre più forte e crescente, dipenderà soprattutto dal superamento delle frammentazioni radicate all'interno del mercato europeo. Questo Libro Bianco espone le proposte di Euralarm sulle priorità politiche europee e l'agenda dei lavori ritenuti essenziali per migliorare la sicurezza dei cittadini europei che, a sua volta, dipende dalla forza innovativa e dalla competitività globale che l'industria europea del settore avrà nel futuro. Le nostre opinioni tengono particolarmente conto della Comunicazione della Commissione Europea con il Piano d'azione per una Industria della sicurezza innovativa e competitiva (1) e del documento di accompagnamento del Gruppo di Lavoro «il cui scopo generale è quello di migliorare la crescita e aumentare l'occupazione nel settore della sicurezza della UE» (2). Euralarm ha partecipato attivamente alle consultazioni che hanno portato a questa comunicazione e accoglie quindi con favore il suo spirito, condividendo l'ambizione di includere i sistemi e i servizi di sicurezza che non rientrano ancora nella Direttiva Servizi.

Allo stesso tempo, intendiamo sottolineare la riflessione espressa dalla Commissione a proposito della competitività delle aziende europee del settore e, quindi, della loro capacità di approfittare della crescita della domanda globale; «...la quota delle imprese della UE nel mercato globale della sicurezza potrebbe diminuire di un quinto, scendendo dal 25% del mercato mondiale nel 2010 al 20% nel 2020, se non si interviene per migliorare la competitività del settore della sicurezza».

Il nostro scopo non è di duplicare il lavoro della Commissione, ma piuttosto di affiancarci a esso, in particolare per evidenziare le questioni e le azioni che riteniamo decisive per le futura capacità dell'industria europea della sicurezza di migliorare la sicurezza dei cittadini contribuendo nel contempo alla crescita dell'occupazione in Europa.

SENSORE INERZIALE MAGNETICO CLIC.

Oltre all'allarme, fa scattare l'invidia.

DIMENSIONI REALI

TSec è lieta di introdurre sul mercato una nuova rivoluzione. Affidabilità della tecnologia Magnasphere, livelli di sensibilità alle vibrazioni paragonabili alla miglior sensoristica oggi disponibile e compatibilità con le schede di analisi più comuni. Il tutto in un involucro estremamente compatto adatto all'incasso a scomparsa senza vincoli di posizionamento. Nuovi sensori inerziali CLIC: cedete all'invidia.

La rivoluzione TSec è solo all'inizio. Seguiteci, vi stupiremo. ▸ www.tsec.it

TSec
TECHNOLOGY FOR SECURITY

CLIC

LA NECESSITÀ DI UN CAMBIAMENTO DELLA ROTTA POLITICA

Estratto dal Documento del Gruppo di Lavoro della Commissione (3): «Il problema di fondo che deve affrontare il settore è costituito dal fatto che le politiche per la sicurezza sono ancora una prerogativa nazionale, per cui i singoli Stati delegano soltanto potere limitato alle entità sovranazionali. Inoltre questo problema è aggravato dalla diversa percezione delle minacce, con conseguenti valutazioni divergenti fra gli Stati membri nell'UE. Ogni Stato membro ha un proprio specifico background culturale e geopolitico, che influenza direttamente le scelte prioritarie in materia di sicurezza. Per esempio alcuni Paesi hanno a che fare più spesso con disastri naturali, come terremoti o grandi incendi boschivi, mentre altri sono stati più volte vittime di attacchi terroristici».

Euralarm condivide pienamente questa valutazione politica (come, del resto, ha fatto oltre l'86% degli operatori pubblici e privati consultati preventivamente della Commissione), perché spiega in gran parte le cause della frammentazione del mercato europeo e delle conseguenti prospettive di erosione della competitività dell'industria europea a livello mondiale.

Inevitabilmente la frammentazione del mercato ostacolerà in misura sempre maggiore la diffusione capillare in Europa a costi accessibili delle innovazioni all'avanguardia e delle migliori pratiche fondamentali per la protezione delle persone e dei beni, in un mondo che diventa sempre più complesso e incerto.

La concretizzazione degli interventi politici proposti da questo Libro Bianco dipende, quindi, in primo luogo dalla condivisone del riconoscimento da parte dei governi degli Stati membri dell'UE e delle autorità pubbliche responsabili della sicurezza che le

politiche e le prassi relative alla sicurezza nazionale (e spesso locale) non sono più in grado di garantire da sole i risultati migliori per l'interesse pubblico. È invece necessaria e urgente una visione europea e internazionale.

I COSTI DELLA NON-SICUREZZA

In questi tempi di ristrettezze economiche gli investimenti in sicurezza vengono visti come un lusso insostenibile. Questa percezione non tiene conto dei costi diretti e indiretti della non-sicurezza. Le stime citate dalla Commissione hanno valutato il totale del mercato europeo per i prodotti e i servizi di sicurezza in euro 36,5 miliardi (4), dei quali 16,4 vengono attribuiti ai membri di Euralarm (sistemi elettronici di sicurezza).

Anche supponendo che queste siano stime sottovalutate, sono ordini di grandezza che impallidiscono nel confronto con i costi crescenti della non-sicurezza. Una ulteriore stima (5) quantifica, infatti, i costi diretti della non-sicurezza in 1.100 miliardi di Euro all'anno, pari al 6% del PIL dell'Europa a 27, peraltro non comprendendo in questo importo elevatissimo costi derivanti dagli incidenti e dagli infortuni mortali. Deve essere inoltre considerato che queste stime non possono cogliere il vero significato che può avere per la società europea la diffusione della percezione inconscia di poter vivere e lavorare in un ambiente sicuro.

IL FATTORE PMI

L'industria europea della sicurezza è caratterizzata da una percentuale molto elevata di piccole e medie imprese (PM) diffuse in tutta Europa.

Per rimanere competitive, esse si basano in genere su innovazioni altamente mirate, che devono essere in grado di portare rapidamente sul mercato per arrivare prima dei concorrenti. In caso contrario, viene compromessa la loro capacità di competere e di crescere.

La complessità, i costi e i tempi necessari per ottenere le certificazioni di conformità alla diverse normative degli stati membri troppo spesso limitano le PMI ai rispettivi mercati nazionali, impedendo loro la possibilità di sfruttare le proprie innovazioni in quello che sarebbe, potenzialmente, il più grande mercato della sicurezza del mondo.

Questo mette le PMI europee in una posizione di particolare svantaggio rispetto alle grandi multina-

zionali concorrenti , in grado di organizzare e finanziare contemporaneamente in più paesi la certificazione di conformità per le proprie innovazioni.
Un sistema di certificazione unificato a livello UE darebbe alle PMI la possibilità di accedere a un mercato molto più ampio, rendendole più competitive e salvando nel contempo l'industria della sicurezza europea nel suo complesso.
Una stima prudenziale quantifica in 29 milioni di Euro all'anno i costi diretti per le certificazioni, senza considerare i costi significativamente più alti causati dal ritardata accesso al mercato.

PRESUPPOSTI GIURIDICI PER L'AZIONE DELLA UE

Tutte le azioni a livello Unione Europea devono trovare un fondamento giuridico nei Trattati. Nel Documento del Gruppo di Lavoro che accompagna il Piano d'azione per una industria della sicurezza innovativa e competitiva, la Commissione ha stabilito quello che rientra nel diritto di intervento della UE per ciascuno dei problemi che si propone di affrontare (6):

- **la sicurezza percepita come una prerogativa nazionale;**
- **la frammentazione del mercato;**
- **il divario tra ricerca e mercato;**
- **l'incerta accettazione sociale delle tecnologie di sicurezza.**

La conclusione che traiamo da questa analisi è semplice: esistono ampi presupposti giuridici per poter attuare le azioni necessarie a livello politico. Ciò che manca è il riconoscimento da parte dei governi degli Stati membri e delle autorità competenti (a tutti i livelli) che la pubblica sicurezza possa venire assicurata meglio in futuro attraverso un'azione comunitaria più incisiva, nell'ambito delle linee indicate dai Trattati. Riteniamo inoltre che ci siano i presupposti sufficienti per dare vita a un mercato unico dei servizi relativi ai sistemi di sicurezza, come l'installazione, la manutenzione e monitoraggio da remoto dei sistemi. Nello stesso tempo la Commissione è stata ben attenta a mettere in chiaro che il Piano d'azione non sarà seguito da nessuna proposta legislativa immediata.
Qualsiasi futura possibile misura di politica legislativa riguardante il settore della sicurezza dovrà venire preceduta da un assessment dedicato agli effetti nonché da approfondite consultazioni delle parti interessate. Anche Euralarm riconosce la necessità di cautela e di chiarezza, in considerazione degli obblighi che la legislazione della UE impone agli Stati membri. Detto questo, Euralarm sollecita i governi europei e i responsabili politici a non trascurare questo tema, essendosi chiaramente dimostrato che costituisce il modo migliore per garantire il raggiungimento degli obiettivi del Trattato.

Il punto della situazione secondo Assosicurezza

a colloquio con Renato Cavalleri, Vicepresidente Assosicurezza
a cura di Raffaello Juvara

Dopo aver pubblicato i dati di mercato del 2012 elaborati da ANIE Sicurezza, abbiamo raccolto i commenti di Assosicurezza, nel corso di una conversazione con il vice presidente Renato Cavalleri che si è estesa ad altri temi di attualità per il settore, come la questione delle certificazioni europee, la formazione, le fiere internazionali.

Secondo ANIE Sicurezza anche nel 2012 il fatturato dell'industria nazionale della sicurezza fisica ha segnato un progresso, andando in controtendenza rispetto agli altri comparti manifatturieri similari raggruppati in ANIE e Assistal. Qual è il commento di Assosicurezza?

Come rappresentante di un'associazione della categoria non posso che esprimere soddisfazione di fronte ai dati del 2012, anche se ritengo che per avere un quadro complessivo e veritiero su come stiano andando effettivamente le cose si debbano prendere in considerazione anche altri fattori, oltre al fatturato. Sono stato molto colpito dal quadro delineato dal presidente di Assistal (la federazione di Confindustria dei costruttori di impianti, a cui aderisce Assosicurezza – NdR), in occasione dell'assemblea del 16 luglio scorso. A fronte di una contrazione del PIL dell'8% tra il 2007 e il 2012, il mercato della componentistica legata alle costruzioni è diminuito del 30%, con una flessione del 21% soltanto nell'ultimo anno. Di fronte a questi numeri il presidente Gargaro si è chiesto come faranno le imprese ad arrivare vive alla ripresa, se e quando arriverà. È una preoccupazione che riguarda anche le nostre aziende, in particolare per l'aspetto finanziario, che spesso sfugge all'attenzione degli analisti. Le difficoltà ad avere finanziamenti dalle banche, sommate alle difficoltà a incassare i crediti non soltanto nei confronti delle PA, possono vanificare qualsiasi risultato brillante sul piano del fatturato.

Possiamo soltanto auspicare che a livello di governo e di sistema bancario emerga la consapevolezza di dover intervenire in tempi rapidi per consentire alle imprese italiane di arrivare vive a quella tanto sospirata ripresa. Entrando nel merito dei dati del 2012, come valuta l'incremento segnato dall'industria italiana che, tra mercato interno e esportazioni, ha messo a segno un +2,51%?

Di per sé è un dato positivo, ma è da guardare con attenzione perché è sempre stato molto difficile ricavare una fotografia esatta di questo mercato. Per esempio, siamo sicuri che al fatturato realizzato dalla produzione non venga sommato, anche solo in parte, quello generato dagli stessi materiali nei passaggi successivi della distribuzione e dell'installazione? Un altro interrogativo: dato che i principali distributori italiani di componentistica di sicurezza trattano quasi esclusivamente materiale importato, come è possibile che il totale dell'import sia "soltanto" di 97 milioni? E quanto del fatturato attribuito alla

produzione è realmente “made in Italy” o deriva, invece, dall’assemblaggio di componenti acquistati all’estero, oppure dalla mera brandizzazione di prodotti OEM?

Sono interrogativi ai quali è oggettivamente difficile dare risposte precise e che riguardano aspetti molto delicati per la struttura di un settore che deve guardare soprattutto verso l’estero. Una condizione che sta rimettendo al centro dell’attenzione la questione delle certificazioni, di cui si sta parlando sempre più anche a livello europeo. Ritiene ci siano stati passi in avanti in questa direzione?

Se posso esprimermi liberamente, le certificazioni europee sono un vero e proprio “pacco”! A tutt’oggi, malgrado i proclami della Commissione Europea di voler unificare le procedure di certificazione, nulla è cambiato: il VDS tedesco continua a non riconoscere le certificazioni rilasciate in altri paesi, e altrettanto dicasi in Francia; in Belgio un Decreto Reale impone che la certificazione debba essere rilasciata utilizzando il modello T014 che, naturalmente, può venire emesso soltanto da enti di certificazione locali. Però l’ANPI (l’ente di certificazione belga – NdR) richiede che i test-report sulla resistenza a vibrazione, shock e anidride solforosa siano timbrati da Accredia (l’ente di accreditamento italiano – NdR) che IMQ non può rilasciare, non essendo accreditato per queste prove.
Se consideriamo, quindi, che per esportare in Germania, Francia e Belgio, che costituiscono mercati esteri molto importanti per i nostri prodotti, è tuttora necessario ottenere e pagare ogni volta le certificazioni rilasciate dai rispettivi enti nazionali, ci vogliono spiegare a cosa servono le certificazioni europee?

Chiarissimo. Guardando gli aspetti operativi legati alle esportazioni, quest’anno Assosicurezza non era presente a IFSEC. Quali sono stati i motivi di una scelta molto notata dagli addetti ai lavori?

È stata una decisione provocata principalmente dai

LE AZIENDE ASSOCIATE AD ASSOSICUREZZA

- Advanced Innovations Srl
- Alba Elettronic Srl
- Argus Security Srl
- Axel Srl
- Axis Communications S.r.l.
- Beta Cavi Srl
- Bosch Security System SpA
- C.E.I.A. SpA
- Cab Commerciale ‘76 Srl
- Cias Elettronica Srl
- Cisa SpA Ingersoll Rand Security Technologies
- Clusit - Associazione It. per la SicurezzaInformatica
- Dallmeier Italia Srl
- D-Link Mediterraneo Srl
- EEA Srl
- El.Mo. SpA
- Elan Srl
- Ermes Elettronica Srl
- Eurogroup Srl
- Fdp International Group Srl
- Gps Standard SpA
- Honeywell Building Solutions Srl
- Honeywell Security Italia SpA
- Lince Italia SpA
- Mesa Srl
- Notifier Italia Srl
- Panasonic Italia brach office di Panasonic Marketing Europe GmbH
- Ramcro SpA
- Safe & Lock Srl
- Scame Sistemi Srl
- Sensitron Srl
- Sicurit Alarmitalia SpA
- Tecnos Srl
- Unitek Italia Srl
- Venitem Srl
- Vimac Security Srl
- Vimo Elettronica Snc di Cavalleri R.L. & C.
- Zucchetti Axess SpA

costi della partecipazione che, tra stand, trasporto, allestimento, energia elettrica e gabelle varie, avevano raggiunto livelli insostenibili, se confrontati con i risultati pratici che si possono realisticamente ottenere da una manifestazione che negli ultimi anni ha perduto progressivamente di interesse. Per questo gli organizzatori riportano IFSEC a Londra, dove si erano tenute le prime edizioni, ma un ulteriore aumento del 10% dei prezzi e la scomodità della location (il polo fieristico Excel – NdR) difficilmente faranno cambiare la tendenza. Assosicurezza parteciperà nel 2014 a Dubai e Essen che, in questo momento, sono le manifestazioni più seguite a livello internazionale. Dubai è una vetrina importante per tutto il mercato medio-orientale, in particolare per le aziende che presentano sistemi completi, mentre Essen è diventata il riferimento di tutto il mercato europeo, anche per il favorevole rapporto tra costi e servizi che offre ai partecipanti.

Affrontiamo un ultimo argomento, quello della formazione degli operatori, che in questi ultimi tempi ha visto ANIE e ANIMA prendere posizione a fianco delle rispettive associazioni ANIE Sicurezza e Assoferma per contrastare la proliferazione dei corsi di formazione organizzati da formatori e aziende non qualificati né, tanto meno, accreditati. Come si sta muovendo Assosicurezza su questo fronte?

Assosicurezza si muove in modo istituzionale nella formazione. In questo momento stiamo partecipando a un gruppo di lavoro presso IMQ assieme a Assistal, AIPS, ANIE Sicurezza e i ministeri interessati per individuare un percorso per la qualificazione degli installatori all'insegna della semplificazione. Ci sarà un primo livello di formazione per la qualificazione di base, demandato alle aziende in possesso dei requisiti organizzativi necessari, al quale seguiranno livelli successivi gestititi direttamente da IMQ. Nel frattempo, continua il nostro impegno con l'Università di Bologna a supporto del Laboratorio di Security e Criminalistica, nell'ambito del corso di Laurea in Scienze criminologiche per l'investigazione e la sicurezza, che si tiene presso la sede di Forlì.

Chi forma i formatori? 2ª puntata

a cura di Cristina Isabella Carminati

Essecome inizia in questo numero il percorso esplorativo tra i protagonisti della formazione aziendale, allo scopo di contribuire ad attribuire al tema della professionalizzazione degli installatori di sistemi di sicurezza la dovuta importanza. Abbiamo già avuto modo di individuare due realtà distinte: la formazione di base individuale, sostenuta da scuole professionali autorizzate, enti di formazione e di certificazione, associazioni rappresentative, e l'addestramento all'uso delle tecnologie sviluppate dalle singole aziende, rispondente a logiche di libero mercato.

In questa seconda puntata incontriamo due importanti realtà italiane: il Centro di Formazione Sicurezza di Hesa e la Gazzoli Engineering.
Entrambe si propongono di sviluppare un'attività educativa mirata a fornire tutti gli strumenti necessari per affrontare ogni possibile scenario nel settore della sicurezza, all'interno di un percorso formativo volto a diffondere la conoscenza delle soluzioni di ultima generazione e ad approfondire i principali aspetti della normativa corrente relativi alla progettazione, alla realizzazione e alla manutenzione dei sistemi di sicurezza.

Panasonic
ideas for life

VIDEO SORVEGLIANZA A 360°

La telecamera dome IP PISF438E fornisce immagini di qualità Full HD a 360° e un'ampia gamma di funzionalità integrate in un telaio discreto e compatto. Utilizza un sensore MOS da 3.1MP di nuova concezione, in grado di produrre immagini HD 1080p@30Fps con multi-stream nei formati H.264 e JPEG.
Grazie alla tecnologia Super Dynamic che fornisce una gamma dinamica 128x, la qualità delle immagini risulta perfetta in qualsiasi condizione di luce.
Sono disponibili diverse modalità di visualizzazione: Wall Panorama, Double Panorama, Quad PTZ, Single PTZ, e Quad streams (H.264/VGA)

www.sicurit.it

PISF438E

i-PRO SmartHD

SICURIT ALARMITALIA

DISTRIBUTORE NAZIONALE

Milano - Via Gadames, 91
Tel. +39 02 380701
E-mail: info@sicurit.it

Torino - Brescia - Padova - Bologna - Firenze - Ancona - Roma - Catania

La formazione secondo il CFS di HESA

a colloquio con Daniela Pitton, responsabile del CFS (Centro Formazione Sicurezza) Hesa
a cura di Cristina Isabella Carminati

Quali sono gli obiettivi della proposta formativa di CFS (Centro di Formazione Sicurezza)?
L'innovazione delle tecnologie, lo sviluppo di nuovi business, l'esigenza di esplorare nuovi segmenti di mercato e di rispondere al meglio alle richieste di sicurezza degli utenti richiedono agli installatori una serie di competenze necessarie per svolgere al meglio la propria attività. HESA si propone quindi di sviluppare un'attività educativa mirata a fornire loro tutti gli strumenti necessari per affrontare ogni possibile scenario che riguarda il settore della sicurezza. Fare formazione significa offrire spunti di riflessione, fornire metodi per migliorare la propria professionalità e contribuire a far nascere nuove idee.
Queste sono le ragioni che hanno spinto HESA a considerare con la massima attenzione l'attività formativa, sviluppandola con il contributo di docenti altamente qualificati e secondo diverse modalità. I funzionari commerciali e i tecnici HESA sono a disposizione dei clienti che vogliono conoscere le novità in gamma e approfondire le potenzialità e il corretto utilizzo dei diversi prodotti. Diversi sono i corsi sviluppati dal CFS (Centro di Formazione Sicurezza) con la collaborazione di docenti esterni. Questi corsi spaziano dagli aspetti tecnici a quelli legali, dalle normative vigenti alle tecniche di vendita, con l'obiettivo di supportare l'evoluzione del settore, elevando il livello e la crescita professionale dei suoi operatori.

I vostri corsi sono rivolti solamente ai clienti HESA (Concessionari, installatori autorizzati) o sono aperti a tutti gli operatori?
I corsi tecnici sono riservati agli installatori che hanno acquistato o desiderano acquistare prodotti

distribuiti da HESA, mentre i corsi di formazione del CFS, così come le presentazioni commerciali, sono aperti a tutti gli operatori del settore.

Quali risultati può vantare il CFS?
HESA ha da sempre un'attenzione particolare all'evoluzione del mercato in cui opera da quasi 40 anni e nel 2011 è stata la prima azienda della sicurezza a creare uno specifico dipartimento di formazione. In soli due anni abbiamo dato vita a ben 14 diversi corsi, replicati 36 volte in nove città italiane. Con nostra grande soddisfazione 336 aziende (67 Concessionari, 57 Installatori Autorizzati e 212 altri operatori del settore) hanno scelto i nostri corsi per formare i propri dipendenti.

Organizzate corsi anche in collaborazione con enti di normativi o di certificazione?
Nell'organizzazione dei corsi è per noi di estrema importanza la scelta di docenti esterni altamente qualificati che siano in grado di dare il massimo contributo alla crescita degli operatori del settore. Da quest'anno abbiamo intrapreso una stretta collaborazione con il CEI (Comitato Elettrotecnico Italiano), sviluppando insieme ai suoi docenti nuovi corsi di formazione, come quelli dedicati al PES (Certificazione Persona Esperta), alla corretta progettazione e installazione delle protezioni perimetrali e all'integrazione dei sistemi per la sicurezza residenziale. Nell'ottica di contribuire all'evoluzione del settore accogliamo con molto favore le proposte di collaborazione da parte degli operatori della sicurezza che intendono fare formazione, mettendo a disposizione l'esperienza e i docenti del CFS per l'organizzazione di corsi specifici. Per fare un esempio ha ottenuto un grande successo l'esperienza con un distributore del Veneto insieme al quale abbiamo organizzato un corso dedicato alle normative e alle responsabilità dell'installatore di sicurezza. Il corso ha visto la collaborazione dell'avvocato Valeria Finazzi, docente del CFS esperta in materia di privacy e responsabilità dell'installatore, e di René Gazzoli, che ha approfondito i temi legati alla parte progettuale dei sistemi di sicurezza.

Che tipo di attestati vengono rilasciati al termine dei corsi?
Al termine dei corsi del CFS e dei corsi tecnici vengono rilasciati attestati che certificano la partecipazione degli installatori a questi validi momenti di approfondimento e di aggiornamento, indispensabili per quanti operano in un settore in costante evoluzione come quello della sicurezza.

CENTRO FORMAZIONE SICUREZZA
PROFESSIONE INSTALLATORE

La formazione secondo Gazzoli Engineering

a colloquio con René Gazzoli, fondatore di Gazzoli Engineering
a cura di Cristina Isabella Carminati

Quali sono gli obiettivi delle proposte formative di Gazzoli Engineering da una parte e di Milestone Systems dall'altra?
Gazzoli Engineering si occupa di Certificazione e di Formazione nell'ambito del Progetto Open Platform. Questo progetto vede coinvolte, oltre a Milestone System, anche le maggiori aziende di produzione e di distribuzione del settore sicurezza, con l'obiettivo di far conoscere e promuovere le soluzioni di sicurezza di ultima generazione.
Tali soluzioni, basate su architetture IP, sono caratterizzate da una elevata integrazione tra i diversi apparati (telecamere ad alta risoluzione, telecamere termiche, telecamere con visione a 360°, sensori di rilevazione esterna di ultima generazione, etc.) e dalla possibilità di utilizzare applicativi di ultima generazione (lettura targhe, analisi video, analisi audio, etc.) e consentono quindi di realizzare sistemi di sicurezza più evoluti, più performanti, più affidabili.
In quest'ambito la formazione ha un ruolo essenziale: oltre a Corsi di Certificazione su alcuni pro-

dotti dei principali partner del progetto, Gazzoli Engineering eroga Corsi di Formazione Tecnica e di Formazione Normativa, inquadrati all'interno di un percorso formativo volto a diffondere la conoscenza delle soluzioni di ultima generazione e ad approfondire i principali aspetti della normativa corrente relativi alla progettazione, alla realizzazione e alla manutenzione dei sistemi di sicurezza. Nell'ambito di questo percorso formativo riscuotono, tra gli altri, particolare interesse i seguenti Corsi:

- Progettazione di sistemi IP
- Sistemi per la protezione delle aree esterne
- Tecniche di video-analisi
- Normativa CEI per sistemi antintrusione e per sistemi di videosorveglianza.

I vostri corsi sono rivolti solamente ai partner di Milestone o sono aperti a tutti gli operatori?

Gli operatori del settore della sicurezza, installatori specializzati e system integrator, provengono da due mondi che negli ultimi anni si sono sempre più avvicinati e integrati:

- la sicurezza tradizionale
- il networking

Le soluzioni di sicurezza di ultima generazione richiedono competenze approfondite in entrambi questi mondi.

Obiettivo principale di Gazzoli Engineering è promuovere, attraverso i propri percorsi formativi, l'acquisizione di tutte le competenze necessarie per la progettazione, la realizzazione e la manutenzione delle nuove soluzioni di sicurezza da parte di tutti gli operatori del settore, quindi non solo ai partner Milestone, creando quindi i presupposti perché si diffondano soluzioni di sicurezza sempre più evolute, più performanti e più affidabili.

Per facilitare il processo di apprendimento alcuni corsi hanno un approccio teorico-pratico: oltre alla presentazione delle soluzioni tecnologiche basate sui prodotti di ultima generazione esistenti sul mercato, sono previste prove pratiche di dimensionamento, di configurazione e di utilizzo dei diversi apparati su sistemi pilota realizzati in aula che simulano le situazioni tipiche dei sistemi di sicurezza destinati alla protezione di edifici residenziali, commerciali o produttivi.

Organizzate corsi anche in collaborazione con enti di normativi o di certificazione?

Organizziamo corsi volti alla diffusione della conoscenza e quindi al rispetto delle norme tecniche, con particolare attenzione alle più recenti Norme CEI EN.

In questo ambito riscuotono particolare interesse i corsi aventi come oggetto:

- le prescrizioni di sistema e i criteri e le metodologie da utilizzare nella progettazione, nella pianificazione, nell'esercizio, nell'installazione e nella manutenzione dei sistemi d'allarme antintrusione e antirapina (Norme delle famiglie 79-2, 79-3 e 50131)
- le prescrizioni di sistema e i criteri e le metodologie da utilizzare nella progettazione, nella pianificazione, nell'esercizio, nell'installazione e nella manutenzione dei sistemi di videosorveglianza (Norme della famiglia 50132).

Che tipo di attestati vengono rilasciati al termine dei corsi?

I corsi di certificazione sui prodotti e sulle soluzioni

dei partner del Progetto Open Platform vengono condotti da trainer preparati e certificati dai partner stessi mediante un opportuno percorso formativo, secondo una precisa e ben definita metodologia:

- il materiale da presentare è concordato con il partner
- le esercitazioni da effettuare sono concordate con il partner

Al termine di ogni corso viene svolto un test, anch'esso condotto secondo una ben definita metodologia:

- domande a cui rispondere definite dal partner
- esercizi da svolgere definiti dal partner

L'attestazione che i partecipanti ricevono alla fine di ogni corso è quindi una Certificazione Ufficiale, emessa dal partner di riferimento, che attesta l'effettiva preparazione e competenza dei partecipanti sugli argomenti oggetto del corso.

Per quanto riguarda i corsi di formazione, che contribuiscono a costruire un'importante base di conoscenza tecnica e normativa, vengono invece rilasciati degli specifici attestati di partecipazione.

GazzoliEngineering

ISAF

www.isaffuari.com

The **Most Comprehensive** Exhibition of the Fastest Growing Sectors of recent years in the **Center of Eurasia**

ISAF IT SECURITY
2ND INFORMATION, DATA AND NETWORK SECURITY EXHIBITION

ISAF SAFETY&HEALTH
2ND OCCUPATIONAL SAFETY AND OCCUPATIONAL HEALTH EXHIBITION

ISAF SMART HOUSES
2ND SMART HOUSES AND BUILDING AUTOMATION EXHIBITION

ISAF SECURITY
17TH INTERNATIONAL SECURITY & RFID EXHIBITION

ISAF FIRE
17TH INTERNATIONAL FIRE PROTECTION, EMERGENCY, SEARCH & RESCUE EXHIBITION

SEPTEMBER 19th-22nd, 2013
ISTANBUL EXPO CENTER (IFM), ISTANBUL/TURKIYE

Supported By

CSGB ÇASGEM TÜMGED YILKODER

MARMARA TANITIM FUARCILIK
www.marmarafuar.com.tr
T. +90 212 503 32 32 | marmara@marmarafuar.com.tr

KOSGEB İSTANBUL

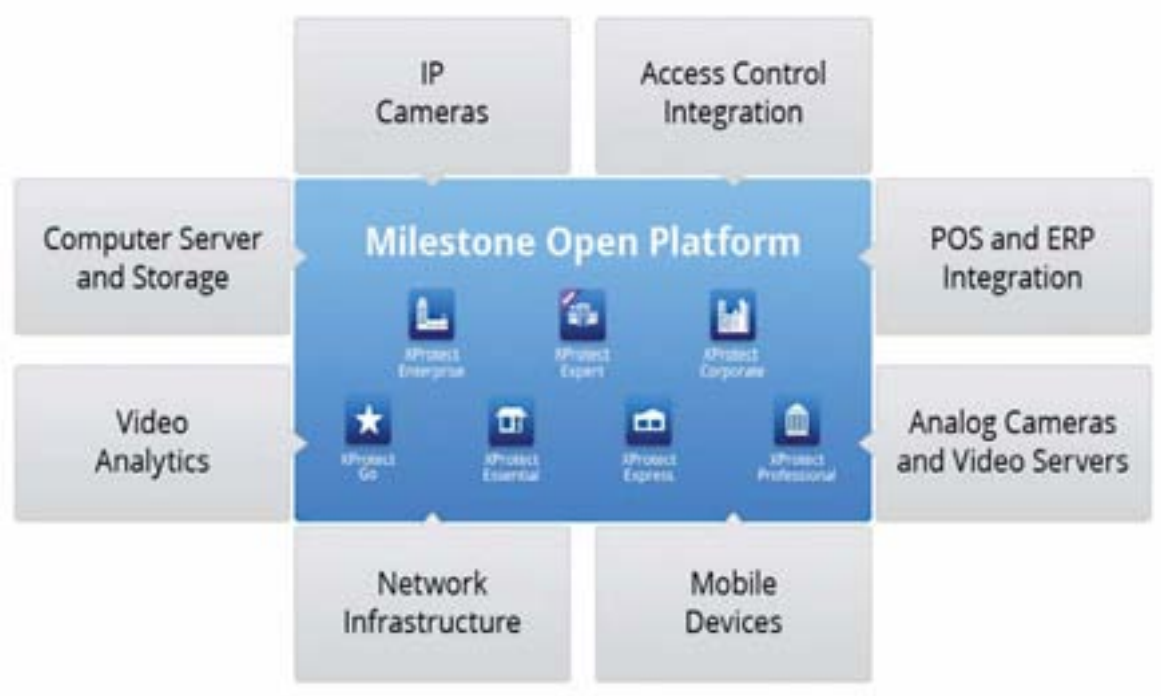
THIS EXHIBITION IS ORGANIZED WITH THE PERMISSIONS OF T.O.B.B. IN ACCORDANCE WITH THE LAW NUMBER 5174.

NO LIMITS!

Come imprimere energia a tutto il mercato

a cura di Maurizio Barbo, Country Manager Italia di Milestone Systems

Milestone Systems, per l'ottavo anno consecutivo, è stata riconosciuta da IMS Research Leader mondiale nel mercato VMS - Video Management System. In Italia segna, nel primo semestre 2013, una crescita vicina al 30%: in una regione dove oltre modo la crisi economica è anche un po' più dura rispetto ad altre nazioni, questo è un segnale positivo non solo per Milestone ma per tutto il mercato della video sorveglianza e della sicurezza. Così, se ora Milestone da una parte sta attuando un processo di consolidamento, dall'altra pensa a come imprimere uno sviluppo e un'accelerazione per tutto il mercato e il comparto che gli ruota attorno. La Piattaforma Aperta Milestone XProtect oggi conta oltre 1069 Milestone Solution Partner, sviluppatori di soluzioni software e hardware su misura: talvolta anche nascosti e poco conosciuti, perché molti sviluppano le soluzioni per il proprio business nell'azienda, altri invece le rendono disponibili per proporle sul mercato come plug-in rivendibile e per lo sviluppo di affari verso tutti. Quindi dare voce e diffondere le soluzioni di Terze Parti, gli MSP Milestone Solution Partners, sarà ancora una volta linea guida per il Team Milestone Italia, e abbraccerà tutti i settori della sicurezza: antintrusione, antitaccheggio, antincendio, controllo accessi e presenze, analisi video e analisi forense, geo localizzazione, etc. (NO LIMITS!). Se vi ricordate, anni fa sono nate associazioni di imprese che avevano lo scopo di spingere un'idea comune d'integrazione, oggi il mercato ha portato ad aprire con forza a questa idea di dialogo tra i sistemi (OPEN). Personalmente, non sento la necessità di associazioni o altro, ma solo di un semplice e sano "Gentleman Business Agreement" tra operatori che hanno buona volontà di innovare e di proporre.



Il "pensare GRANDE", lavorando con tenacia e correndo a mille in tempi ristrettissimi, produrrà risultati inaspettati!

Aggiungiamo poi che siamo "con la bussola in mano, alziamo le vele e… AVANTI TUTTA!". Diamo spazio a nuove idee e a iniziative innovative di qualsiasi tipo! La prima arriva con Forza21Nodi: dove una volta si chiamavano "sub distributori", oggi invece saranno "Wholesalers", un gruppo di professionisti già riconosciuti che, con le nuove tecnologie, il nuovo modo IP e l'Eco Sistema Milestone, vogliono essere in prima linea e farsi portavoce di valori aggiunti per il proprio Cliente, aiutandolo nella formazione, nella progettazione, nello start up del sistema, conducendolo per mano in un mondo di soluzioni & integrazioni sempre più strategiche e vincenti.

Nascerà una ragnatela di Wholesalers a copertura di tutte le 21 regioni italiane, per soddisfare anche territorialmente tutte le aree e tutti i Clienti. Essi saranno supportati dall'attuale Distribuzione Milestone, che già opera in modo eccellente collaborando attivamente allo sviluppo di sinergie comuni come questa. Forza21Nodi diventerà quindi un vettore per soluzioni dell'Ecosistema: in un modo molto più semplice e veloce, tutti arriveranno alla soluzione completa e ricercata (NO LIMITS!), mettendo in connessione diretta l'installatore (richiesta dall'utente finale) con lo sviluppatore, MSP Milestone Solution Partner e/o ricercatori universitari che lavorano "sul pezzo".

Per diventare Wholesaler Milestone, basta contattare un nostro Distributore o direttamente il Team Milestone Italia, la porta è OPEN!

Il progetto Forza21Nodi con i nuovi Wholesalers Milestone sarà un tassello importante, insieme alla Formazione, per questo fine 2013. E la già completa offerta di Formazione con i corsi PROFESSIONAL, ADVANCED, EXPERT e SDK, si arricchirà di altre proposte per perfezionare la linea di Training; ci sarà la possibilità di essere formati in lingua Tedesca nelle aree dell'Alto Adige, ed arriverà anche la possibilità di migliorare le proprie strategie di vendita con il corso MILESTONE VALUE SALLING.

Abbinati a questi, crescerà anche la proposta di Webinar dedicati anche alle singole funzioni dei prodotti XProtect, per avere padronanza nelle caratteristiche delle varie versioni e degli add-on aggiuntivi come, per esempio, utilizzare al meglio la lettura targhe in Milestone XProtect LPR.

Ma ci saranno anche gli MPOP Webinar realizzati con i nostri 118 Partner, produttori di telecamere o encoder, chiamati MAP (Manufacturer Alliance Partners): oggi, con più di 2219 periferiche compatibili in XProtect, oltre a vari dispositivi in serie e dispositivi OEM singolarmente non individuabili, continuano a rilasciare nuovi modelli con nuove funzioni e caratteristiche: si può quindi, realmente mirare la telecamera su misura per la propria installazione.

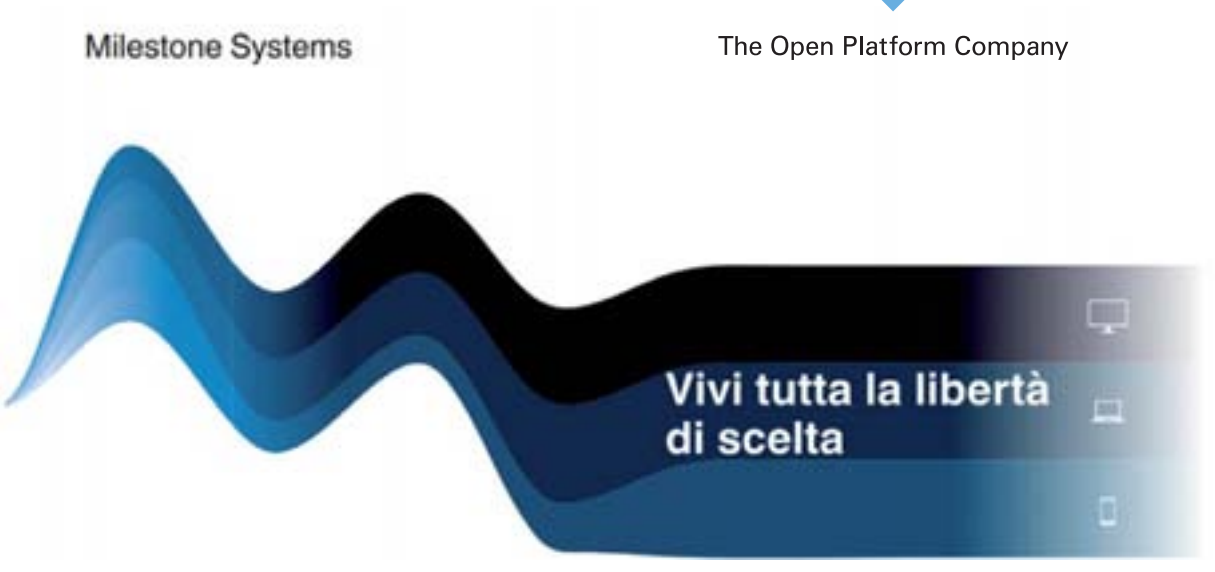
Altra grande novità per il 2014, tralasciando in questo frangente i la linea di nuovi prodotti che arriveranno con XProtect 2013, sarà MPOP Università,

che identifica l'evoluzione dell'evento MPOP e che porterà un segnale chiaro in tutta Italia: se da un lato siamo promotori dei valori Open Platform e dell'Eco Sistema, dall'altro dobbiamo dare voce ai giovani ricercatori: un'azienda come la nostra, sente il dovere di spronare la ricerca e metterla in evidenza. Sarà una vetrina internazionale per i giovani ricercatori, per gli sviluppatori di Appliance software e hardware, e per altri produttori che, come noi, condividono questa filosofia, ovviamente sempre vestita dall'originalità di esposizione del Marketing Team Milestone.

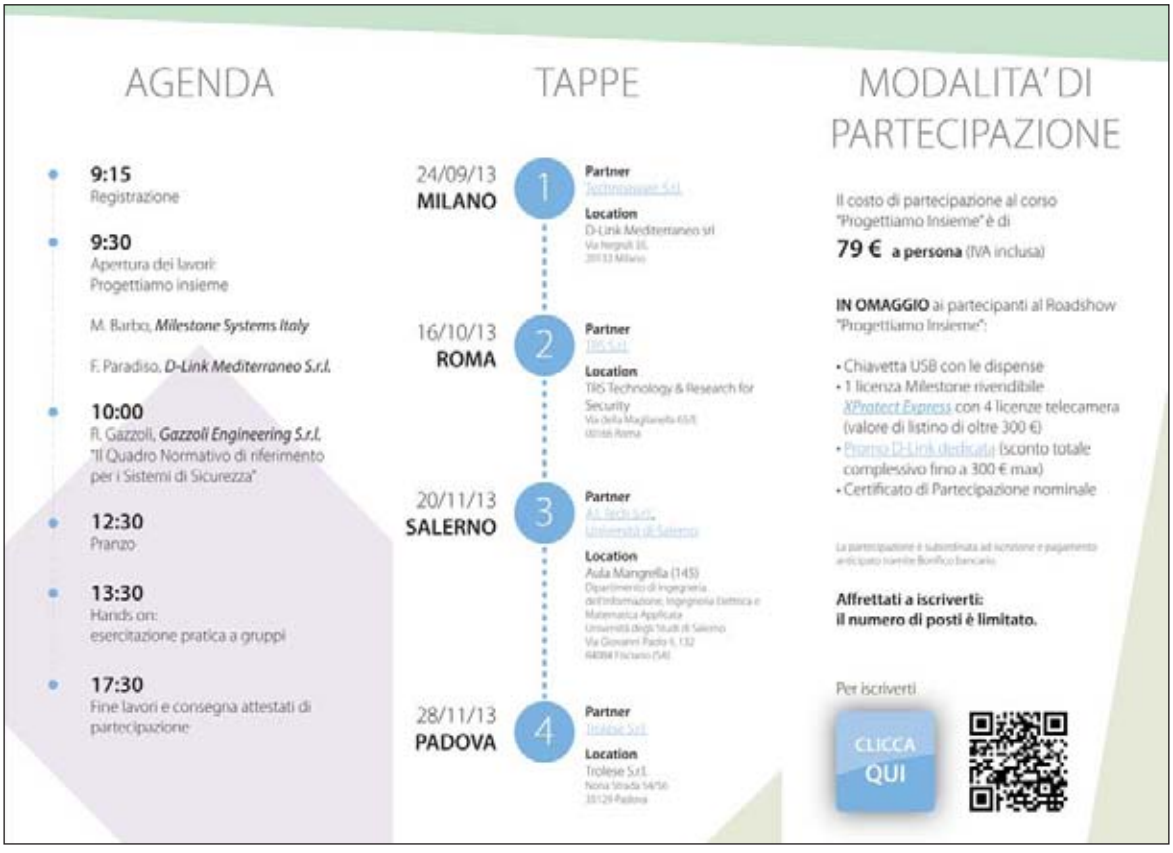
Nessuna area geografica verrà esclusa: intediamo arrivare nel tempo in tutte le regioni italiane, perché siamo convinti che ognuno di noi può, senza alcun problema, esprimere il meglio direttamente dalla propria terra e, di conseguenza, anche l'installatore, il progettista, e l'utente finale evoluto avranno a portata di mano ricerca, cultura, soluzioni, in un continuo e piacevole sharing & exchange made by Milestone.

Stiamo progettando di includere questi protagonisti anche in un contesto importante come SICUREZZA 2014, facendo così evolvere la stessa nostra presenza in qualcosa di molto più accattivante, per la Fiera stessa e i suoi visitatori.

Pensare ad un Ecosystem Village dove tutti possono pensare GRANDE… è un esplicito invito aperto a tutti!




ROADSHOW2013
D-Link
milestone
VIDEOSORVEGLIANZA:
PROGETTIAMO INSIEME
Un roadshow tecnico-formativo per aiutarti a progettare un sistema di Videosorveglianza su IP integrato e a norma di legge.
ORGANIZZATO DA
D-Link
milestone
24/09/13 | Milano
16/10/13 | Roma
20/11/13 | Salerno
28/11/13 | Padova
PARTNERS
AITech
TechnoAware
TROLESE
DISTRIBUIAMO SICUREZZA
TRS
PROGRAMMA
Le aziende sponsor e partner evidenzieranno, in una breve introduzione, le principali problematiche che gli installatori incontrano nella realizzazione di un impianto di sicurezza.
Seguirà la sessione tecnica tenuta dall'Ing. Gazzoli, che aiuterà a far chiarezza sulla normativa, a capire cosa sta cambiando nel mondo della Videosorveglianza e della Sicurezza: verranno illustrate le norme di riferimento da osservare nella progettazione, installazione e manutenzione ed esercizio dei Sistemi di Sicurezza, con particolare riferimento alle più recenti Norme CEI della famiglia EN 50132 relative ai Sistemi di Videosorveglianza ed ai principali obblighi per gli installatori derivanti dalla Normativa sulla Privacy.
La seconda parte sarà una sessione pratica "hands on" in cui ci focalizzeremo sulla configurazione e installazione di una soluzione D-Link-Milestone con l'integrazione dei plugin dei partner presenti. Divisi in gruppi, avrete modo di imparare a configurare correttamente un sistema di Videosorveglianza completo: videocamere, NVR, network di base, software di Management, sistemi Intelligenti di rilevamento targhe e conteggio persone.
Docente
Il corso è tenuto dall'Ing. Gazzoli, fondatore della Gazzoli Engineering S.r.l., società che si occupa di progettazione, formazione e consulenza nell'ambito della Security dal 2003.
A chi si rivolge
• Installatori di sicurezza
• System Integrator
• Progettisti
• Studi di consulenza


AGENDA
9:15
Registrazione
9:30
Apertura dei lavori:
Progettiamo insieme
M. Barbo, Milestone Systems Italy
F. Paradiso, D-Link Mediterraneo S.r.l.
10:00
R. Gazzoli, Gazzoli Engineering S.r.l.
"Il Quadro Normativo di riferimento per i Sistemi di Sicurezza"
12:30
Pranzo
13:30
Hands on:
esercitazione pratica a gruppi
17:30
Fine lavori e consegna attestati di partecipazione
TAPPE
24/09/13
MILANO
1
Partner
Technoaware S.r.l.
Location
D-Link Mediterraneo srl
Via Negroli 35,
20133 Milano
16/10/13
ROMA
2
Partner
TRS S.r.l.
Location
TRS Technology & Research for Security
Via della Magliarella 65/E
00166 Roma
20/11/13
SALERNO
3
Partner
A.I. Tech S.r.l.
Università di Salerno
Location
Aula Mangrella (145)
Dipartimento di Ingegneria dell'Informazione, Ingegneria Elettrica e Matematica Applicata
Università degli Studi di Salerno
Via Giovanni Paolo II, 132
84084 Fisciano (SA)
28/11/13
PADOVA
4
Partner
Trolese S.r.l.
Location
Trolese S.r.l.
Nona Strada 54/56
35129 Padova
MODALITA' DI PARTECIPAZIONE
Il costo di partecipazione al corso "Progettiamo Insieme" è di
79 € a persona (IVA inclusa)
IN OMAGGIO ai partecipanti al Roadshow "Progettiamo Insieme":
• Chiavetta USB con le dispense
• 1 licenza Milestone rivendibile XProtect Express con 4 licenze telecamera (valore di listino di oltre 300 €)
• Premio D-Link dedicati (sconto totale complessivo fino a 300 € max)
• Certificato di Partecipazione nominale
La partecipazione è subordinata ad iscrizione e pagamento anticipato tramite Bonifico bancario.
Affrettati a iscriverti:
il numero di posti è limitato.
Per iscriverti
CLICCA QUI

Infrastrutture critiche, il centro dell'attenzione

a colloquio con Sandro Bologna, presidente AIIC – Associazione Italiana esperti in Infrastrutture Critiche
a cura di Raffaello Juvara

"Infrastruttura critica" è un termine entrato nell'uso comune in tempi relativamente recenti e richiede una messa a fuoco per evitare confusioni. Quali sono dunque i termini di definizione di IC e quali i soggetti che aderiscono all'Associazione Italiana delle Infrastrutture Critiche - AIIC?

Gli eventi degli ultimi anni dimostrano la fragilità della nostra società, fortemente dipendente dalle infrastrutture tecnologiche, tra loro sempre più mutuamente dipendenti. Sviluppo, sicurezza e qualità della vita dipendono dal funzionamento continuo e coordinato delle "infrastrutture critiche": reti energetiche, reti di trasporto (aereo, navale, ferroviario, stradale), di telecomunicazione, informatiche, sanitarie, circuiti finanziari, di governo e per la gestione delle emergenze, infrastrutture sempre più complesse, interconnesse e dipendenti. Si sono così migliorate efficienza e qualità dei servizi contenendo i costi, ma inducendo nuove vulnerabilità, alla base di pericoli per lo sviluppo e il benessere quotidiano, non soltanto per inevitabili guasti di sottosistemi e componenti, ma per minacce legate ai fenomeni naturali e alla tormentata situazione geo-politica. Il pericolo è l'effetto domino, capace di paralizzare una nazione.

L'AIIC, associazione scientifica e tecnica senza fini di lucro, promuove e sostiene una cultura interdisciplinare per favorire nel Paese lo sviluppo di strategie, metodologie, tecnologie e una formazione capaci di gestire correttamente la sicurezza di tali infrastrutture per assicurarne la continuità operativa.

L'AIIC intende stimolare la conoscenza e la condivisione delle esperienze maturate nella protezione e sicurezza delle infrastrutture tecnologiche strategiche e favorire un approccio interdisciplinare, intersettoriale e scientifico.

AIIC svolge un'attività divulgativa con eventi tecnico-scientifici, studi e ricerche tematiche. Ne fanno parte centinaia di soci, tra cui accademici, studiosi, profes-

sionisti, esperti di enti pubblici e organismi privati attivi nelle diverse infrastrutture critiche che, mettendo a fattor comune le loro competenze, permettono la formazione di una specifica cultura e di una visione complessiva in grado di sostenere concretamente la gestione di questo complesso e delicato dominio.

Per parlare di sicurezza delle IC si deve ricorrere a tutte le declinazioni del termine: sicurezza verso atti dolosi (security) e sicurezza verso eventi accidentali e naturali (safety), IT security e physical security, sicurezza ambientale, resilienza e altre ancora. Quali sono le linee seguite da AIIC sul tema? Quali sono le principali normative di riferimento per la sicurezza delle IC, in ambito nazionale ed europeo?

L'approccio seguito da AIIC nell'affrontare il soggetto della protezione infrastrutture critiche è un approccio olistico che partendo da una accurata analisi di rischio, considerando tutte le possibili minacce, eventi accidentali, eventi naturali e atti dolosi, mira a stabilire delle "Best Practice", in linea con quanto stabilito dalla Direttiva Europea 2008/114/CE, recepita dall'Italia con il Dlgs n. 61, 11 Aprile 2011. Recentemente, tra tutte le possibili minacce, la minaccia cyber è salita alla ribalta dell'attenzione e conseguentemente la cybersicurezza è diventata un elemento fondamentale da considerare per la sostenibilità e lo sviluppo sociale ed economico di tutti i paesi del mondo, ma in particolare di quelli fortemente in-

dustrializzati come l'Italia. In Italia manca ancora un documento strategico nazionale in materia, o meglio una strategia di sicurezza nazionale che prenda in considerazione anche lo spazio cibernetico. Soltanto lo scorso 19 marzo 2013 è stato pubblicato nella GU n. 66 il Decreto nominato come "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". Purtroppo la governance definita da tale decreto è troppo frammentata e al momento - a quanto risulta - non ci sono tempi certi per la nascita del CERT, anche se dovrebbe essere entro il 2013 per rispettare le richieste dell'Unione europea. C'è la sensazione che l'organizzazione sia troppo articolata, di difficile comprensione e crei sovrastrutture poco efficienti.

Ma l'Europa chiede di accelerare. Il 7 febbraio la Commissione Europea e l'Alto Rappresentate per gli affari esteri e la politica di sicurezza, Catherine Ashton, hanno sottoposto al Consiglio e al Parlamento Europeo una Comunicazione congiunta su Strategia dell'Unione europea per la cybersicurezza. La Comunicazione parte dal presupposto che oggi la tecnologia dell'informazione e delle comunicazioni è diventata la spina dorsale della crescita economica e una risorsa critica da cui dipendono tutti i settori dell'economia europea. Purtroppo l'esperienza degli anni recenti dimostra che il mondo digitale, oltre a procurare enormi vantaggi, presenta anche numerose vulnerabilità, con un impatto diretto anche sull'attuazione dell'Agenda digitale, in quanto la sicurezza delle infrastrutture rappresenta la base imprescindibile su cui costruire una strategia digitale.

Gli incidenti a carico della cybersicurezza, intenzionali o fortuiti, che stanno crescendo a un ritmo allarmante, sono suscettibili di perturbare la fornitura di servizi essenziali che diamo per scontati, come la distribuzione idrica, le cure sanitarie, l'elettricità o i servizi mobili. Seguendo l'impostazione tracciata dall'Unione Europea, negli Stati Uniti il Presidente Obama ha deciso di ricorre a un Executive Order sulla cybersicurezza, emesso in data 12 febbraio 2013, per provare a proteggere al meglio le infrastrutture critiche nazionali dagli attacchi provenienti dallo spazio cibernetico.

Come la strategia europea, anche quella statunitense è basata su una precisa specificazione e assunzione dei ruoli e delle responsabilità di ciascun attore, sia privato sia governativo, chiamato a farvi fronte e sulla creazione di un clima di fiducia reciproca, tale da favorire la condivisione delle informazioni e la collaborazione tra pubblico e privato.

Da parte sua AIIC sta portando avanti una serie di attività di diffusione mirate a creare la consapevolezza del problema, nonché promuovere attività formative e di ricerca su alcuni aspetti specifici, quali la preparazione dei piani di sicurezza operatore, l'analisi delle vulnerabilità dei sistemi di controllo industriali, l'impatto sulla cybersicurezza delle nuove proposte di cloud computing. La storia ci insegna che la sicurezza assoluta non esiste. Dopo tanti fallimenti, più recentemente si è introdotto il concetto di resilienza. La resilienza nasce da un modo di porsi che rende capaci di convivere con i fallimenti e le sconfitte, mentre spinge a trovare e valorizzare tutte le risorse e potenzialità: tecnologiche, organizzative, economiche e sociali. Il concetto del "non è mai successo" è sostituito dalla visione del "se dovesse succedere", che non significa necessariamente il sovradimensionamento delle soluzioni, ma la predisposizione e la preparazione all'accadimento dell'evento.

Quali sono i presupposti della partecipazione di AIIC a CP EXPO e quali obiettivi si propone di raggiungere?

L'adozione di standard internazionali, procedure e Best Practice a sostegno della continuità operativa favorisce la resilienza promuovendo lo sviluppo e facilitando l'ingresso nei mercati anche da parte di piccole e medie imprese. A causa dell'interdipendenza dei si-

stemi, l'adozione di tali migliori pratiche nello sviluppo della protezione delle infrastrutture deve essere quanto più ampia possibile e condivisa in modo trasversale da tutti gli stakeholders dell'innovazione coinvolti. L'implementazione di nuove metodologie e tecnologie mirate a consolidare la sicurezza comporta inoltre opportunità di crescita nel mercato dei professionisti e dei prodotti della sicurezza alla condizione di adeguarne la preparazione e le competenze in base ai bisogni creati dalla situazione contingente. Il focus della manifestazione CPEXPO intende approfondire il tema della protezione delle comunità e dei cittadini, ponendo in risalto il corretto funzionamento delle infrastrutture critiche alla luce dei rischi di sistema derivanti dalla loro (parziale o totale) messa fuori uso da cause antropiche o naturali e le possibili soluzioni (nel campo della prevenzione e in quello della resilienza) per assicurare alle IC continuità di funzionamento. AIIC tramite gli studiosi della materia e gli esperti nelle diverse infrastrutture critiche, che costituiscono il cuore dell'Associazione, con il seminario "Procedure e Tecnologie per la Protezione delle Infrastrutture Critiche", calendarizzato per il giorno 30 Ottobre 2013, dalle ore 14:00 alle ore 18:00, si propone di condividere le esperienze e le conoscenze tecniche e procedurali di gestione di questi complessi domini nell'ambito di CPEXPO, supportando i fruitori e gli organizzatori della manifestazione fieristica genovese nel pieno completamento degli obiettivi di protezione delle comunità e delle infrastrutture di riferimento, stimolando e arricchendo il dibattito tra gli attori istituzionali in gioco e creando i presupposti per una partecipazione delle Piccole e Medie Imprese italiane a tutte le opportunità di business che ne possono derivare.

Infrastrutture Critiche, PSIM per il DLGS 61

a colloquio con Nils Fredrik Fazzini, Direttore Operations di Citel
a cura di Raffaello Juvara

Energia e Trasporti, i due settori classificati come ICE (Infrastrutture Critiche Europee - vedi box), hanno una rilevanza analoga nell'attuale società civile dei nostri tempi. Ma sono contesti molto diversi se confrontati sul piano dei rischi in chiave di sicurezza fisica e delle misure per fronteggiarli; basti pensare che nel caso dell'energia (non nucleare) i rischi si traducono prevalentemente in perdite economiche, mentre nel caso dei trasporti i rischi di perdite di vite umane sono quelli maggiormente temuti e meno fronteggiabili.
In vista del Convegno CPEXPO di Genova, con questo articolo cerchiamo di approfondire le possibilità di penetrazione delle piattaforme PSIM (Physical Security Information Management) nell'ambito delle IC italiane, alla luce degli obblighi imposti dalla legislazione espressamente emanata. Lo facciamo rivolgendo le nostre domande al Nils Fredrik Fazzini, Direttore Operations di Citel Spa, società milanese con una posizione indiscussa di leadership nel mercato nazionale delle piattaforme di tipo PSIM in architettura aperta multifornitore.

Il tema della sicurezza fisica delle IC è sempre stato attuale, anche se oggi a fare notizia sono le minacce di hackers che si dicono in grado di bloccare intere infrastrutture di produzione e distribuzione in campo energetico senza doversi preoccupare di violare protezioni fisiche. Restando invece nel campo della protezione fisica delle IC, avete potuto rilevare una evoluzione dell'utenza interpretabile come uno spostamento dalle soluzioni tradizionali a quelle di tipo PSIM?
Senza alcun dubbio lo spostamento è in corso per una serie di fattori concomitanti. Uno è l'evoluzione tecnica favorita dalla digitalizzazione della società. Un secondo fattore è la maturazione dell'utenza anche in base all'esperienza: consideri che le IC sono state nel passato tra le prime a sentire l'esigenza di adottare piattaforme di supervisione della sicurezza fisica che andavano per la maggiore tra i grandi utenti. I sistemi di supervisione di allora hanno mostrato negli anni limiti di rigidità funzionale e di chiusura architetturale sempre più inadatti all'evoluzione delle esigenze dell'utenza, con il risultato di aprire la strada – anche per reazione – alle soluzioni gestionali di tipo PSIM nell'accezione Frost & Sullivan che, ricordo, si basa su 6 requisiti funzionali non riconducibili a un supervisore di trattamento degli allarmi ma a un sistema informatico sui generis (vedi box e riferimento all'articolo sul numero 01-2013 di Essecome).

Si tratta di vostre ipotesi da osservatori esterni o queste tendenze vi hanno direttamente coinvolto?

LE INFRASTRUTTURE CRITICHE INDIVIDUATE DAL DLGS 61

Rispetto all'accezione generica "infrastrutture critiche", che riguarda qualsiasi infrastruttura che fornisca un qualsiasi servizio la cui interruzione possa avere effetti deleteri per la comunità, il termine PSIM qui viene riferito a quelle IC individuate dal DLGS 61 del 2011 che recepisce la Direttiva Europea 114 del 2008 e che ispira il Convegno CPEXPO, prima rassegna internazionale sulle innovazioni e le soluzioni integrate per la protezione delle comunità e delle infrastrutture critiche. Più precisamente si tratta dei cosiddetti settori ECI (European Critical Infrastructures), "ICE" per il DLGS 61, che trascriviamo così come sono riportati nel DLGS:

Settore I. ENERGIA

- Elettricità - Infrastrutture e impianti per la produzione e la trasmissione di energia elettrica per la fornitura di elettricità
- Petrolio - Produzione, raffinazione, trattamento, stoccaggio e trasporto di petrolio attraverso oleodotti
- Gas - Produzione, raffinazione, trattamento, stoccaggio e trasporto di gas attraverso oleodotti - Terminali GNL

Settore II. TRASPORTI

- Trasporto stradale
- Trasporto ferroviario
- Trasporto aereo
- Vie di navigazione interna
- Trasporto oceanico, trasporto marittimo a corto raggio e porti

Ci hanno coinvolto in pieno, direi: le attività di sviluppo tecnico e i ricavi di Citel negli ultimi anni hanno visto crescere a vista d'occhio la componente non bancaria, grazie alla progressiva sterzata verso i PSIM da parte di grandi imprese italiane, in particolare nel settore dell'energia che, guarda caso, insieme ai trasporti è un "settore ICE" ovvero Infrastrutture Critiche Europee. Pertanto enti e imprese che dispongono di simili infrastrutture ricadono nell'applicazione delle norme contenute nel Decreto Legislativo n. 61 del 2011 che, a sua volta, è concepito per attuare la Direttiva 114 del 2008 emanata dalla Comunità Europea.

Suppongo che la normativa che si applica alle ICE non contempli espressamente il concetto di PSIM; in che modo quindi le IC italiane classificabili ICE si orientano verso uno PSIM?

Semplificando, il DL61 prevede che le infrastrutture individuate dalla Pubblica Amministrazione come critiche per l'interesse pubblico siano soggette a degli adempimenti per la protezione dai rischi e per la gestione delle emergenze, coinvolgendo organi pubblici e l'operatore/proprietario dell'infrastruttura sul terreno delle misure, della gestione, della pianificazione della sicurezza. Tra i "Requisiti minimi del piano di sicurezza dell'operatore (PSO)" sono riportati, letteralmente:

….

- sistemi di protezione fisica (strumenti di rilevazione, controllo accessi, protezione elementi e di prevenzione);
- predisposizioni organizzative per allertamento comprese le procedure di gestione delle crisi;
- sistemi di controllo e verifica;
- sistemi di comunicazione;
- addestramento e accrescimento della consapevolezza del personale;
- sistemi per la continuità del funzionamento dei supporti informatici.

….

A parte la prima voce, scontata e generica, le altre potrebbero anche essere interpretate e attuate in senso tradizionale ma, considerata la delicatezza dell'ambito e le responsabilità connesse, non ho dubbi sul fatto che contribuiscano a spingere i gestori delle ICE verso soluzioni (e non più solo prodotti) coincidenti con un sistema informatico per la sicurezza fisica, ovvero uno PSIM.

Ricordiamo gli elementi qualificanti di un PSIM secondo Frost & Sullivan per analizzarli rispetto ai requisiti del PSO:

1. **interazione con il campo su base locale e territoriale: il software di gestione indipendente deve raccogliere i dati provenienti da un numero qualsiasi di dispositivi di sicurezza o di sistemi diversi; deve inoltre interagire con essi per azionamenti locali, feedback etc. in modo da limitare al minimo l'intervento umano sul posto;**
2. **analisi: il sistema analizza e correla i dati relativi a eventi e allarmi, per identificare le situazioni reali e la loro priorità;**
3. **verifica: il software PSIM presenta le informazioni relative alle diverse situazioni in un formato rapido e facilmente comprensibile per l'operatore, per agevolare la verifica della situazione;**
4. **risoluzione: il sistema deve fornire le procedure operative standard (SOP), con istruzioni "passo dopo passo" basate sulle best practice e sulla policy dell'organizzazione, assieme agli strumenti per risolvere la situazione;**
5. **tracciabilità: il software PSIM tiene traccia di tutte le informazioni e di tutte le operazioni ne-**

cessarie per redigere i report di conformità e, se necessario, consentire gli approfondimenti investigativi;

6. **controllo: i software PSIM controlla anche come ogni operatore interagisce con il sistema, tenendo traccia di eventuali modifiche manuali ai sistemi di sicurezza, delle anomalie di gestione nel sito allarmato e il computo dei tempi di reazione per ogni evento.**

Quale rapporto c'è tra le prescrizioni del PSO rispetto ai requisiti del PSIM?
Ovviamente non va cercata la coincidenza letterale tra i punti del PSO e quelli del PSIM, trattandosi di un "piano" in un caso e di un "sistema informatico" nell'altro; ma non occorre essere dei tecnici per comprendere come un PSIM possa essere decisivo nella gestione organica e responsabile di un PSO per una infrastruttura critica e, a maggior ragione, per un insieme di infrastrutture critiche gestite allo stesso operatore. Senza contare che uno PSIM permette anche il coinvolgimento di società di security evitando l'impiego 24 ore su 24 di personale del gestore, proprio in virtù del fatto che lo PSIM prevede procedure obbligate "passo dopo passo", strettamente contestualizzate, interamente tracciate e tali da poterne "scalare" in corsa la gestione a un livello di responsabilità superiore per un situation management a rischio di criticità.

Siamo quindi arrivati al punto che i requisiti di un sistema moderno per la gestione della sicurezza fisica sono impliciti in una norma di legge?
È piuttosto un caso di convergenza di orientamenti che hanno implicazioni tendenziali più ampie per il mercato della sicurezza fisica. Noi di Citel siamo i primi a esserne gratificati visto che abbiamo dovuto fare la fatica del battistrada dello PSIM per quasi 20 anni. Ma la gratificazione maggiore è stata quella di essere stati scelti dai principali operatori del settore energetico nazionale secondo una selezione esclusivamente naturale e meritocratica, basata sulla specializzazione, sulle referenze, sulla reputazione di qualità e flessibilità maturate nel tempo.

Quali sono gli sviluppi evolutivi del vostro PSIM "Centrax" che potranno essere apprezzati in modo specifico dagli operatori di IC?
Fino a oggi, a parte procedure, gestione tracciata, cruscotti grafici, l'apprezzamento convinto dell'uten-

za IC è andato all'apertura architetturale. Non come semplice dichiarazione di disponibilità: non costa nulla dichiararsi disponibile. Molto più impegnativo, costoso e rischioso, far seguire alla disponibilità l'attività di un laboratorio hardware e software in grado di integrare funzionalmente via protocollo qualsiasi altro sottosistema e dispositivo di vari produttori, anche in capo al mondo, anche concorrenti. Mi riferisco in particolare – per restare nel capo dei progetti per il settore energetico – al controllo accessi con Axess, alle centrali di allarme di Honeywell, a quelle antincendio Notifier, ai sistemi di videosorveglianza IP con i VMS di Avigilon e Genetech, con telecamere termiche SightLogix, con cui abbiamo messo a punto su PSIM anche la gestione delle coordinate geografiche di ogni singolo pixel. Potrei citarne altri operatori ma dovrei essere autorizzato preventivamente.

Altra caratteristica architetturale della nostra piattaforma che si sta confermando decisiva in questo mercato è la possibilità di per i nostri correlatori nel sito di comunicare con più di un PSIM in relazione a fattori riconducibili a defaillance o ritardi nella gestione degli eventi, al tipo di evento, a problemi di comunicazione, etc. Quanto ai prossimi sviluppi, quelli ormai certi sono una derivazione delle applicazioni bancarie più recenti (il settore bancario è per noi una fonte continua di idee innovative, di investimenti e, fortunatamente, di ritorni). Il campo applicativo è quello della multimedialità dell'interazione tra control room e sito remoto, in altre parole l'integrazione bidirezionale di video, fonia e azionamenti over-IP nei due sensi, con la tendenza a ottenere funzionalità che configurano una presenza nel sito remoto che non è più una persona fisica ma un addetto virtuale generato dall'operatore in control room.

Le banche hanno aperto la strada da diversi anni in tale direzione, con la guardia remota associata alla videosorveglianza intelligente. Il passo ulteriore, in fase di messa a punto, è quello di funzioni PSIM di tipo tele-portierato/tele-accoglienza over-IP per quei casi in cui il video-citofono over-IP, per quanto integrabile nel nostro Centrax, non è sufficiente.

WISE
WARSAW

BE WISE.
BE SECURED.

Varsavia, Esposizione Internazionale sulla sicurezza e protezione

INCONTRIAMOCI

Moduli di iscrizione ed informazioni dettagliate
si possono trovare sul sito: **wise-warsaw.pl**

19 - 21 Novembre 2013

EXPO XXI Varsavia, Polonia

WISE: LA MANIFESTAZIONE INTERNAZIONALE DEI SETTORI SECURITY E ANTINCENDIO.

UN'OPPORTUNITÀ UNICA PER CONOSCERE I PRODOTTI PIÙ INNOVATIVI: SISTEMI DI IDENTIFICAZIONE, TECNOLOGIE ANTINTRUSIONE, CONTROLLO ACCESSI, ANTINCENDIO.

WISE 2013 RAPPRESENTA UNA FANTASTICA OCCASIONE DI INCONTRO E DI SCAMBIO PER TUTTI GLI OPERATORI DEL SETTORE

Organizzatori:

Nasce l'Osservatorio di Eurispes sulla Sicurezza

a cura della Redazione

Negli ultimi trenta anni la sensibilità ai temi della sicurezza delle infrastrutture "informatiche" – ovvero del complesso, fisico e logico, di tecnologie HW, reti, applicazioni, sistemi, basi dati – è andata sviluppandosi con velocità e obiettivi diversi. E con essa è prima cresciuto, e successivamente esploso, come dimostrano i dati sul giro d'affari generato a livello mondiale, anche un business della security, in un rapporto di causa ed effetto con la sensibilizzazione delle imprese e delle Istituzioni, non sempre razionale e non sempre facilmente interpretabile.

L'Osservatorio sulle Tecnologie per la Sicurezza opererà raccogliendo la collaborazione di stakeholder istituzionali e coinvolgerà, nel contempo, le principali aziende del settore operanti sul mercato civile e militare, le aziende clienti, le Università e i laboratori di ricerca. L'intento è quello di sviluppare un dibattito allargato e multidisciplinare sui differenti aspetti della sicurezza IT, di formulare per i diversi scenari di crisi ipotizzati modelli di intervento organizzativi, normativi e tecnici. L'Osservatorio, attraverso la propria attività di ricerca, di raccolta e di riorganizzazione della conoscenza, potrà in ultima analisi mettere a disposizione del Legislatore nazionale e delle Authority letture integrate dei fenomeni evolutivi dei processi di gestione della informazione e comunicazione, contribuendo così alla realizzazione di un ancor più consapevole processo di produzione normativa e regolatoria.

L'attività dell'Osservatorio, che si avvale anche della collaborazione del Ce.S.I., per gli aspetti di sicurezza internazionale, sarà strettamente legata alla 1° Rassegna internazionale sulle innovazioni e le soluzioni integrate per la protezione delle comunità e delle infrastrutture critiche. Un evento che nasce nell'ambito del progetto CPEXPO-Community Protection e che si svolgerà il 29-30-31 ottobre prossimi a Genova presso la Fiera Internazionale.

CPEXPO è una piattaforma di comunicazione interattiva, che consiste in una manifestazione fieristica internazionale affiancata e supportata da un portale web permanente, i cui obiettivi, saldamente connessi tra loro, sono quelli di stimolare il dibattito e far convergere su Genova l'attenzione internazionale di istituzioni, aziende, università, mondo della ricerca, paesi esteri, decision maker, responsabili di IC, media di settore e, più in generale, professionisti ed esperti della filiera di riferimento. Proprio Genova è una città che di per sé è uno straordinario prototipo di IC (altissima concentrazione in area urbana di aeroporto, terminal passeggeri, terminal VTE) e può contare su un tessuto produttivo all'avanguardia e di aree di eccellenza nel campo dell'università e della ricerca, segnatamente al settore delle tecnologie per la community protection.

In questo quadro, l'Osservatorio sulle Tecnologie per la Sicurezza è il luogo di analisi e di confronto tra studiosi e, insieme, di approfondimento delle tematiche riguardanti il settore delle IT e della sicurezza, mentre l'Expo sulla Sicurezza di Genova sarà il luogo dove si incontreranno e dialogheranno le Istituzioni e le aziende.

a colloquio con Gian Maria Fara, Presidente Istituto Eurispes

Considerando l'ampiezza del tema "sicurezza", quali sono gli ambiti specifici che prenderà in esame l'Osservatorio permanente costituito da Eurispes insieme a CESI e a CP EXPO?

Il tema della sicurezza, generalmente inteso, è molto ampio e si presta a letture e interpretazioni che spaziano e attraversano campi di intervento diversi e spesso distanti. Il nostro Osservatorio nasce con l'obiettivo specifico di studiare e monitorare l'evoluzione delle tecnologie per la sicurezza delle cosiddette infrastrutture critiche. E ciò interessa evidentemente fronti tra loro diversi e soltanto apparentemente distanti: dalle problematiche legate alla salvaguardia e alla tutela dell'ambiente alle infrastrutture, dalle reti di comunicazione ai sistemi di controllo e protezione della sicurezza dei cittadini nel loro vivere quotidiano. Il concetto di sicurezza, infine, per potersi esprimere in tutta la sua valenza, deve potersi tradurre in prevenzione, ovvero nella capacità di anticipare e neutralizzare i fattori di crisi e le possibili emergenze. Prevenire significa prendere le precauzioni necessarie perché qualcosa non avvenga e anche prevedere un insieme di azioni attraverso le quali orientare i processi e volgerli verso gli esiti desiderati.

Quali saranno i criteri di individuazione/selezione delle fonti?

L'Eurispes ha sempre avuto come metodologia l'approccio interdisciplinare allo studio e all'analisi dei problemi e, insieme, la convinzione che la complessità non accetti semplificazioni. La complessità richiede spiegazioni complesse. Nello stesso tempo l'Eurispes si è sempre nutrito della "cultura del dubbio". Il che, tradotto in termini, sta a significare che non esistono verità rivelate dalle quali partire e da difendere. Ogni fonte è degna di attenzione e di approfondimento e quindi può essere utilizzata. L'essenziale è che la fonte, quale che ne sia la matrice, possa essere verificata nella qualità dei dati e nelle informazioni che produce. Quindi massima apertura, ma anche grande attenzione, grande cautela e verifiche approfondite sulla qualità.

Come verrà presa in considerazione la sicurezza fisica sempre più integrata con quella informatica nell'ambito particolare delle infrastrutture critiche?

È chiaro che al centro di ogni azione, di ogni politica della sicurezza, debba esserci l'uomo, la sua libertà di movimento, di organizzazione e di espressione. Le nuove tecnologie rappresentano, insieme, , un fattore di crescita e nuove opportunità e vantaggi in direzione del miglioramento della qualità della vita delle persone. E questo vale sia che si parli della sicurezza e riservatezza delle comunicazione dei singoli cittadini sia che si parli della protezione delle infrastrutture critiche, che costituiscono i luoghi nei quali e attraverso i quali il vivere sociale si esprime e si organizza.

Naturalmente ciascuno di noi potrà mettere in atto strategie, più o meno raffinate, di prevenzione nella organizzazione della propria vita quotidiana, nella gestione della attività economica e di quella professionale, nella conduzione dei rapporti sociali. Tuttavia, per quanto accorta e prudente possa essere la nostra condotta, per quanto si cerchi di prevenire e di pianificare, l'esercizio di tale virtù, praticato a livello soggettivo, da solo non potrà mai essere sufficiente. Insomma, la nostra volontà e il nostro impegno privati possono avere un senso solo se sono parte di una strategia più ampia che per essere efficace e condivisa deve essere pubblica, cioè esercitata dalle Istituzioni.

EURISPES

a colloquio con Andrea Margelletti, presidente Ce.S.I. - Centro Studi Internazionali

Quali saranno gli ambiti specifici che Ce.S.I. seguirà nell'attività dell'Osservatorio permanente costituito da Eurispes assieme a Ce.S.I. e a CPEXPO?
Il Ce.S.I. – Centro Studi Internazionali — è un think tank che si occupa di Relazioni Internazionali e Difesa, pertanto il contributo all'Osservatorio si concentrerà su queste tematiche. In particolare, sarà posta grande attenzione alle prospettive internazionali di cybersecurity e cyberdefence, agli scenari ipotizzabili e ai nuovi trend in materia di utilizzo offensivo delle capacità cibernetiche.

Quali saranno i criteri di individuazione/selezione delle fonti?
I criteri di individuazione/selezione delle fonti saranno quelli tradizionali dell'Istituto basati su obiettività e trasparenza, affiancati però dal tratto distintivo del Ce.S.I. che fornisce trend e prospettive secondo uno schema diverso rispetto al classico approccio accademico. Il nostro modo di operare, infatti, si basa sull'esperienza diretta dei luoghi e il contatto con gli interlocutori internazionali sia statuali che non, circostanza questa che consente di generare analisi e report di taglio agile e operativo che spesso affrontano tematiche "poco frequentate" dai mezzi di informazione mainstream.

Come verrà monitorata la componente della sicurezza fisica sempre più integrata con quella informatica, in particolare per la protezione delle infrastrutture critiche in ambito civile?
Questo aspetto attualmente esula dalla sfera d'interesse del Ce.S.I. e sarà sicuramente monitorato nell'ambito del Comitato Scientifico dagli autorevoli esperti e "addetti ai lavori" che ne fanno parte.

Ce.S.I.
Centro Studi Internazionali

a colloquio con Paola Girdinio, presidente del comitato scientifico internazionale di CPEXPO e Giorgio Da Bormida, membro del comitato esecutivo di CPEXPO

Quali sono gli scopi della partecipazione di CPEXPO all'Osservatorio permanente su IT e Sicurezza costituito assieme a Eurispes e CE.S.I.?
CPEXPO partecipa all'Osservatorio permanente su IT e sicurezza, costituito assieme a Eurispes e CE.S.I., perché rappresenta un contesto neutrale privilegiato per contribuire ad acquisire dati su un settore divenuto ormai strategico e primario per le imprese e per il paese. All'Osservatorio, infatti, aderiscono e collaborano le istituzioni, le imprese e le associazioni che operano nell'ambito della sicurezza delle infrastrutture critiche.
L'Osservatorio potrà beneficiare delle attività di CPEXPO non soltanto come fonte di informazioni sulle innovazioni e le soluzioni integrate per la protezione delle comunità e delle infrastrutture critiche, ma anche come palcoscenico in cui presentare i propri risultati a un pubblico nazionale e internazionale.
Fin dalla prima edizione saranno infatti presenti a CPEXPO numerose delegazioni internazionali, che avranno l'opportunità di confrontarsi con l'industria italiana specializzata in tecnologie per la realizzazione di sistemi integrati e di soluzioni per la sicurezza delle Infrastrutture critiche.
Una piattaforma indipendente come l'Osservatorio appena costituito permette di garantire valutazioni indipendenti, studi oggettivi e di dare visibilità a una pluralità di contributi e di esperienze.

L'Expo che si terrà a Genova dal 29 al 31 ottobre sarà quindi un primo momento di un più ampio progetto, rivolto alla comunità internazionale delle infrastrutture critiche, ma anche a Genova e alle sue istituzioni. Quale sarà in particolare il ruolo dell'Università in questo progetto?
CPEXPO, come prima rassegna internazionale sulle innovazioni e le soluzioni integrate per la protezione delle comunità e delle infrastrutture critiche, affronterà una grande varietà di temi legati alla Sicurezza, con particolare riguardo ai settori Logistic & Transports, Cybersecurity e Sistemi informativi, Environment, Utilities, Bank & Finance, Health, Smart Cities. L'Expo sulla Sicurezza sarà un appuntamento permanente, con l'obiettivo di mettere a sistema un settore economico in costante espansione, capire la sua evoluzione e fornire una visione integrata sul futuro, sui rischi emergenti e sulle possibili soluzioni. Per un progetto di questa portata risulta di assoluta importanza condividere e divulgare la conoscenza delle tecnologie di avanguardia in tutti i contesti di interesse, che, data la grande molteplicità dei settori prima citati, coprono di fatto tutto lo spettro delle moderne tecnologie.
Un ruolo primario dell'università in questo progetto sarà mettere a disposizione di CPEXPO la propria attività di ricerca e innovazione in tutti i campi di

GIORGIO DA BORMIDA

Ha oltre 20 anni di esperienza nell'europrogettazione e nella gestione e sviluppo del business internazionale in innovazione e tecnologia.
Dopo aver prestato servizio come Business Development Manager in ricerca e innovazione per il terzo più grande editore italiano, Da Bormida ha fondato l'azienda italiana di consulenza ELGI, basata sulla sua vasta rete di contatti e specializzata nella consulenza in materia di sviluppo dell'innovazione basata sulla conoscenza e la valorizzazione, attraverso la partecipazione a grandi progetti internazionali.
ELGI annovera tra i suoi clienti aziende di grandi dimensioni (per esempio Hewlett-Packard, De Agostini, Vivisol), università ed enti locali (comuni, regioni) e centrali (ministeri) e le pubbliche amministrazioni in Italia, in Europa e all'estero.
Da Bormida ha vinto numerosi progetti europei finanziati in diversi programmi e concepiti in base alle strategie dei clienti. Da Bormida è un esperto della Commissione Europea sulla selezione delle migliori proposte di progetti da finanziare. Da Bormida è autore di articoli e relazioni in conferenze internazionali.

interesse, garantendo l'accesso ai più recenti sviluppi dello stato dell'arte. Genova, per la sua collocazione geografica e per il suo ruolo portuale e logistico, costituisce in molti contesti essa stessa una struttura critica, e l'università ha di conseguenza maturato una rilevante esperienza in molti dei settori interessati.

L'ecosistema industriale genovese, con il quale l'università ha da tempo stretto rapporti per la ricerca e l'innovazione, ha inoltre molte e qualificate competenze in numerosi contesti del settore, e ha stimolato l'università a sviluppare una rete di contatti scientifici di alto livello internazionale, che verranno messi a disposizione di CPEXPO e costituiranno un ulteriore importante ruolo di supporto all'iniziativa.

Come si svilupperanno l'attività scientifica e la divulgazione tra un Expo e l'altro?

L'attività scientifica e la divulgazione tra un'edizione di CPEXPO e l'altra saranno sviluppate e garantite grazie alla comunità online ("community of practice") che trova la sua base naturale nel portale di CPEXPO, in costante aggiornamento ed evoluzione. È importante sottolineare, infatti, che CPEXPO è un progetto triennale che mira ad avviare una piattaforma interattiva permanente per la sicurezza e sostenibilità delle infrastrutture critiche e delle comunità. Una delle attività principali di CPEXPO è l'evento annuale che si articola in una conferenza internazionale di alto livello, una serie di workshop specializzati e un grande expo interattivo.Tuttavia CPEXPO ha obiettivi ben più ambiziosi, tra cui:

- raccogliere e presentare in un unico contesto le migliori tecnologie per favorirne il confronto e l'acquisto;
- coinvolgere i maggiori esperti del settore per dibattere sullo stato dell'arte, l'innovazione e le esperienze più significative mondiali;
- facilitare l'incontro tra imprese interessate a sviluppare business internazionale;
- creare un ponte tra i fabbisogni, la necessità di prevenire le crisi e le soluzioni;
- fornire soluzioni integrate e rafforzate da un insieme di servizi che si estendono oltre l'evento stesso.

In questo contesto è chiaro quindi come l'evento annuale assuma un ruolo di "milestone" del percorso di crescita, un momento in cui presentare i propri risultati a un pubblico selezionato e con interessi specifici.

Inoltre la comunicazione e continuità di azione è garantita anche dalla partecipazione all'Osservatorio permanente su IT e Sicurezza, costituito assieme a Eurispes e CE.S.I. L'Osservatorio per CPEXPO ha un valore altamente strategico perché non soltanto ne "istituzionalizza" le attività rendendole ancor più indipendenti dal singolo evento, ma anche perché permette di raggiungere un pubblico più ampio assicurando una pluralità di contributi e esperienze.

Chiaramente tra un expo e l'altro prevediamo di organizzare numerose attività di collegamento come, per esempio:

- seminari di approfondimento su temi specifici, tecnologie emergenti o scenari interessanti;
- giornate di formazione specialistiche;
- roadmap di eventi di comunicazione e relationship-building internationale grazie alle reti che hanno firmato accordi con CPEXPO, come Commonwealth Telecomunication Organization, AFCEA, ASREN, BIZON, EURISPES…;
- partecipazione a eventi e iniziative su invito di delegazioni estere, istituzioni e enti.

Tutto questo è già in lavorazione e gli sponsor, o meglio partner, di CPEXPO hanno scelto di entrare in questo ecosistema proprio considerando la sua natura olistica, ben diversa da un singolo evento fieristico.

Gli eventi di CPEXPO

(aggiornamento al 31 agosto)

29 OTTOBRE

WORKSHOP

Tuesday, 29th October - 14:00 - 16:00
Room D
Interdipendenze

Tuesday, 29th October - 14:00 - 16:00
Room C
Trasporti e Logistica

Tuesday, 29th October - 14:00 - 16:00
Room H
Business Continuity nuovi standard

Tuesday, 29th October - 14:00 - 16:00
Room I
Up-stream e down-stream, il punto su security e safety nelle due dimensioni dell'Oil & Gas

Tuesday, 29th October - 14:00 - 16:00
Room H

Tuesday, 29th October - 14:00 - 16:00
Room F

Tuesday, 29th October - 14:00 - 18:00
A Multidisciplinary outlook to Resilient Critical infrastructures

Tuesday, 29th October - 14:00 - 18:00
Room B
Sicurezza Trasporti Marittimi

Tuesday, 29th October - 16:00 - 18:00
Room I
PSIM, la nuova frontiera della sicurezza fisica.

Tuesday, 29th October - 16:00 - 18:00
Room E

Tuesday, 29th October - 16:00 - 18:00
Room D

Tuesday, 29th October - 16:00 - 18:00
Room E

Tuesday, 29th October - 16:00 - 18:00
Room F

Tuesday, 29th October - 16:00 - 18:00
Room H
Infrastrutture e reti di sottosuolo

30 OTTOBRE

WORKSHOP

Wednesday, 30th October - 14:00 - 16:00
Room D
Enviroment Risk Management

Wednesday, 30th October - 14:00 - 16:00
Room A
Cyber security

Wednesday, 30th October - 14:00 - 16:00
Room F
S3: Secure, Safe, Smart City

Wednesday, 30th October - 14:00 - 16:00
Room B
From Video Analytics to Social-Physical Security

WORKSHOP

30 OTTOBRE

Wednesday, 30th October - 14:00 - 16:00
Room C
Vulnerability Identification and Defence in Utilities

Wednesday, 30th October - 14:00 - 16:00
Room H
Il ruolo delle telecomunicazioni in caso di emergenza

Wednesday, 30th October - 14:00 - 16:00
Room H

Wednesday, 30th October - 14:00 - 18:00
Room K
Procedure e Tecnologie per la Protezione delle Infrastrutture Critiche

Wednesday, 30th October - 14:00 - 18:00
Room I
Security for Retail Forum

Wednesday, 30th October - 16:00 - 18:00
Room H
Progetti Europei sulle infrastrutture critiche già finanziati

RELATORI PRINCIPALI

29 OTTOBRE · ORE 10

Mario Mauro
Minister of Defence, Republic of Italy

Giuseppe Abbamonte
head of unit, trust and security, DG CNECT, European Commission

Neil Thompson
Former director of Geospatial Intelligence at Canadian Forces (Canada)

Lasantha De Alwis
Corporate Secretary, Commonwealth Telecommunication Organisation (UK)

Oliver Salvi
Secretary General of ETPIS
General Manager of EU-VRi

Kevin Wallinger
Managing Director Global Risk Reduction Inc.

Lorenzo Fiori
Senior Vice President Strategy Finmeccanica

Umberto Saccone
Security Director, ENI Corporate (Italy)

Bernardo De Bernardinis
Deputy Head of Italian Civil Protection and President of ISPRA (Italy)

RELATORI PRINCIPALI

30 OTTOBRE · ORE 10

RELATORI PRINCIPALI

31 OTTOBRE · ORE 10

CPEXPO COMMUNITY PROTECTION

SECPROTEC EAST AFRICA

SECURITY | PROTECTION | TECHNOLOGY

East and Central Africa's LEADING TRADE FAIR for the Security and Protection Industry

"Security Technology is key in East Africa, especially in Kenya. KSIA members consist of 100,000 guards throughout Kenya and do have other offices / branches in other East and Central African countries. KSIA members look forward to welcoming international partners to SecProTec East Africa."

MR JOHN THUO, ADVISOR KSIA
(KENYA SECURITY INDUSTRY ASSOCIATION)

SecProTec East Africa Summit: International Conference Program

- Fire Safety – International Standards and Regulations
- Aviation Security
- Security Research
- Multisensory Applications / Crowd and Traffic Control Systems
- ICT Protection
- Identification Technology
- Personal and Property Protection
- Oil and Gas Security
- Cross Border counterfeit (products)

25th – 27th SEPTEMBER 2013
KICC, NAIROBI, KENYA

www.secproteceastafrica.com

REPUBLIC OF KENYA
MINISTRY OF TRADE

KenInvest

KSIA
"taking care"

epc

ORGANIZER:
planetfair

TF EA

Ermes Elettronica a CPEXPO per la sicurezza delle comunità

a colloquio con Filippo Gambino, CEO di Ermes Elettronica
a cura di Cristina Isabella Carminati

Quali sono le realizzazioni che ERMES ELETTRONICA presenterà a CP EXPO, rivolte alla sicurezza delle comunità?

ERMES ELETTRONICA è specializzata nella realizzazione di sistemi di comunicazione audio e audio/video over IP con apparati stand alone collegati direttamente alla LAN e che utilizzano un protocollo di comunicazione Peer-To-Peer.

Questi sistemi non necessitano per il loro funzionamento di server o elementi centrali di gestione di nessun tipo in quanto gli apparati gestiscono direttamente e autonomamente sia le chiamate sia lo scambio di audio e video sotto forma di dati. Con questa tecnologia si realizzano sistemi di citofonia, interfonia, diffusione annunci (public address), chiamate di emergenza (SOS) che, grazie al protocollo comune, possono essere integrati in un unico sistema di gestione delle comunicazioni di sicurezza.

In particolare a CP EXPO vogliamo illustrare come l'applicazione di queste tecniche in ambito ferroviario ha contribuito ad aumentare in maniera significativa il livello di sicurezza dell'infrastruttura fornendo, allo stesso tempo, nuovi servizi ai passeggeri. Il caso concreto è quello di FERROVIENORD sulla cui rete ferroviaria sono state installate diverse tipologie di sistemi:

- un sistema di tele-diffusione sonora che consente di diffondere dal DCO di Saronno sulle stazioni dell'intera rete sia gli annunci automatici relativi alla circolazione sia quelli manuali;
- un sistema di colonnine SOS di tipo audio/video con pulsanti di chiamata differenziati per le richieste di informazioni, di soccorso sanitario o di soccorso di polizia;

- un sistema di remotizzazione degli ascensori installati nelle stazioni che consente di accentrare le telesegnalazioni dello stato degli ascensori, di effettuare telecomandi come la messa in servizio o la messa fuori servizio, di ricevere richieste di soccorso dagli utenti grazie all'help point audio/video installato nella cabina;
- un sistema analogo per il controllo delle scale mobili;
- un sistema per l'accertamento dei passaggi a livello che permette di verificare visivamente lo stato di occupazione dei binari, di impartire disposizioni alle persone presenti nell'area del PL per mezzo di un sistema di tele-diffusione sonora, di ricevere richieste di soccorso mediante un help point audio/video.

I sistemi di comunicazione over IP consentono soluzioni integrate di security e safety. Quali sono gli ambiti applicativi più importanti?

Nei sistemi di comunicazione over IP la separazione tra security e safety è difficilmente definibile in quanto i sistemi installati risolvono quasi sempre problemi di entrambe le aree.

Per esempio il sistema installato presso i passaggi a livello è sistema di security in quanto è presente un help point audio/video per richieste di soccorso in relazione a qualsiasi tipo di emergenza ma dall'altro svolge funzioni di safety in quanto integra i sistemi di segnalazione nell'area del PL consentendo all'operatore di verificare tramite le immagini l'eventuale impegno dell'area e quindi di intervenire sia con la diffusione di avvisi sia con le opportune azioni atte a regolare la circolazione dei treni. Altri ambiti in cui le tecniche di comunicazione over IP trovano utile applicazione sono quelli delle sicurezza cittadina, della gestione delle emergenze in aree industriali o nelle strutture destinate a ospitare eventi sportivi e, in generale, in tutti i luoghi ad alta frequentazione.

Quali sono le strategie di sviluppo di ERMES ELETTRONICA nel prossimo futuro, quando si diffonderanno sempre più le soluzioni integrate per la sicurezza globale dei luoghi ad alta frequentazione e delle infrastrutture critiche?

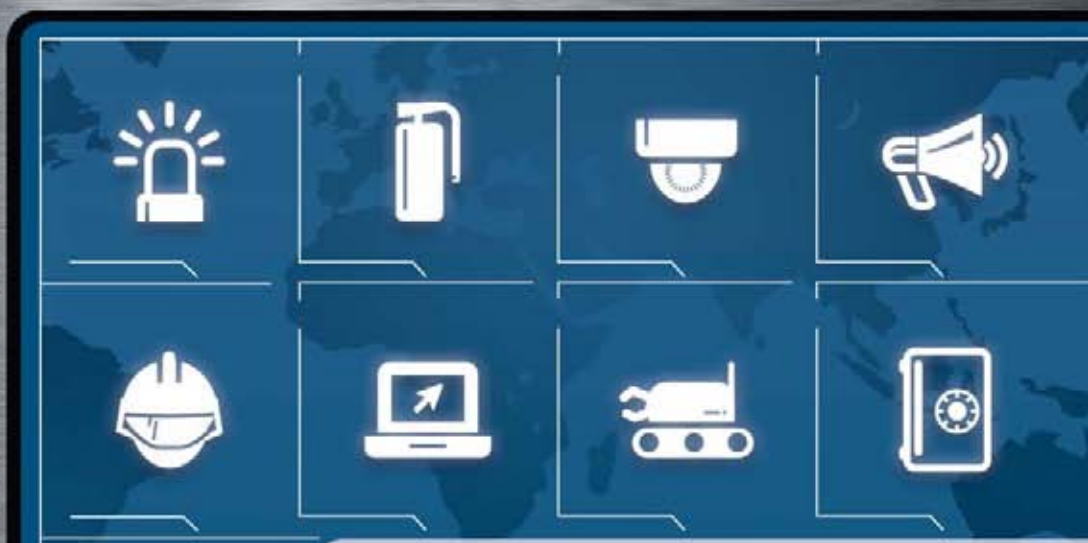
Il caso di FERROVIENORD indica in maniera chiara quali siano le linee di evoluzione che ERMES ELETTRONICA dovrà perseguire.

Il successo nello specifico ambito ferroviario, infatti, deriva dall'aver saputo integrare i sistemi di chiamata di emergenza con funzioni specifiche utili nel particolare ambito in cui questi apparati sono installati. Illuminante a questo proposito è il caso dei sistemi installati negli ascensori dove l'help point per la richiesta di soccorso installato all'interno della cabina si è integrato con un sistema che consente la raccolta di informazioni sullo stato dell'ascensore stesso e l'effettuazione di telecomandi che permettono la gestione delle principali emergenze funzionali dell'elevatore. ERMES ELETTRONICA punta a sviluppare e a proporre non generiche "colonnine SOS" ma apparati diversi destinati a quelle realtà in cui la funzione base è arricchita da specifiche funzioni aggiuntive destinate a risolvere i problemi specifici dell'ambito di installazione.

intersec

January 19 – 21, 2014

Dubai, UAE



990 companies from **54** countries
21,549 visitors from **116** countries
attended the record breaking
show this year.

Book your stand now & be part
of the region's foremost trade
show for Security, Safety and
Fire Protection next year!

www.intersecexpo.com

messe frankfurt

GS250 di Paradox: una protezione a regola d'arte

a cura della Redazione

Intesa Sanpaolo sceglie il rivelatore accelerometro pluriassiale senza fili GS250 di PARADOX distribuito da DIAS per la protezione di Gallerie d'Italia.

L'ESIGENZA

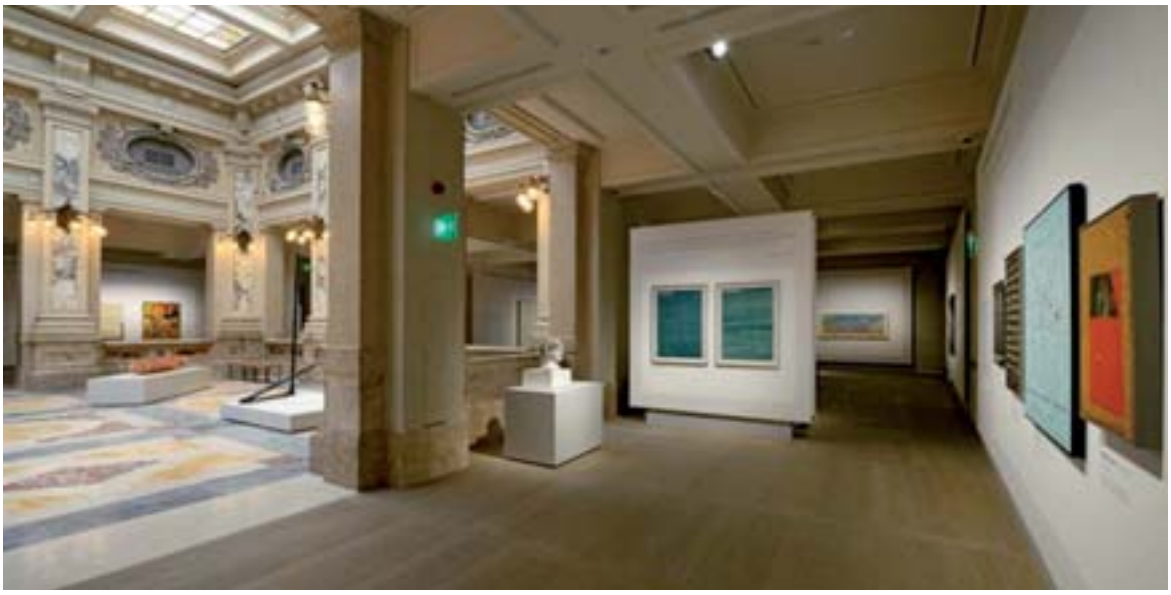
L'ideazione delle Gallerie d'Italia scaturisce dal desiderio di Intesa Sanpaolo di condividere con la collettività l'ingente patrimonio appartenente al gruppo bancario, costituito da pregevoli collezioni d'arte che vanno dai reperti archeologici alle testimonianze più alte del Novecento. Valorizzare le opere d'arte rendendole fruibili al pubblico ha determinato nuove esigenze di sicurezza per questi tesori, sottratti alla protezione confortante dei caveau nei quali erano custoditi per renderli accessibili nelle sale all'ammirazione di migliaia di visitatori. Per la protezione di molte di queste opere, Intesa Sanpaolo si è affidata all'esperienza di DIAS e ha scelto il rivelatore GS250 di PARADOX.

«Il tema della protezione delle opere d'arte è di massima importanza nel nostro operato, e va di pari passo con la valorizzazione del patrimonio artistico di proprietà. Intesa Sanpaolo, avendo il privilegio di disporre di un patrimonio d'arte di grande valore frutto della storia mecenatizia di oltre 250 istituti confluiti nel Gruppo, e ispirata da un radicato senso di responsabilità sociale, ha scelto infatti di mettere a disposizione del pubblico alcune raccolte di particolare importanza per farne veicolo di crescita civile

e culturale del Paese», evidenzia il responsabile dei Beni archeologici e storico-artistici di Intesa Sanpaolo Andrea Massari. «Oltre ai prestiti e ai comodati di opere in importanti sedi e rassegne nazionali e internazionali, abbiamo dato vita alle Gallerie d'Italia, rete di poli museali e culturali di Intesa Sanpaolo a Milano, Vicenza e Napoli che presentano alcune fra le maggiori raccolte delle nostre collezioni e sono spazi attivi di interazione culturale con le città in cui sono inseriti. La scelta di condividere i principali nuclei di questo patrimonio, che conta nel complesso circa 20.000 opere di cui 10.000 di valore significativo, all'interno delle nostre sedi museali, è quindi un impegno preciso che mira anche a contribuire allo sviluppo delle città, e in particolare dei centri storici, in cui si trovano i palazzi precedentemente utilizzati per attività istituzionali e commerciali della Banca. Il tema della sicurezza in spazi che volutamente consideriamo aperti e interattivi è quindi per noi imprescindibile, e viene trattato in modo approfondito all'interno delle normative di tutela del patrimonio artistico che hanno visto la nostra banca impegnata nel dotarsi di regolamenti interni molto stringenti, che prevedono fra l'altro l'utilizzo di sistemi di protezione di massima sicurezza e efficienza».

LA SOLUZIONE

GS250 di PARADOX è un rivelatore di movimento da interno senza fili che utilizza la tecnologia avanzata accelerometrica a tre assi (X, Y e Z) con sofisticato algoritmo software per una rilevazione sicura. Di dimensioni ridotte (mm 75x27x7) e facilmente occultabile alla vista, quando viene fissato a un oggetto da proteggere, quale un quadro o un vaso, attiva un allarme che scatta a ogni rimozione o spostamento dell'oggetto. La possibilità di regolare la sensibilità permette di realizzare la migliore protezione per ogni singolo oggetto e per ogni installazione. Le impostazioni possono essere effettuate per alta sicurezza (movimenti da 1 a 3 secondi) o sicurezza standard



(movimenti da 3 a 5 secondi). Inoltre si possono aggiungere fino a 4 secondi per ciascuna impostazione di sensibilità. GS250 offre una doppia protezione: antimanomissione, per l'apertura del coperchio del rivelatore, e antirimozione dell'oggetto protetto, se viene spostato impropriamente. Ogni volta che viene inserita la batteria (avviamento), o quando si apre il coperchio, GS250 entra in modalità prova, per uscirne dopo circa 15 minuti, o dopo un periodo di 5 minuti senza alcun movimento. Il rivelatore GS250 offre anche la modalità di risparmio energetico: se due allarmi consecutivi avvengono entro un periodo di 5 minuti l'uno dall'altro, il rivelatore entra in questa modalità per un periodo di 3 minuti. Tutte queste caratteristiche (oltre alla lunga durata della batteria - circa 2 anni con 2 rilevazioni alla settimana) la supervisione batteria bassa e la doppia rilevazione antimanomissione per rimozione o apertura del rivelatore fanno del rivelatore GS250 la soluzione ideale e più innovativa per la protezione di collezioni di valore, quali quadri e oggetti antichi.

I VANTAGGI

Intesa Sanpaolo ha scelto questo dispositivo per la protezione di moltissime opere esposte nei poli museali di Milano, Vicenza e Napoli per l'altissima affidabilità unita ai vantaggi della tecnologia senza fili, indispensabile in tutte quelle situazioni in cui la protezione delle opere non poteva avvenire tramite soluzioni cablate. La tecnologia senza fili e le dimensioni estremamente ridotte del dispositivo hanno permesso di non compromettere in alcun modo l'estetica degli ambienti e delle opere d'arte, tanto che nemmeno il visitatore più attento potrebbe accorgersi della presenza di GS250. Questo dispositivo si è rivelato la soluzione più adatta alle esigenze di Intesa Sanpaolo anche dal punto di vista economico. Soprattutto nel caso delle esposizioni temporanee, che avvengono frequentemente nei tre poli museali - l'ultima, dal titolo "1963 e dintorni. Nuovi segni, nuove forme, nuove immagini", è in corso a Milano alle Gallerie di Piazza Scala. L'utilizzo di GS250 permette di contenere enormemente i costi della messa in sicurezza perché ciascun rivelatore si adatta perfettamente a tutte le opere da proteggere - siano esse sculture, dipinti, ceramiche, vetri o reperti archeologici - e può quindi essere utilizzato di volta in volta per tutte le mostre, attraverso una semplice e veloce installazione. La possibilità di regolare la sensibilità permette infatti di realizzare la migliore protezione per ogni singolo oggetto e per ogni installazione.

CONTATTI

DIAS S.R.L.
Tel. (+39) 02 38036901
www.dias.it

25th YEAR

ufi Approved Event

THE WORLD'S BIGGEST SECURITY TRADESHOW

115,000m² 1,800 Exhibitors 200,000 Visitors 5,500 Booths

CPSE2013™

THE 14TH CHINA PUBLIC SECURITY EXPO

Oct 29 - Nov 1, 2013 | SHENZHEN CHINA

www.cpse.com.cn

The CPSE Golden Excellence Award 2013

CPS Forum 2013 - The 10th China Public Security Forum

The Public Security Academic Forum

October

29

SHENZHEN CHINA

Exhibitior partial list

ARONIX AXIS BOSCH Canon CHANGHONG CSST COSHIP DVR EverFocus FERMAX FUJICA HIKVISION

Honeywell H3C HUAWEI Infinova JinPeng JSST LG Panasonic Relong SANYO

SONY SIEMENS Skyworth SECOM VIDEOTREC YAAN ZTE

Da Venitem un nuovo alimentatore switching

a cura della Redazione

TSW 155 e TSW 157 sono i nuovi alimentatori switching di Venitem da 5 A o 7 A – 13,8 Vdc regolabili per TVCC, domotica e illuminatori a LED, con carica batterie tampone integrato.

Venitem ha progettato questo nuovo prodotto per rispondere alle più recenti esigenze di installazione per impianti di telecamere a circuito chiuso. Elevata potenza in un contenitore compatto, in grado di alimentare fino a 8 telecamere e impostare la tensione di uscita per compensare la caduta di tensione dei cavi in impianti TVCC medio-grandi. Il nuovo alimentatore si presenta come un prodotto altamente performante, in grado di fornire un importante valore aggiunto rispetto agli altri prodotti della sua categoria e risolvere alcune problematiche relative agli impianti di videosorveglianza. Le sue prestazioni d'avanguardia provengono da un'accurata ricerca di mercato, volta a soddisfare le più esigenti richieste di installazione e funzionamento, e fornire soluzioni pratiche, intuitive e alla portata di tutti. Inoltre utilizzando tecnologia switching è possibile avere un alto rendimento di conversione dell'energia a costi di utilizzo piuttosto contenuti.

Il TSW è dotato di 4 (versione a 5 A) o 8 (versione a 7 A) uscite indipendenti, ciascuna con protezione elettronica auto-ripristinante per cortocircuito e sovraccarico e LED di segnalazione fusibile aperto. Il circuito di ricarica della batteria è limitato in corrente per evitare il danneggiamento della batteria stessa; in caso di cortocircuito o batteria scollegata l'alimentatore è in grado di erogare ugualmente corrente, garantendo comunque un perfetto funzionamento dell'impianto.

Un'elegante e funzionale mascherina serigrafata è in grado di fornire indicazione ottica su: presenza rete (verde) – batteria ok (verde) – bassa (rosso) - sovraccarico (rosso) - guasto generale (giallo). Il sinottico sul retromascherina può essere applicato anche in un secondo momento, per soddisfare le più svariate esigenze prestazionali. Sul sinottico sono presenti un relè per la segnalazione remota delle anomalie e guasti e un relè per

segnalazione mancanza rete con ritardo programmabile. Tra le funzioni più innovative, la possibilità di monitorare in maniera remota il funzionamento dell'impianto, collegando i due relè sopraindicati a un combinatore telefonico GSM (che può essere comodamente alloggiato all'interno del box metallico), capace di inviare in maniera estremamente rapida la segnalazione di guasti. A seconda dell'utilizzo e delle performance desiderate, è possibile alloggiare batterie fino a 18Ah. Il box metallico è realizzato in due misure (a seconda che si tratti della versione a 5 A o 7 A), in lamiera d'acciaio zincata con sistema Aluzink, verniciata a polveri in colore grigio chiaro. Il box è completo di tamper anti-apertura del coperchio, collegabile a un combinatore GSM per segnalazione remota di apertura o manomissione.
Modelli disponibili: TSW 155 (alimentatore a 5 A) – TSW 155C (alimentatore a 5 A con scheda di controllo) - TSW 157 (alimentatore a 7 A) – TSW 157C (alimentatore a 7 A con scheda di controllo).

CONTATTI

VENITEM SRL
Tel. (+39) 041 5740374
www.venitem.com
info@venitem.com

FLIR-Aimetis Symphony™ una migliore protezione perimetrale a costi ridotti

a cura della Redazione

L'ESIGENZA

Solarpack è una società multinazionale di gestione integrata focalizzata su progetti di produzione di energia elettrica nel campo dell'energia solare fotovoltaica, specializzata nello sviluppo, finanziamento, costruzione, conduzione e gestione dei progetti. Il controllo di una vasta area su cui sono installate attrezzature di elevato valore non è un compito facile e di solito richiede ingenti investimenti per garantire una sufficiente protezione dell'impianto.

Per uno degli impianti fotovoltaici più importanti della parte occidentale della Spagna, Solarpack ora protegge il perimetro di 41 ettari con una soluzione di analisi intelligente realizzata dal CCTV CENTER di Valencia, che integra termocamere FLIR e il potente software di analisi Aimetis Symphony™.

Solarpack esamina continuamente nuove soluzioni per la sicurezza per disporre di un sistema pratico e in grado proteggere i propri impianti, tenendo in considerazione la complessità degli impianti solari. In questo progetto l'obiettivo era il contenimento dei costi di investimento e manutenzione, rendendo al contempo più efficace e affidabile il sistema di sicurezza e comprendendo la notifica automatica di allarmi ed eventi. Un ulteriore requisito essenziale era la rapida ricerca e visualizzazione delle immagini video. Diverse prove effettuate con altri sistemi di sicurezza hanno portato Solarpack alla conclusione che le termocamere e soprattutto le termocamere FLIR costituissero la soluzione migliore. A quel punto Solarpack si è rivolta a CCTV CENTER, distributore e integratore ufficiale di FLIR in Spagna.

LA SOLUZIONE

CCTV CENTER ha offerto una soluzione in cui le termocamere FLIR venivano abbinate al software di analisi video Aimetis Symphony. Aimetis Symphony è un premiato software intelligente di videosorveglianza che offre un'unica, innovativa piattaforma video IP aperta, per la gestione video, l'analisi video, l'integrazione di sistemi e la gestione degli allarmi.

Le immagini di qualità eccellente prodotte dalle termocamere FLIR insieme alle capacità analitiche di Aimetis Symphony si sono rivelate una soluzione ottimale per l'intero sistema.

L'utente finale aveva precedente esperienza in progetti comprendenti termocamere e aveva indicato come requisito principale una buona qualità delle immagini. Per l'elevato contrasto delle loro immagini, le termocamere sono particolarmente indicate per l'analisi in applicazioni perimetrali. Le termocamere sono in grado di rilevare bersagli umani a una distanza fino a 2.000 metri e di produrre immagini chiare e nitide nel buio più profondo, attraverso nebbia leggera e pioggia, in condizioni proibitive per le comuni telecamere TVCC. Le termocamere rappresentano una soluzione ideale per la sorveglianza 24/7, eliminando i costi per illuminatori IR o altri sistemi di illumi-

I bersagli umani vengono tracciati e attiveranno l'allarme all'attraversamento della recinzione virtuale

nazione supplementari. Per la protezione perimetrale di questo impianto fotovoltaico sono state installate 21 termocamere FLIR Serie F con una risoluzione di 320x240 pixel su pali alti 2-3 metri, lungo un recinto di filo metallico. Le termocamere Serie F sono completamente abilitate al controllo e funzionamento tramite reti digitali e analogiche. La Serie F fornisce immagini ad alto contrasto, ottimizzate per ottenere il massimo dal software di analisi video. Digital Detail Enhancement assicura immagini termiche chiare e correttamente contrastate in tutte le condizioni climatiche. Le termocamere operano insieme a un sistema di rilevamento anti-intrusione, entrambi collegati a un CSA (Stazione Centrale di Allarme). Tutte le termocamere sono integrate con il software Aimetis Symphony in modo che possano essere controllate da un PC server installato remotamente.

Nel software Aimetis Symphony viene definita una recinzione virtuale, in modo che quando un intruso ne attraversa la linea virtuale, determinata dall'operatore, viene attivato un allarme. L'allarme viene poi inviato al CSA, dove l'operatore ne riceve il segnale. L'operatore si collega con il client di Aimetis Symphony e controlla il relativo flusso video per verificare

Gli animali vengono considerati intrusi autorizzati e non attivano l'allarme

se si tratta di un falso allarme o di una minaccia reale. Il sistema è in grado di distinguere gli animali dagli umani. Quando il sistema individua il bersaglio come essere umano ne avvia il tracciamento. Il software attiva un allarme solo se il bersaglio attraversa la linea virtuale configurata dall'operatore. Quando il sistema identifica un bersaglio come animale od oggetto sconosciuto, non attiva alcun allarme, anche quando un animale attraversa la barriera virtuale. Questo, perché gli animali sono considerati come intrusi autorizzati nell'ambito del sistema. L'elevata qualità delle termocamere e l'affidabilità delle analisi rende possibile questa distinzione, con una conseguente diminuzione drastica del numero di falsi allarmi.

I VANTAGGI

Prima dell'installazione del nuovo sistema occorrevano da 10 a 15 guardie per garantire la sicurezza dell'impianto. Al momento non ci sono più guardie in pattuglia o a controllo dell'accesso all'impianto fotovoltaico. Ora tutto può essere gestito da una workstation remota da uno o due operatori.

«Integrare le termocamere FLIR della Serie F con il software Aimetis è stata una splendida soluzione», dice Pablo Campos di CCTV CENTER, responsabile di questo progetto. «Abbiamo utilizzato termocamere FLIR in precedenza con Aimetis Symphony e la Serie F di FLIR è compresa nella lista di dispositivi compatibili. Una volta calibrato, le prestazioni analitiche sono eccellenti. Il nuovo impianto ci procura un significativo risparmio ed è molto più efficace che avere una squadra di guardie di sicurezza che osservano le telecamere diurne incapaci di produrre immagini di notte o in condizioni meteorologiche avverse. Inoltre l'uso della tecnologia di imaging termico ci evita i costi di implementazione e manutenzione di un sistema di illuminazione. Infine, utilizzando termocamere invece di altre soluzioni, è ridotto anche il consumo di energia elettrica e anche i costi di manutenzione sono ridotti», conclude Pablo Campos.

CONTATTI

FLIR Systems Srl
Via Luciano Manara 2
I-20812 Limbiate (MB)
Tel. (+39) 02 99 45 10 01
Fax (+39) 02 99 69 24 08
www.flir.com
flir@flir.com

Communication network quali prospettive?

a colloquio con Francesco Della Mora, Regional Sales Manager – South Europe and LATAM – ComNet
a cura di Cristina Isabella Carminati

L'ingresso di Comnet nel mercato della sicurezza avviene al seguito della videosorveglianza over IP. Quale sarà il futuro dei communication network per la security: cavo in rame, fibra ottica o wireless? E quale sarà il ruolo del protocollo EtherNet?

L'ingresso di ComNet nel settore della Sicurezza è avvenuto nel 2008, anche se il dipartimento di sviluppo aveva già al proprio attivo due o più cicli di sviluppo di prodotti di trasmissione. La mission aziendale è dare soluzione a tutte le esigenze di connettività dei settori sicurezza, traffico/trasporti e comunicazioni. Il campo applicativo delle nostre soluzioni si limita alla connettività e alla trasmissione, anche se avremmo le capacità ingegneristiche per sviluppare sistemi di elaborazione/analisi di segnali video.

La videosorveglianza su IP si sta affermando come lo standard principale, guadagnando progressivamente quote di mercato sulla videosorveglianza basata su sistemi analogici (primi tra tutti le videocamere PAL). Nel quadro della sua mission, ComNet segue l'evoluzione della tecnologia e sviluppa costantemente nuove soluzioni per trasmettere i segnali generati dai nuovi sistemi di sicurezza. La trasmissione del Video over IP avviene tramite il protocollo Ethernet, che può appoggiarsi a vari mezzi fisici: il cavo in rame, la fibra ottica e l'etere (comunemente indicato come wireless).

Il futuro vedrà sicuramente Ethernet imporsi come standard preponderante, ma rimarranno alcune applicazioni di nicchia per la trasmissione analogica e altri standard digitali (come l'HD-SDI per esempio). Negli Stati Uniti la trasmissione video SDI ha avuto successo perché offre qualità e livello di risoluzione digitale lavorando in tipologia punto-punto, senza richiedere la configurazione di complesse reti Ethernet.

Un altro mercato importantissimo è quello dei sistemi che permettono la convergenza analogico-IP: codificare in IP i segnali generati dalle tradizionali videocamere PAL e trasmetterli attraverso una rete Ethernet non è l'unica soluzione di migrazione.

Le soluzioni di trasmissione ibride in grado di trasmettere simultaneamente segnali analogici e segnali Ethernet sullo stesso mezzo trasmissivo (cavo in rame o fibra ottica) permettono una migrazione graduale e una coesistenza delle due tecnologie e già oggi costituiscono un segmento di mercato importante e in crescita.

Quali caratteristiche devono avere le reti wireless per essere idonee a impieghi di security, in particolare in applicazioni ad alto rischio (infrastrutture critiche, installazioni militari, etc.)?

Il wireless è sicuramente interessante dove ci sono grandi distanze in gioco e dove il cablaggio fisico rappresenta un problema, perché le soluzioni di trasmissione sono provvisorie o perché la stesura di un cavo in fibra ottica è troppo costosa o impossibile. Le prestazioni del wireless sono inferiori a quelle della fibra a livello di ampiezza di banda e il rischio di intercettazione è superiore. Il wireless si pone quindi come alternativa valida per reti di videosorveglianza con esigenze di contenimento dei costi, con problemi di cablaggio e con richieste di ampiezza di banda medie.

L'approccio ComNet si propone di semplificare il prodotto in quanto a procedura d'ordine, struttura di licensing, installazione e modalità di configurazione. I nostri prodotti con antenna integrata hanno i limiti regolatori già preconfigurati a livello hardware, a differenza di molti altri prodotti in commercio che lasciano il compito di una configurazione esatta all'installatore. Nel prezzo base di acquisto vengono inclusi tutti i tipi di licenze, comprese le configurazioni ad ampiezza di banda massima. Il nostro prodotto per trasmissione punto-punto offre il setup più semplice del mercato. Disporremo presto di feature hardware e software richieste dal mercato della videosorveglianza come per esempio le opzioni di alimentazione PoE per il PD (Powered Device) e il PSE (Power Sourcing Equipment). Offriamo garanzia a vita, oltre ad altre feature in corso di sviluppo che ci differenzieranno maggiormente quando i relativi prodotti verranno lanciati nei prossimi mesi.

Abbiamo avuto richieste di sviluppo per sistemi a criptazione AES a 256 bit o FIPS per applicazioni militari. Il settore militare tuttavia tende a preferire tecnologie di trasmissione differenti dal wireless a causa della sua intrinseca vulnerabilità, salvo che non sia l'unica soluzione possibile. Le soluzioni wireless continueranno a evolvere verso l'integrazione tra 802.11 and 4G LTE and WiMAX; gli standard 802.11n and 802.11ac continueranno a essere utilizzati per applicazioni punto-punto fisse e punto-multipunto. Sistemi mobili e/o dinamici potrebbero integrare ulteriormente sistemi mesh basati su 4G LTE e 802.11. Prevediamo che un numero crescente di costruttori offrirà sistemi di backhaul ad alta ampiezza di banda operanti nella banda dei 6Ghz (aperta di recente) e sistemi a licenza gratuita operanti sui 24Ghz e 80Ghz caratterizzati da prezzi aggressivi.

Quali sono i mercati verticali più ricettivi per le soluzioni di network wireless? E quali i mercati geografici?

Elencare tutti i mercati verticali per il wireless sarebbe molto lungo. Il nostro focus verticale è il mercato della videosorveglianza e del controllo accessi. Man mano che la tecnologia evolve, l'installazione e l'affidabilità dei sistemi continuerà a migliorare.

L'affollamento dello spettro continuerà a essere un problema come ora lo è nella banda senza licenza dei 5Ghz. Il wireless non è invece molto adatto ad applicazioni di massima sicurezza.
I mercati geografici più favorevoli per il wireless sono i paesi con scarsa infrastruttura di trasporto dell'energia elettrica, che rendono difficoltosa l'alimentazione dei sistemi di trasmissione attivi o le economie emergenti che non sono in grado di investire in infrastrutture di cablaggio costose ma stabili nel tempo.

Quali strategie e quali obiettivi ha Comnet per il mercato italiano?

In Italia ComNet si sta posizionando come leader di mercato per qualità dei prodotti, quota di mercato e livello di servizio. La nostra politica di vendita si basa su canali di distribuzione ad alto valore aggiunto, ma come costruttore offriamo supporto tecnico diretto agli integratori/installatori e promuoviamo il prodotto presso i clienti finali e le ingegnerie in modo autonomo. ComNet offre anche corsi di formazione gratuiti in formato Webinar, con l'obiettivo di creare una base di clienti stabile e fedele e di promuovere il nostro brand all'interno di una ristretta cerchia di professionisti attraverso il marketing virale.

comnet
Communication Networks

JVC, ritorno dal futuro

a colloquio con Galileo Girotto, Country Manager Italy JVC Professional Europe Ltd.
a cura di Cristina Isabella Carminati

Precedente

JVC è un brand di grande tradizione nella videosorveglianza, che si ripropone sul mercato dopo un importante riassetto a livello corporate. Quali sono le novità più importanti per gli utilizzatori dei prodotti della divisione Security?
JVC Professional è ritornata con ambizione sul mercato europeo CCTV dallo scorso anno, con 4 nuove linee di prodotto (2 analogiche e 2 IP). Per essere più competitivi è stata creata una nuova organizzazione pan-Europea per gestire le vendite nei territori EMEA utilizzando la stessa politica commerciale e lo stesso listino prezzi. Come ben noto il marchio JVC è impegnato a fornire prodotti di alta qualità e affidabilità, può quindi offrire sul mercato prodotti con valori più alti di MTBF. Una delle caratteristiche principali di JVC sono infatti le nuove telecamere, che offrono soluzioni ideali per applicazioni in condizioni di luce ridotta, sia con prodotti analogici che IP. Abbiamo pertanto inserito delle categorie di prodotti che sono contraddistinte con il nuovo marchio Super LoLux.

A quale tipologia di utenti finali si rivolge ora JVC?
Idealmente i nostri prodotti si prestano a ogni tipo di installazione e uso professionale, specialmente dove viene richiesto un prodotto affidabile, di alta qualità, e soprattutto nei casi dove esistono criticità di illuminazione. Nonostante tutto siamo comunque focalizzati su mercati verticali dove possiamo offrire soluzioni ideali per la sorveglianza: la logistica, il settore distribuzione e grande distribuzione, i settori finanziari e le aree quali casinò e sale giochi.

Il passaggio da analogico a IP sta cambiando la configurazione del mercato, con l'entrata in

scena di nuovi vendor con partner di canale diversi da quelli tradizionali della security fisica. JVC a quali partner di canale si rivolge?
Non possiamo ignorare la crescita costante della tecnologia IP e l'attuale aumento della richiesta, ma non dobbiamo nemmeno trascurare quanto è ancora richiesto dal mercato analogico. La nostra azienda ha quindi deciso di offrire soluzioni per entrambi i mercati inserendo nel catalogo 4 nuove linee di prodotto: 2 linee analogiche LoLux + Super LoLux a22 Line 1080p HD, e Lolux HD + Superlolux HD.

La volontà è quella di identificare partner affidabili e preparati che, unitamente al nostro supporto, trasferiscano e/o completino le competenze dei vari professionisti sul mercato, eventualmente collaborando anche con system integrator per quei progetti e installazioni più complesse e ampie.

Quali sono i progetti di JVC per il mercato italiano, che si sta dimostrando sempre più interessato a soluzioni di video analysis e sta iniziando ad aprirsi verso la VssaS cloud based (videosorveglianza as a service su cloud)?
Nel mercato italiano, anche in questo caso, ci si concentra fortemente sul mercato verticale. Per fornire la soluzione ottimale e ideale per i nostri partner lavorando a stretto contatto con aziende leader quali Milestone, Seetec e VMS.

Nuova Everio

JVC PROFESSIONAL

SIA acquista Emmecom ed entra nella sicurezza

a colloquio con Andre Galeazzi, direttore Divisione Network Services di SIA e presidente Emmecom
a cura di Raffaello Juvara

Lo scorso luglio SIA ha acquisito il 51% del capitale sociale di Emmecom, società torinese ad alta tecnologia, con l'obiettivo di lanciare nuovi servizi di rete per banche ed esercenti a livello europeo, e di sviluppare soluzioni di rete innovative per il monitoraggio remoto basate sulla tecnologia M2M (machine to machine) che consente a dispositivi diversi – come sensori, sonde, telecamere, etc. – di essere controllati a distanza e di inviare in automatico segnali di stato a centrali di raccolta e gestione delle informazioni.

Emmecom, specializzata in reti di telecomunicazioni fisse, mobili e satellitari, fondata nel 2000 e con un fatturato di oltre 10 milioni di euro nel 2012, permetterà a SIA di diventare un player di riferimento in Europa nell'ambito dell'ultimo miglio dei pagamenti con carta ("transaction collection") e di entrare nel mercato della tecnologia M2M, che si caratterizza per un elevato potenziale di crescita: secondo gli analisti, infatti, potrebbe decuplicarsi nell'arco di un decennio, passando dai circa 4,4 miliardi di euro nel 2011 a oltre 44 miliardi di euro nel 2020.

Essecome ha intervistato Andrea Galeazzi, attuale direttore Divisione Network Services di SIA e nominato presidente di Emmecom, sulle prospettive di coinvolgimento di SIA nell'ambito dei sistemi evoluti per la sicurezza.

Dottor Galeazzi, quali sono le possibili interazioni tra le infrastrutture di rete per la gestione dei pagamenti con carta e il monitoraggio da remoto di sistemi di sicurezza?
Facendo leva sulla capillarità europea dell'infrastruttura tecnologica multiprotocollo e multiservizio di SIA, siamo ora in grado di sviluppare ulteriori servizi di rete integrati a supporto di ambiti applicativi tra loro anche molto diversi. Grazie all'acquisizione di Emmecom, società specializzata nella raccolta del traffico dei pagamenti con carta generato dai POS in multicanalità, possiamo gestire tutta la catena del valore lato acquiring, compreso l'ultimo miglio dei pagamenti con carta, ovvero la connessione finale dal terminale POS al server dell'istituto di credito. La stessa soluzione di rete può anche essere utilizzata per il monitoraggio da remoto di sistemi di sicurezza sfruttando la tecnologia M2M che rende dispositivi diversi come, per esempio, sensori, sonde, telecamere, etc. equiparabili ai terminali POS. Tali dispositivi possono di conseguenza essere controllati a distanza e inviare in automatico segnali di stato con latenza sempre minore a centrali di raccolta e gestione delle informazioni.

CHI È SIA

SIA è leader europeo nella progettazione, realizzazione e gestione di infrastrutture e servizi tecnologici, dedicati alle Istituzioni Finanziarie e Centrali, alle Imprese e alle Pubbliche Amministrazioni, nelle aree dei pagamenti, della monetica, dei servizi di rete e dei mercati dei capitali.
Il Gruppo SIA è attualmente presente in circa 40 paesi e opera anche attraverso controllate in Ungheria e Sud Africa. La società ha sedi a Milano e Bruxelles.
Con 9,2 miliardi di transazioni annue relative a carte, incassi, pagamenti e corrispondenti a oltre 4 miliardi di operazioni effettuate, SIA gestisce 63 milioni di carte e trasporta in rete 11,9 mila miliardi di byte di dati.
Il Gruppo si compone di sette società: la capogruppo SIA, le italiane Emmecom (applicazioni innovative di rete per banche e imprese), Pi4Pay (servizi per Payment Institution), RA Computer (soluzioni di tesoreria per banche, imprese e PA) e TSP (servizi di payment collection per aziende e PA), Perago (infrastrutture per banche centrali) in Sudafrica e SIA Central Europe in Ungheria.

Questo vuole dire che SIA potrà gestire anche il monitoraggio da remoto dei sistemi di sicurezza delle banche e dei negozi dotati di POS?
Assolutamente si. Questo è l'obiettivo di servizio a cui puntiamo anche se ci muoveremo attraverso gli operatori già presenti sul mercato, siano essi istituti di vigilanza o banche. Partendo dalla nostra capacità di gestire infrastrutture sicure e resilienti, ci proponiamo in questo nuovo settore mettendo a disposizione dei diversi attori soluzioni tecnologiche innovative in grado di migliorare e semplificarne i processi e di ridurne i costi. Il nostro approccio è neutrale e di tipo esclusivamente infrastrutturale: così come non entriamo nel merito della componente finanziaria delle transazioni con carte, di esclusiva pertinenza delle banche e dei loro clienti, non ci occuperemo della gestione dei segnali di allarme, al di là degli aspetti normativi che tuttora la riservano agli istituti di vigilanza autorizzati.

Tornando alla tecnologia M2M, quali sono gli ambiti applicativi che potranno rientrare nella vostra offerta?
I campi di applicazione del "machine to machine" sono molteplici, spaziando dalla sicurezza alla geolocalizzazione, dai trasporti alla sanità, dall'energia alla telemetria, fino alla supply chain delle aziende. Tra tutte, SIA si concentrerà in particolare sulle applicazioni più in linea con il core business della società, escludendo quelle più distanti dal nostro settore di competenza come, per esempio, l'ambito medicale e logistico. Come già detto, tramite l'infrastruttura di SIA sarà possibile abilitare servizi di monitoraggio remoto delle filiali bancarie e dei negozi a supporto degli istituti di vigilanza; oppure nell'ambito delle cosiddette "smart grid" sarà possibile gestire la rilevazione in tempo reale delle informazioni relative alla produzione di energie rinnovabili per bilanciare la potenza delle centrali elettriche tradizionali al fine di distribuire energia in modo efficiente.

Accessibilità e controllo:
valutare il livello di esposizione a crimini predatori

di Lorenzo P. Luini, Sapienza - Università di Roma
e Marco Scorzelli, Operatore per la sicurezza e il controllo sociale

La rapina è classificata tra i "delitti contro il patrimonio" e viene percepita socialmente come uno dei crimini più violenti, alla stregua dell'omicidio, della violenza sessuale e delle aggressioni.
Il timore di possibili condotte violente da parte dei rapinatori (aggressioni fisiche, ferimenti, omicidi, cattura di ostaggi) fa di questo reato un problema sociale, con costi onerosi non semplicemente per l'istituto/banca rapinato ma anche per la collettività.
Un'analisi sistematica delle condizioni nelle quali si verificano le rapine suggerisce che possano essere individuati e utilizzati strumenti e misure di prevenzione più efficaci che consentano di ottimizzare le attività e gli interventi con l'obiettivo di elevare il livello di sicurezza e di scoraggiare l'adozione di comportamenti criminosi e di rapina, riducendone l'impatto sociale e aziendale.
Grande attenzione è stata dedicata sino a oggi alla "fortificazione delle banche", utilizzando controlli, barriere e ostacoli - fisici e tecnologici – che impedissero accessi illegittimi, e sensibilmente meno alla "analisi del rapinatore", alla valutazione, cioè, delle caratteristiche e degli aspetti psicologico-motivazionali che determinano la volontà e la relativa decisione di effettuare una rapina.
In particolare sembra essere interessante determinare se esistono caratteristiche architettoniche, urbanistiche territoriali e ambientali che influenzano in modo significativo la decisione di commettere una rapina in banca.

Fig. 1

Fig. 2

I processi cognitivi che si celano dietro la decisione e la messa in atto di una rapina in banca sono tutt'altro che lineari o elementari.

Indipendentemente se tale condotta sia un'attività criminale pianificata e premeditata (posta in essere da un professionista) piuttosto che un reato commesso senza grande pianificazione e senza pensare alla possibilità di essere arrestati (posto in essere da rapinatori improvvisati e occasionali), quello che sembra utile considerare è quali siano i fattori che intervengono nel processo di selezione dell'obiettivo, prima, e di passaggio all'atto rapina, poi.

La letteratura internazionale di riferimento (elaborata quasi esclusivamente negli USA) suggerisce che possa essere individuato un modello di vittimizzazione delle dipendenze bancarie basato su determinate variabili territoriali e ambientali, ossia che vi possa essere una qualche relazione tra rapina e ambiente/territorio. Le ricerche condotte hanno evidenziato come i fattori maggiormente presi in considerazione dai rapinatori siano la localizzazione dell'istituto (con particolare riferimento alla presenza di vie di fuga e alla prossimità a un posto di polizia), la necessità di un veicolo per fuggire, la necessità di cambiare veicolo durante la fuga, la prossimità a luoghi appartati/nascosti, la presenza di vigilanza/guardiania, le dimensioni della banca e la tipologia degli accessi (più entrate, accesso diretto dall'esterno).

Sulla base della letteratura prodotta da studi internazionali sembra siano otto le variabili da dover considerare, e che queste possano essere raggruppate in due tipi di fattori principali riconducibili all'accessibilità e il controllo, come di seguito schematizzato.

Le variabili di "accessibilità" all'obiettivo sarebbero:

1. la prossimità a un'arteria stradale principale e molto veloce (autostrada, tangenziale e similari);
2. la prossimità a un parcheggio/area di sosta/area di scambio;
3. la categoria della strada sulla quale si trova la sede bancaria (SS o superiori, SP, SC e strada locale);
4. il tipo di circolazione della strada sulla quale insiste la sede bancaria (a senso unico o a doppio senso di circolazione);
5. la velocità media rilevata sulla strada sulla quale si trova la sede bancaria;

mentre le variabili di "controllo" all'obiettivo sarebbero identificabili con vicinanza ad:

1. un posto di polizia;
2. un'altra filiale bancaria;
3. un distributore di carburante.

In una ricerca da noi recentemente condotta, considerando i dati relativi al Comune di Roma per il triennio 2009-2011, è stato possibile analizzare complessivamente 1321 agenzie bancarie e 374 eventi rapina.

Nel corso della stessa ricerca è stato inizialmente selezionato in modo casuale un campione di 200 filiali bancarie rapinate e 200 filiali non rapinate, e sono state calcolate le loro distanze: 1) dal benzinaio più

vicino; 2) dalla filiale bancaria più vicina; 3) dal posto di polizia più vicino; 4) dal parcheggio/area di sosta più vicina; 5) da un'arteria stradale principale e molto veloce.

Successivamente sono state comparate le medie delle distanze relative ai vari siti considerati e sottoposte al t-test —T Test di Student (W.S. Gossett, 1908) — per verificare se vi fossero differenze significative tra esse.

Inoltre è stata condotta un'analisi della regressione sui dati relativi alle distanze sopradette utilizzando il modello di regressione "Probit" che offre l'opportunità di individuare la probabilità che una filiale bancaria, date le sue specifiche caratteristiche territoriali e ambientali, possa essere oggetto di rapina.

I risultati del t-test hanno evidenziato come la prossimità a un'arteria stradale principale e molto veloce e la vicinanza a un parcheggio e a un benzinaio, risultino significativamente correlate alla probabilità che un obiettivo venga rapinato.

Tali risultati evidenziano come la distanza/vicinanza territoriale a determinati elementi urbani possa influire significativamente sulla possibilità che un obiettivo venga vittimizzato (rapinato).

In merito alla seconda analisi utilizzando il modello di regressione "Probit" anche i modelli di regressione e i vari coefficienti individuati evidenziano come la distanza/vicinanza ovvero la presenza/assenza di determinate caratteristiche urbane e territoriali influiscano significativamente sulla possibilità che un obiettivo venga vittimizzato (rapinato).

L'analisi di dettaglio di ciascuno dei modelli individuati sembra poter dare informazioni utili per la migliore comprensione del fenomeno "rapina in banca" e del ruolo delle variabili territoriali nella distribuzione degli obiettivi.

I risultati hanno infatti mostrato come:

- una filiale bancaria che si trovi su una strada veloce abbia una probabilità di essere rapinata maggiore rispetto a quelle sedi bancarie che invece non soddisfano tale condizione;
- la distanza da un'area di sosta sia inversamente proporzionale alla probabilità di essere rapinati: all'aumentare della distanza delle filiali bancarie da parcheggi/aree di sosta/aree di scambio si riduce la probabilità stimata di essere rapinati;

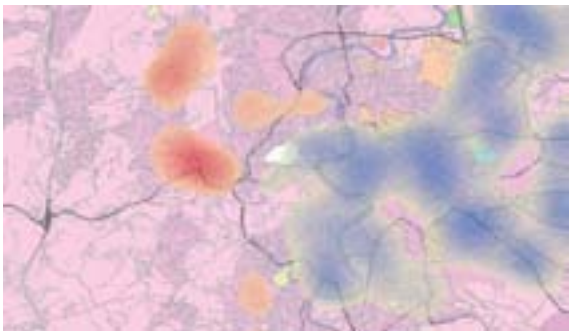


Fig. 3

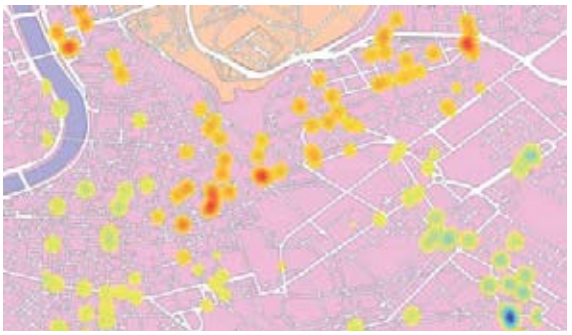


Fig. 4

- la distanza da un distributore di carburante sia inversamente proporzionale alla probabilità di essere rapinati: all'aumentare della distanza delle filiali bancarie dai benzinai si riduce la probabilità stimata di essere rapinati;
- la distanza da un'arteria stradale principale e molto veloce (autostrada, tangenziale e similari) sia inversamente proporzionale alla probabilità di essere rapinati: all'aumentare della distanza delle filiali bancarie dalle "strade veloci", si riduce la probabilità stimata di essere rapinati;
- una filiale bancaria che insista su una strada con velocità media ridotta (inferiore a 45 km/h) abbia una probabilità di essere rapinata minore rispetto a quelle sedi bancarie che invece si trovino su strade con velocità media elevata.

L'obiettivo principale del nostro studio pilota è stato quello di analizzare l'incidenza di determinate variabili territoriali e determinate caratteristiche ambientali sul fenomeno rapina; in particolare si è cercato di stabilire se e quali elementi territoriali/ambientali influenzino in modo significativo il processo di selezione dell'obiettivo-banca da rapinare.

A partire anche dalle risultanze e dalle raccomandazioni degli studi internazionali sono state individuate complessivamente otto variabili da analizzare e sperimentare, di cui cinque variabili di "accessibilità" alla filiale bancaria e tre variabili di "controllo" della filiale bancaria.

Grazie ai risultati ottenuti si può ragionevolmente pensare a un nuovo e innovativo, nonché più strutturato, indice di rischio ambientale, che abbiamo definito "Indice di Rischio Territoriale Rapine (RTR)".

Tale indice (che non tiene in alcuna considerazione le variabili endogene delle filiali bancarie) è strettamente legato alle caratteristiche urbanistico-territoriali dell'ambiente in cui insiste la singola dipendenza bancaria: ha quindi una valenza "discreto-puntuale", e non di area, rione, quartiere, municipio o comune.

Concludendo, grazie a questo studio, per quanto pilota, sembra che ora siamo in grado di fornire un valido strumento per una migliore comprensione del ruolo delle variabili territoriali nella definizione di un indice di rischio rapina sempre più aderente alle esigenze di safety e security del mondo bancario.

Proprio in tale ottica i modelli utilizzati in questo studio sembra si prestino in modo pertinente e forte per la valutazione del rischio rapina in tutte le fasi di pianificazione in cui è necessario attuare strategie per prevedere, gestire, ridurre o contenere le minacce (fig. 1), al fine di garantire l'incolumità delle persone e ridurre al minimo le eventuali perdite economiche e di immagine.

L'indice RTR potrà essere quindi, per esempio come in fig. 2, calcolato per ogni area d'interesse e utilizzato per integrare le misure già comunemente utilizzate al fine di ottenere una visione migliore del rischio rapina.

Allo stesso modo, l'indice RTR potrà essere utilizzato per individuare i cosiddetti "Punti Caldi" e "Punti Freddi", zone a maggiore o minore rischio, e poter così valutare il rischio a cui potrebbero essere esposti i siti, in caso sia di espansione che di contrazione del numero delle filiali (fig. 3 e 4).

Articolo estratto dal paper presentato e raccolto negli atti del convegno della 14° Conferenza Nazionale Utenti Esri, Roma 17-18 aprile 2013.

Oil & Gas, il terreno della sicurezza globale

a cura della Redazione

Spaziando dalle piattaforme off-shore alla stazione di servizio sotto casa, il mondo dell'Oil & Gas è di vastità estrema, richiedendo di fatto ogni possibile applicazione della sicurezza in tutte le declinazioni, come avevamo già accennato in precedenza (Essecome n. 1/2013).

È un mondo in cui il confine tra security e safety è molto opinabile, forse più determinato dalla natura delle cause degli eventi che dai loro effetti: per esempio l'incendio di un deposito produce gli stessi danni ambientali, economici e funzionali se causato da un atto doloso o da un incidente, con le stesse esigenze di contenimento, estinzione e ripristino; le misure preventive saranno invece molto diverse, in funzione della causa di pericolo dal quale proteggere l'impianto.

In relazione a questo approccio obbligatoriamente olistico alla sicurezza dell'Oil & Gas, Essecome ha raccolto alcuni contributi relativi a applicazioni sia di security che di safety, presentati dagli operatori più accreditati a livello mondiale.

Iniziamo con Dräger, multinazionale tedesca specializzata nei sistemi di protezione della vita, con l'intervista a Giampiero Moroni, sales manager per i sistemi di protezione individuale.

Quali sono le caratteristiche principali delle tecnologie per la protezione delle persone nel mondo Oil & Gas?

Le condizioni lavorative estreme di chi opera nel settore Oil & Gas richiedono standard di sicurezza particolari, che consentano di soddisfare qualsiasi esigenza e che siano nello stesso tempo conformi a tutte le specifiche tecniche previste. È di essenziale importanza che le tecnologie impiegate rispettino i rigorosi standard di qualità in modo da garantire un funzionamento autonomo degli impianti di produzione e delle piattaforme 24 ore su 24. È indispensabile quindi usare sempre l'equipaggiamento più adatto. I sistemi Dräger sono stati studiati per far fronte alla maggior parte dei pericoli che si possono presentare e si distinguono per la loro durata e resistenza, nonché per un funzionamento affidabile e sicuro.

Per garantire la massima sicurezza Dräger offre una vasta serie di prodotti e un programma di assistenza completo, che comprende le operazioni di manutenzione ordinaria e straordinaria, la formazione e la fornitura di accessori, tutti perfettamente compatibili e adattabili alle esigenze individuali. Che si tratti di protezione respiratoria, rilevamento

gas e apparecchiature di misurazione, della sospensione completa delle attività di un impianto, del noleggio di attrezzature, della formazione sulla sicurezza o della misurazione del tasso alcolico sul luogo di lavoro: in tutti questi casi si può sempre contare sugli oltre 100 anni di esperienza Dräger nel continuo sviluppo di sistemi di rilevamento gas e di misurazione, estremamente sensibili e di lunga durata.

Parliamo dei dispositivi di protezione individuale
Dräger offre una gamma completa di dispositivi per la protezione personale necessari per operare in situazioni di rischio o pericolo. Il materiale di protezione garantisce la sicurezza di tutto il personale che lavora all'interno di un impianto produttivo. Il comfort e la facilità di utilizzo garantiscono un indice di gradimento superiore da parte di tutto il personale coinvolto. Si va dalla protezione leggera delle vie respiratorie (facciali filtranti delle serie X-Plore 1700) a maschere e semimaschere (X-plore 6500 e X-plore 3300 solo per citarne alcune) alla protezione degli occhi (Occhiali serie X-pect 8000).

I dispositivi di emergenza come vengono definiti?
Soprattutto in situazioni di emergenza, o lavorando in condizioni estreme, si ha la necessità di essere attrezzati per una sicura evacuazione dalle aree compromesse. Ogni qualvolta scoppia un incendio o si verifica un'emergenza con rilascio di sostanze pericolose nell'aria, una fuga rapida e sicura può costituire un elemento fondamentale per la sopravvivenza. Dräger dispone di un'ampia gamma di soluzioni: filtrazione dell'aria ambientale, ad aria compressa o a rigenerazione d'ossigeno.

Dräger ha sviluppato in modo particolare i dispositivi di rilevamento gas a livello individuale, di particolare importanza per l'impiego in ambiti operativi diversi
I dispositivi portatili di rilevamento gas della Dräger sono stati concepiti per soddisfare le esigenze riscontrate nel lavoro quotidiano. Sono maneggevoli e robusti, soddisfano standard tecnici elevati e vengono testati e provati in diversi ambiti applicativi. Uno tra i sistemi più all'avanguardia è costituito dal Dräger X-zone 5000 che trasforma i dispositivi di

rilevazione gas a uso individuale Dräger X-am 5000 in sistemi di monitoraggio ambientale per un'ampia gamma di applicazioni.
Una combinazione brevettata per una maggiore sicurezza: rispetto ai dispositivi di monitoraggio tradizionali a uso individuale, Dräger X-zone 5000 può essere posizionato nelle aree a rischio di fughe di gas. Dräger X-zone 5000 rileva i gas pericolosi generalmente in un'area compresa nel raggio di circa 25 metri ma l'area può essere aumentata collegando fino a 25 ulteriori dispositivi e andando così a creare una rete di monitoraggio completamente wireless. L'unità è composta dal rilevatore portatile X-am 5/5600, che può rilevare fino a sei tipologie di gas, e che è posizionato all'interno di un alloggiamento sulla parte superiore: questo consente ai gas di diffondersi all'interno dello strumento, indipendentemente dalla direzione del vento. Dräger X-zone 5000 funziona con una batteria che può alimentare il sistema fino a 5 giorni lavorativi e la cui ricarica avviene in 14 ore attraverso un caricabatterie tradizionale con eventuale opzione di caricabatterie a induzione. Dräger X-zone 5000 è dotato di un allarme visivo a led con visibilità a 360°, da un allarme acustico (110dB) e dispone di un contatto pulito al quale è possibile collegare per esempio lampeggianti remoti, semafori e altri dispositivi come per esempio un disgiuntore di potenza elettrica.

È possibile integrare le soluzioni di Dräger per la safety in sistemi gestionali di sicurezza globale?
I nostri dispositivi sono sicuramente integrabili con altre tecnologie rivolte alla sicurezza, ma sono applicazioni che vengono sviluppate da aziende specializzate nel "system integrator" le quali realizzano i sistemi globali per i clienti finali.

Dräger

Stride la vampa…!

a cura di Cristina Isabella Carminati

Un teatro non viene fatto rientrare fra le infrastrutture critiche, se viene distrutto da un incendio non si ferma il mondo e molti pensano, come quel ministro di un nostro recente governo, che «con la cultura non si mangia». In realtà, come fortunatamente molti altri sostengono, la cultura e la sua gemella arte possono invece creare molte opportunità di lavoro e, in un paese come l'Italia, contribuiscono in modo significativo al PIL nazionale, in modo diretto e indiretto.
Senza ridurre il problema alla mera questione economica, è pacifico che teatri, musei e monumenti artistici debbano essere considerati almeno "obiettivi sensibili" per il valore storico, artistico e socio/culturale dei contenitori e dei loro contenuti, per non parlare degli aspetti correlati alla protezione delle persone. Sono obiettivi da proteggere in termini di security e di safety e rappresentano un ambito applicativo importante per l'industria della sicurezza.
Per questo motivo, Essecome pubblica, a partire da questo numero, una serie di articoli dedicati agli incendi che hanno distrutto tre teatri negli anni '90, con un'accurata analisi delle circostanze che hanno li hanno provocati.

di Valerio Weinberger

OUVERTURE

Si dice che quando si apre un nuovo teatro è un momento lieto, quasi che, come la nascita di una nuova creatura in una famiglia, ciò portasse l'allegria e la gioia in tutte le famiglie della città. E si dice che quando un teatro brucia è come se un lutto colpisse l'intera comunità.
Gli anni novanta sono stati segnati dai disastrosi incendi di tre fra i più importanti e storici teatri d'opera europei: due in Italia, il Teatro La Fenice di Venezia e il Teatro Petruzzelli di Bari, e uno in Spagna, il Gran Teatre del Liceu di Barcellona.
Se il caso di Barcellona è abbastanza chiaramente da imputare a un incidente occorso durante lavori di manutenzione e adeguamento, i due casi di Venezia e Bari sono invece stati oggetto di interminabili controversie giudiziarie, e sono risultati essere di natura dolosa.
Nei tre casi che raccontiamo, riducendo l'analisi all'es-

senziale, si può dire che il caso di Barcellona nasce principalmente da un "errore umano", mentre nei due casi italiani le cause hanno a che fare con atti e comportamenti criminali.
In ogni caso una cosa è chiara, confermata dalla storia, e anche da questi episodi degli ultimi decenni: raramente (e per fortuna…) i teatri bruciano mentre uno spettacolo è in corso, con la presenza del pubblico. E ciò non soltanto perché le norme di sicurezza sono ormai quasi ovunque molto cogenti, perché l'impiego di materiali ritardanti, ignifughi o ignifugati è ormai largamente diffuso, perché gli impianti elettrici e termici sono ormai da qualche tempo assai più sicuri e meglio funzionanti rispetto al passato, e anche perché durante gli spettacoli sono sempre presenti, in varie parti del teatro, squadre di numerosi addetti antincendio, appositamente addestrati allo scopo, incaricati di vigilare, ma soprattutto perché, per pratica professionale consolidata da generazioni, quanti lavorano regolarmente in teatro, sia durante gli spettacoli sia durante le prove, hanno sempre avuto molta paura del fuoco, perché l'antico artigianato teatrale ha sempre lavorato con "naturale" accortezza, attuando normalmente comportamenti controllati e prudenti, derivanti dalla consapevolezza di operare in una situazione potenzialmente rischiosa, e perché comunque tutti i tecnici che lavorano in un teatro hanno una certa preparazione e una specifica formazione in materia di prevenzione e spegnimento degli incendi.
Quindi come e perché i teatri bruciano?
Andiamo con ordine, a ritroso, partendo dall'incendio più recente.

ATTO PRIMO

29 gennaio 1996 – Teatro La Fenice, Venezia

In questo caso il dolo si è sommato ad altre concause. I canali che circondavano l'isoletta della Fenice erano in secca per lavori di pulizia, dopo circa cinquant'anni. Il teatro era temporaneamente chiuso per lavori di restauro e adeguamento alle norme vigenti in materia di prevenzione (ironia della sorte e curiosa coincidenza!) degli incendi. Molte ditte, di Venezia e non soltanto, anche in subappalto, lavoravano in contemporanea, più o meno alacremente, per l'ultimazione dei lavori. Il teatro, infatti, doveva riprendere l'attività all'inizio di marzo 1996, con uno spettacolo firmato da Woody Allen. Mentre i lavori erano in corso l'impianto di rilevazione fumi era disattivato e non utilizzabile, mentre l'impianto di spegnimento fisso era parzialmente inattivo. Alcune

porte, tagliafuoco e non, erano aperte per consentire il passaggio dei cavi elettrici provvisori e alcune finestre erano aperte per l'eliminazione di detriti e macerie, o chiuse temporaneamente con teli di plastica. Gli impianti elettrici erano in parte attivi. Le indagini seguite all'incendio hanno inoltre mostrato responsabilità per la situazione piuttosto trasandata e trascurata del cantiere. A tutte queste cause, molte derivanti da incuria colposa, si è intrecciato il dolo, come fattore determinante e scatenante.
Va osservato, a margine, che è soltanto grazie alla tempestività, alla perizia e alla professionalità dei vigili del fuoco veneziani, intervenuti nell'arco di pochi minuti dopo le prime segnalazioni, intorno alle ore ventuno, se i danni sono stati limitati al teatro, se l'incendio non si è propagato agli edifici circostanti, i quali hanno subito solo danni e disagi di limitata entità, e se non ci sono state perdite di vite umane.
Con sentenza definitiva sono stati condannati due addetti, installatori elettrici di una delle ditte esterne impegnate nei lavori in corso. Enrico Carella e Massimiliano Marchetti, questi i loro nomi, sono stati condannati in primo grado rispettivamente a sette e sei anni di reclusione,per aver deliberatamente appiccato

il fuoco al teatro, con l'ausilio di un fluido accelerante di fiamma.
La condanna è stata confermata in appello nel 2002 e in Cassazione nel 2003. Insieme a loro è stato condannato, ma soltanto al pagamento di una multa, anche il direttore del cantiere, Sisto Ruggiero, per non aver preso tutte le cautele dovute.
Motivazione scellerata del gesto dei due installatori: avrebbero appiccato il fuoco per evitare di pagare una penale, essendo in forte ritardo con i lavori. Inoltre, uno dei due era carico di debiti, anche perché – si disse – faceva per giunta uso di sostanze stupefacenti…
Insomma, l'iter processuale ha dimostrato abbastanza rapidamente che l'incendio della Fenice è stato di carattere doloso e non è stato provocato dal "solito" cortocircuito che si tira in ballo sempre in queste occasioni. Rileggendo i giornali del 30 gennaio 1996, o rivedendo i telegiornali di quei giorni, la prima ipotesi data in pasto all'opinione pubblica era quella dell'incendio sviluppatosi per un guasto all'impianto elettrico. Questa ipotesi, e non è soltanto il caso della Fenice, è stata ripetuta una tale quantità di volte al punto da fissarsi nella mente delle persone come una verità assoluta: ecco, siamo alle solite, quando un teatro brucia la colpa è sempre di un malfunzionamento elettrico. Falso.
Ciò non significa sostenere che gli impianti elettrici non provochino mai incendi: magari così fosse. Significa solamente che una maggiore attenzione nel pubblicare le notizie provocherebbe qualche distorsione della verità in meno.
Certo è che oggi le normative in materia, nazionali ed europee, sono chiare e stringenti al punto che le chances di una "fatalità" legata a una disfunzione degli impianti si riducono al minimo, se appena queste normative sono applicate con coerenza e puntualità. E questo è il vero punto.
L'applicazione delle norme vigenti su materiali, impianti, dispositivi di sicurezza, uscite d'emergenza e comportamenti, deve essere verificata con regolarità, severità, attenzione.
E ciò, specie in Italia, avveniva (avviene?) talora in maniera non metodica, non certa, non attenta. (Non più tardi di pochi mesi fa, chi scrive ha visto alcuni addetti, presumibilmente di una ditta esterna, in una pausa del lavoro presso un importante teatro d'opera italiano, fumare in una sorta di ripostiglio, arieggiato da un finestrone e adiacente al palcoscenico, e separato da una porticina tagliafuoco lasciata semiaperta, e poi abbandonare mozziconi di sigaretta in una specie di bidone metallico…)

Federsicurezza e il default della vigilanza privata

di GpG – Gossip particolare Giurato

Il 16 luglio scorso, Federsicurezza ha presentato a Roma il Rapporto 2012 sulla vigilanza privata,(www.federsicurezza.it/public/documenti/2152012142710.pdf), realizzato per la quarta volta dall'istituto Format Research. Una giornata che verrà ricordata per almeno tre motivi:

1. i dati economici presentati, per quanto riferiti a un ormai lontano 2010, non lasciano dubbi sulla gravità di una crisi che sta falcidiando utili, investimenti e posti di lavoro nella maggior parte delle imprese del settore;
2. la ricerca ha messo in luce una sorprendente ignoranza del DM 269 presso la maggior parte degli operatori intervistati, aprendo in tal modo non pochi interrogativi sulle reali capacità/volontà di adeguamento alla nuova norma e, quindi, di

sopravvivenza delle aziende che questi signori possiedono o dirigono;

3. l'avvocato Luigi Gabriele, uno dei protagonisti della storia recente della vigilanza, ideatore e governatore indiscusso di Federsicurezza, ha pubblicamente dichiarato concluso il progetto federativo e ha sollecitato un ripensamento globale, mettendo sul tavolo anche il proprio ruolo di presidente.

Andando per ordine, secondo il Rapporto Federsicurezza nel quadriennio 2007/2010 gli addetti sarebbero scesi del 10,3%, passando da 49.166 a 44.098, mentre il numero degli istituti censiti sarebbe aumentato nello stesso periodo dell'1,24%, solamente grazie a un exploit del centro Italia (+14,41%) in netta contro-tendenza con il nord e il sud/isole, per un totale complessivo di 966 entità. Nel 2010 il 35% delle aziende avrebbe chiuso il bilancio in perdita e il 48% avrebbe ottenuto un risultato positivo inferiore a 50 mila euro. L'indebitamento avrebbe costituito la metà delle risorse per finanziare investimenti e circolante e, per finire, il 38% delle 878 aziende monitorate avrebbe avuto una contrazione del fatturato nel 2010, sugli stessi livelli di quanto era già avvenuto nel 2009 (40%).

Abbiamo usato il condizionale perché, per ammissione degli stessi ricercatori di Format Research, i dati economici presentati sono da assumere con beneficio di inventario per le difficoltà incontrate nella ricostruzione dei bilanci depositati. È stata evidenziata l'impossibilità di rilevare correttamente l'osmosi tra guardie giurate e portieri all'interno delle aziende, ed è stata ammessa la possibile inattendibilità dell'anagrafe, non potendosi rilevare dal codice di attività se le aziende sono in possesso o meno di licenza di PS per l'attività di vigilanza privata.

In ogni caso è presumibile che il quadro presentato da Federsicurezza nel 2013 sulla scorta di dati risalenti al 2010 sia ulteriormente peggiorato nel periodo intercorso. I dati forniti da ASSIV– Confindustria sul ricorso alla Cassa Integrazione Guadagni nell'ultimo biennio, evidenziano che le ore di CIGS sono passate da 756.464 ore nel 2011 a 1.123.083 nel 2012 (+48,5%) e quelle in deroga sono quasi raddoppiate, passando nello stesso periodo da 563.590 a 1.076.728 (+91,1%).

La somma delle ore integrate nel 2012 ha quindi superato il 3% delle ore nominali lavorate, mentre le 4.035 domande di disoccupazione e mobilità denunciano una ulteriore, presunta perdita del 9% dei posti di lavoro rilevati alla fine del 2010, non essendo stato fornito il dato del 2011.

Ma la parte più sorprendente del Rapporto Federsicurezza è senza dubbio quella relativa alla ricerca condotta sul livello di conoscenza del DM 269 da parte degli operatori. Gli intervistati hanno dato tali risposte che Format Research, forse spinto da compassione, ha ritenuto di sostituirli con più astratte imprese "parlanti". Riportiamo testualmente il passaggio della relazione del presidente Pierluigi Ascani, all'interno del Rapporto pubblicato nel sito di Federsicurezza:

«I primi dati evidenziano chiaramente un livello insufficiente di informazione da parte degli Istituti di Vigilanza. Solo il 53,6% delle imprese intervistate afferma di essere a conoscenza del D.M. 269/2010. Di queste, il 44,4% afferma inoltre di averne un livello di conoscenza "molto scarso". Scendendo nel dettaglio del livello di conoscenza delle singole materie trattate dal decreto, soltanto il 16,4% si ritiene realmente informato sul decreto, il 25,4% ne ha dichiarato un livello di conoscenza medio, mentre il 58,2% ha dichiarato di esserne poco o per nulla informato. Di fatto, soltanto il 22,4% del totale delle imprese ritiene di conoscere realmente il DM 269/10».

Di fronte a questo quadro, si possono fare 4 supposizioni: 1) i ricercatori hanno intervistato, a loro insaputa, imprenditori della vigilanza del Burundi o del Tagikistan; 2) gli imprenditori italiani della vigilanza si sono di colpo rimbecilliti; 3) gli imprenditori italiani della vigilanza hanno paura del DM 269 e mettono la testa sotto la sabbia per non vederlo; 4) gli imprenditori italiani della vigilanza hanno ciurlato nel manico. È praticamente impossibile credere che solo un imprenditore su cinque abbia dichiarato agli intervistatori di Format, si presume nella primavera del 2013, di ritenersi "realmente informato" sul DM 269/2010, a fronte della quantità esorbitante di informazioni circolate da quando il testo del decreto viaggiava ancora in bozza nel 2010, degli innumerevoli incon-

LBM ITALIA

LAUREL

MONEY
COMPETENCE

LBM-Italia S.p.A. è il nuovo pilastro nell'area della gestione efficace del flusso del contante.
LBM-Italia, introducendo nuovi dinamismi e nuovi rapporti costituisce un ponte più agevole e veloce fra l'esistente e il futuro.

LBM-Italia oltre ad essere il distributore ufficiale italiano della **LAUREL**, leader mondiale riconosciuta nella produzione di macchine per il trattamento delle banconote e delle monete, completa la sua offerta con una selezione d'eccellenza di apparecchiature complementari.

Ogni banconota Euro è caratterizzata da un ponte.
Il ponte è il primo fondamentale strumento che mette in relazione persone, merci e informazioni, collegando stabilmente due sponde opposte prima non facilmente raggiungibili.
Il ponte che consente l'efficace circolazione del contante si fonda su due pilastri: il trasporto e il controllo valori, e apparecchiature realmente robuste ed efficenti, assistite e garantite nel tempo.
Con LBM-Italia il sistema del contante dispone finalmente dell'alternativa data da uno dei più potenti Marchi internazionali e da una struttura operativa italiana snella come un ponte, tenace come un pilastro.

Ad esempio:
selezionatrice K12 a 12 cassetti
Novità assoluta, solo da **LAUREL**

LBM ITALIA
LAUREL
MONEY COMPETENCE

LBM Italia S.p.A.

C.so Principe Oddone, 37
10144 Torino (TO) Italia
tel. ++39 011 4731316
fax ++39 011 4304930
mail: info@lbm-italia.com
www.lbm-italia.com

tri organizzati dalle associazioni e dalle singole prefetture dal giorno dopo della sua pubblicazione, del fatto che, subito dopo la pubblicazione, il decreto è stato impugnato davanti al TAR da un nutrito gruppo di imprenditori che, evidentemente, lo conoscevano benissimo, ma soprattutto a fronte della naturale, morbosa curiosità che un qualsiasi imprenditore di qualsiasi settore ha per tutto ciò che può riguardare la sua azienda oggi, domani e dopo.

Siamo pronti a scommettere che, se fosse stata condotta una ricerca in parallelo sul livello di conoscenza del DM 269/2010 presso le guardie giurate che lavorano presso quegli stessi imprenditori intervistati, i risultati sarebbero stati molto diversi.

Come non pensare che, tra le cause delle esternazioni dell'avvocato Gabriele del 16 luglio, ci sia stata anche una incontenibile esasperazione verso una categoria che si presenta in tal modo?

Un pensiero suffragato da quanto Gabriele ha scritto in un passo dell'introduzione al Rapporto postata sul sito di Federsicurezza: «In verità non abbiamo avuto la capacità di titolare compiutamente questo nostro quarto incontro, forse in coerenza con la crisi d'identità del nostro comparto produttivo, in piena transizione normativa regolamentare, in confusione organizzativa strutturale, in difficoltà per scarsa capacità di rappresentanza organica, privo di acume lobbistico collegiale, addirittura travagliato da divaricazioni del contesto di rappresentanza datoriale a dir poco lesive dell'insieme».

Davvero difficile pensare che da bruchi di questo genere possano nascere farfalle, di qualsiasi tipo.

Vigilanza, la parola alle guardie giurate

a cura della Redazione

Essecome sta seguendo con estrema attenzione l'evoluzione degli istituti di vigilanza, che rappresentano un mercato importante per l'industria della sicurezza, sia come utenti diretti che come naturali distributori/system integrator di tecnologie, per tutte le fasce di utenti finali.
Ma, per parlare compiutamente di vigilanza (e di trasporto valori, che viene svolto dagli stessi soggetti imprenditoriali per un'altra anomalia prodotta dal Regio Decreto del 1931), non ci si può limitare agli aspetti tecnologici o alle strategie di impresa: è un settore ad alta intensità di manodopera, oggi formato da poco più di 40.000 persone mal contate in base delle stime delle associazioni di categoria, che stanno vivendo sulla propria pelle la metamorfosi delle aziende presso le quali lavorano e, più in particolare, della propria identità professionale di "guardia giurata". Volendo quindi far parlare anche le guardie, Essecome inizia da questo numero una collaborazione stabile con Il ***Calendario della Vigilanza Privata*** *d*i Andrea Caragnano, il blog più accreditato e seguito dai "ragazzi" della vigilanza.

IL PUNTO DELLA SITUAZIONE

di Andrea Caragnano

Mi alzo al suono della sveglia come ogni giorno, sono le cinque e trenta. Sento fischiare forte il vento, qui c'è la bora, mi ha strappato un angolo del telo del gazebo in giardino, poco male, cuce Rossana. Anche lei si alza con me, stessi orari, stesso lavoro, stessi sacrifici. Si rientrerà a casa solamente stasera, prima delle nove. Per avere uno stipendio "normale" abbiamo dato la disponibilità a fare le dodici ore, non c'è alternativa. Montiamo in macchina e facciamo la costiera che ci porta a Trieste. La strada è bellissima e a quest'ora non c'è nessuno. Poi oggi, vigilia di ferragosto, con il cielo color antracite e il vento forte, non si vedono neanche quei pochi, soprattutto anziani, che arrivano presto sulle rive adiacenti il Castello di Miramare per essere sicuri di prendere sempre lo stesso posto, quello un po' al sole e un po' all'ombra, che anche giocare a carte è bello in un giorno d'estate. La prima cosa che vediamo, una volta arrivati in città, è la Stazione Ferroviaria. Chi ci ha passato la notte dormendo sul pavimento in marmo, non per la scelta di un giorno ma per la condanna di una vita disgraziata, si guarda davanti con gli occhi ancora socchiusi e sporchi, come se aspettasse sì di svegliarsi, ma con la prospettiva di un'altra vita davanti, una vita con gli occhi puliti. A seguire, si apre davanti a noi Piazza Unità che oggi è più bella che mai e ci riserva un piccolo regalo.

Ormeggiato sul mare davanti c'è il quinto yacht del mondo, proprietà di uno sceicco degli Emirati Arabi, del valore di cinquecentocinquanta milioni di euro, millecento miliardi di vecchie lire. A cento metri di distanza la povertà assoluta e la ricchezza illimitata convivono, si fa per dire. Poi arriviamo sul posto di lavoro. Accendo il computer e vedo l'accredito della busta paga e dell'intero rimborso Irpef. E penso ai colleghi che in questi mesi si sono trovati senza lavoro. Come faranno adesso? Chi li aiuterà? E mi sento un privilegiato pur non essendolo. Domani è domenica, per gli altri. Io e Rossana lavoreremo. Sveglia alle cinque e trenta e rientro alle venti e trenta.

E ringraziare Dio di avere quello che abbiamo…

Già, ringraziare Dio di quello che abbiamo, ma quanto durerà? È la domanda che ci facciamo quotidianamente tutti, nessuno escluso. Alcuni, credo più per esorcizzare il futuro che non per reale convinzione, parlano in continuazione di nuove qualifiche e amenità simili, ma il destino è un altro, una buona metà di noi è destinata a cambiare lavoro. È proprio di questi giorni la notizia che rischia di essere la pietra tombale di questa fase della vigilanza privata italiana: ENAC ha deciso di sostituire le Guardie Giurate con i Portieri per la vigilanza presso le torri di controllo aeroportuali. L'operazione è stata fatta per poter dirottare i soldi risparmiati verso l'acquisizione di nuove tecnologie per aumentare, afferma ENAC, il grado di sicurezza del sistema aeroportuale italiano. Bruttissima notizia, è l inizio della fine, come purtroppo è già da un po' che dalle pagine del blog vado dicendo. E non è la ricerca di un lettore in più, ma la concreta voglia di dare quegli "avvisi ai naviganti" che, se opportunamente recepiti nei tempi e nei modi, possono salvare in navigazione la vita e, nel nostro caso, un futuro lavorativo a migliaia di colleghi. Ora, coloro che resteranno a casa che prospettive avranno, visto che ciecamente tra di noi si pensa più ad amenità quali qualifiche varie che non guardare in faccia la realtà dei fatti? La presenza delle Guardie Giurate presso le torri di controllo era un imperativo, vista la minaccia terrorismo e la conseguente definizione di sito sensibile. E, visto che si può fare a meno delle Guardie giurate dal sito sensibile per eccellenza, l'aeroporto, si può prevedere che la stessa operazione verrà proposta e realizzata in altri siti sensibili sull'intero territorio nazionale, che poi in alcuni casi, così sensibili non lo sono affatto. Oggi, per la committenza investire in sicurezza significa sempre più investire in tecnologie e non in Guardie Giurate, destinate a diventare un ricordo del passato a bassa tecnologia.

Non penso di sbagliare dicendo che il numero delle Guardie Giurate è destinato, nella migliore delle ipotesi, a dimezzarsi. Cominciamo a pensare alle cose serie intendendo, con questo, l'imminente chiusura di questa fase. Quale fase? Quella che ricorderemo come il "periodo della vigilanza privata a bassa tecnologia".

Adesso la stella polare che dovrà guidare il nostro cammino si chiama "concretezza". Cosa faranno le migliaia di Guardie Giurate che perderanno il lavoro? Come aiutarle "concretamente"? Riqualificarle nel portierato sembra essere la scelta più logica, tenendo presente che questo, almeno a tutt'oggi, significa vedersi ridurre sensibilmente la busta paga. Aiutare e dirigere la transizione di questi operatori della sicurezza significherà essere "realmente concreti". Qualcuno lo farà? Sono convinto che nel nostro settore, nel quale non sono mancati né ieri né oggi imprenditori dei quali si sarebbe fatto volentieri a meno, siano comunque in netta maggioranza coloro che hanno a cuore non soltanto il business ma anche le persone che hanno legato il loro destino e quello delle loro famiglie ai propri Istituti d'appartenenza, abbracciando la vita della Guardia Giurata come fosse una missione al servizio del bene comune. Ora c'è bisogno di organizzare questo "passaggio attraverso le acque". Nessuno di noi è Mosè, ma uomini e donne responsabili e capaci non mancano certo.

Wise, la porta per il mercato polacco

a colloquio con Wiktor Pietruch, Project Manager WISE 2013
a cura della Redazione

Quali sono le dimensioni del mercato della security in Polonia, e quali sono i segmenti più ricettivi (residenziale, bancario, governativo, industriale, retail)?
Nonostante la crisi mondiale la Polonia è l'unico paese UE che ha mostrato una crescita economica costante. L'utilizzo efficace dei fondi concessi dalla UE, circa 73 miliardi di Euro, influenzerà sicuramente un ulteriore sviluppo tra il 2014 e il 2020. Parallelamente alla crescita dei diversi settori economici, rileviamo un grande potenziale per le imprese operanti nel settore dei sistemi di sicurezza e di videosorveglianza.
Una delle aziende leader nel settore delle soluzioni di sicurezza e di controllo ha stimato che in prospettiva il mercato coinvolge circa nove milioni di famiglie e un milione di piccole e medie imprese. Soltanto il 6 per cento del mercato potenziale è coperto e se la tendenza continua le cifre raddoppieranno entro cinque anni.

È un mercato più aperto all'acquisizione di tecnologie "made in Italy" da parte di distributori locali oppure a soluzioni complete, fornite a grandi utenti finali da parte di system integrator specializzati?
Il mercato polacco è aperto alle nuove tecnologie. Parallelamente all'elevata crescita economica e allo sviluppo tecnologico il mercato polacco ha bisogno di soluzioni complete di security e videosorveglianza fornite ai consumatori finali dai system integrator internazionali specializzati. Le aziende polacche sono interessate a soluzioni affidabili e personalizzate. È l'occasione perfetta per i produttori e i system integrator italiani i cui prodotti sono ben noti per la loro qualità e il design user-friendly.

Quale pubblico visita WISE, e quali sono le attese per l'edizione di quest'anno?
Ci aspettiamo circa 4-5 mila visitatori professionali per la prima edizione della nostra manifestazione.

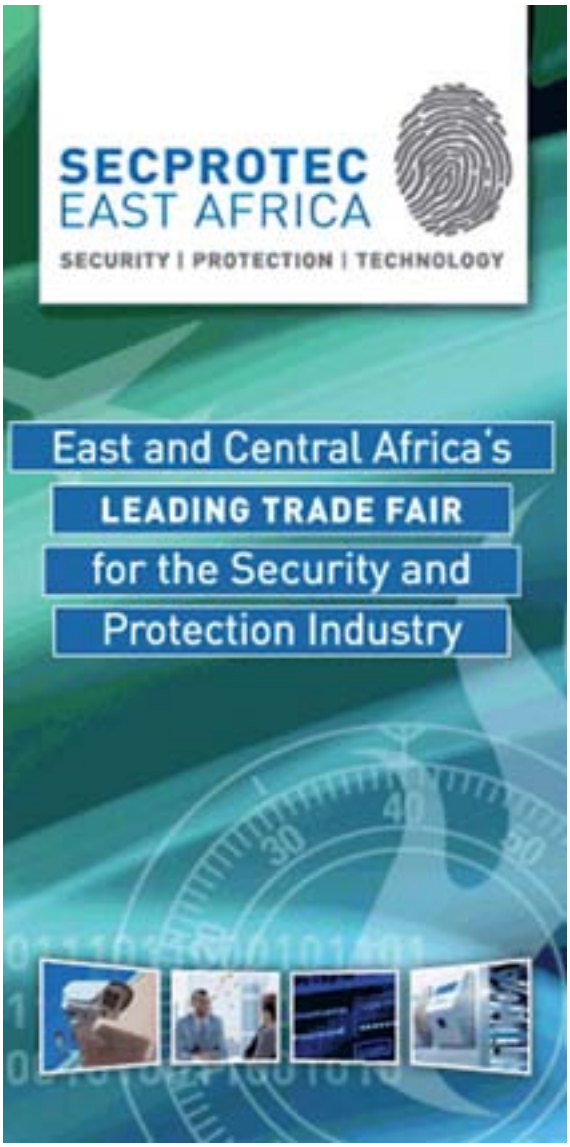
Abbiamo realizzato un'estesa campagna marketing e avremo tra i nostri visitatori distributori di prodotti e rivenditori al dettaglio, progettisti e architetti, consulenti, esperti e revisori, installatori, integratori, rappresentanti dei ministeri e degli enti locali, servizi civili, agenzie di sicurezza e i responsabili della sicurezza di aziende dei settori più diversi. WISE 2013 offrirà informazioni complete su prodotti, servizi e sulla situazione generale del mercato della sicurezza in Polonia.

Quali servizi offre WISE alle aziende italiane eventualmente interessate a partecipare?
Offriamo servizi di networking, che mettono in contatto i produttori italiani con i distributori polacchi interessati all'importazione e vendita di prodotti e soluzioni italiani. Forniremo una speciale area per il networking e gli incontri dei business partner. Offriamo anche una promozione speciali per i partecipanti italiani: una pubblicità gratuita nel catalogo della mostra, la possibilità di presentare un prodotto o una soluzione durante l'Open Discussion Forum o l'invio di newsletter dedicate. Grazie alla nostra campagna promozionale, i produttori e i system integrator italiani avranno una opportunità unica per contattare i distributori e gli utenti finali, ricevere un feedback sui loro prodotti e stabilire contatti d'affari.

Kenya, un mercato da scoprire

a colloquio con Skander Negasi, CEO Trade and Fairs Consulting GmbH
a cura della Redazione

Quali sono le dimensioni del mercato della sicurezza in Kenya e quali i segmenti più ricettivi (residenziali, banche, governo, oil & gas, vendita al dettaglio)?
L'Africa orientale è una grande piattaforma con un alto tasso di crescita per il mercato internazionale delle attrezzature di sicurezza. Vi è un numero considerevole di clienti facoltosi che sono disposti a pagare per la loro sicurezza privata. In particolare organizzazioni internazionali, ambasciate, enti governativi, Ong, grandi imprese, banche e società di comunicazione, nonché le classi media e alta, oltre naturalmente agli stranieri... sono tutti potenziali clienti per le aziende della sicurezza. Il Ministero del commercio tedesco, per esempio, ha già compreso l'importanza di questa industria e sostiene l'iniziativa "Sicurezza civile: un mercato strategico per il futuro".
Nairobi rappresenta l'hub per le organizzazioni internazionali. Importanti clienti per le tecnologie della sicurezza sono le organizzazioni antincendio private, così come la protezione civile. Un'altra at-



tività di rilievo è la protezione del trasporto valori, la cui domanda è aumentata recentemente. Inoltre, sia in Africa orientale sia in quella centrale, un altro potenziale segmento è la geolocalizzazione dei veicoli. Soltanto in Kenya vi sono 2.000 aziende registrate nel settore della sicurezza. Si attendono all'esposizione visitatori professionali provenienti da oltre 16 paesi dell'Africa orientale e centrale.

È un mercato più aperto all'acquisizione di tecnologia "made in Italy" da parte di distributori locali o propenso a soluzioni complete, fornite agli utenti finali da un system integrator specializzato?
La tecnologia "made in Italy" può essere venduta dai distributori locali, ma anche dalle sedi centrali. Alcune delle tecnologie vengono acquistate dalle autorità (aeroportuali, portuali, Revenue Authority, autorità nazionale di sicurezza, etc.) o unicamente da enti governativi. In questi casi il business sarà realizzato direttamente tra gli acquirenti del Kenya e le sedi centrali italiane. Altri utenti, come banche, alberghi, edifici governativi, ambasciate etc. possono essere gestite dai distributori locali.

Che tipo di visitatori vi aspettate a SECPROTEC e quali sono le aspettative per l'edizione di quest'anno?
Ci aspettiamo enti governativi, ministeri e importanti autorità da circa 16 paesi dell'area. Inoltre abbiamo invitato circa 42.000 potenziali acquirenti della regione attraverso il nostro partner Kenya Security Industry Association (KSIA) e altri supporter (tra quali la East Africa Bankers Association e la Kenya Hotel Keepers Association), così come varie ambasciate internazionali, organismi delle Nazioni Unite e altri organismi governativi.

Quali servizi offre SECPROTEC alle imprese italiane eventualmente interessate a partecipare?
Offriamo incontri riservati B2B con funzionari di alto livello, uno slot per intervenire alle conferenze così come uno sconto speciale riservato ai soli italiani che sarà commisurato al numero delle aziende coinvolte.

CPSE 2013: Shenzhen calling

a cura della Redazione

CPSE 2013, il 14° China Public Security Expo, che si terrà dal 29 Ottobre al 1° Novembre nella capitale mondiale del settore, attirerà su di sé ancora una volta l'attenzione di tutti.

Il CPSE di quest'anno, l'unica esposizione cinese autorizzata dall'UFI (The Global Association of the Exhibition Industry), ha già coinvolto 1.500 espositori provenienti da oltre 30 paesi, tra cui 55 fra le principali 500 aziende mondiali del comparto. Si stima che circa 120.000 visitatori visiteranno la mostra per conoscere i prodotti più recenti e all'avanguardia e cercare opportunità di business nel maggior distretto di produzione di sistemi di sicurezza che esista. Da oltre vent'anni il China Public Security Expo rappresenta la più grande esposizione mondiale sulla sicurezza, ed è determinato a raggiungere risultati ancora maggiori. Il CPSE 2011 ha rappresentato una svolta, giungendo a utilizzare tutti i nove padiglioni del Shenzhen Convention and Exhibition Center per la prima volta. Anche il CPSE 2013 sarà in grado di utilizzare tutti i 110.000 mq di spazio espositivo a disposizione. A seguito dei risultati raggiunti nell'edizione del 2011, il CPSE ha guadagnato la fama di principale mostra sulla sicurezza della Cina e si è affermata come un evento chiave atteso dagli opera-

tori del settore per tutta l'Asia. Con la conferma della presenza di oltre il 96% degli espositori del 2011, il CPSE è stato riconosciuto dai professionisti della sicurezza come la piattaforma ideale per le aziende che intendono mettere in luce le novità in fatto di tecnologie e di prodotti.

I più recenti ritrovati provenienti da tutto il mondo saranno in mostra: l'intera gamma della videosorveglianza, controllo accessi, antintrusione e allarme, citofonia, il meglio della tecnologia smart home, sicurezza perimetrale, tecnologia di gestione dei parcheggio e altro ancora. Inoltre, anche settori correlati avranno ampio spazio, come la sicurezza antincendio, anti-contraffazione, attrezzature di polizia, sistemi di trasporto intelligenti, sistemi d'ispezione, lotta al terrorismo e prevenzione dei reati, sicurezza del network e via dicendo. In rappresentanza delle più recenti innovazioni in fatto di prodotti, tecnologie, servizi e soluzioni, oltre 900 produttori di sicurezza, tra cui aziende leader come Huawei, Bosch, Honeywell, Panasonic, Samsung, Sanyo, Sony e Siemens hanno confermato la loro partecipazione alla manifestazione di quest'anno, per presentare gli ultimi ritrovati del settore. «Il China Public Security Expo è sempre stato una vetrina importante, per lanciare novità, raccogliere suggerimenti, percepire le aspettative degli utenti e cogliere le dinamiche tecnologiche del mercato», afferma Jian Pei, vice presidente dell'application business department di Sony China Professional Solutions Group (CPSG). «Speriamo di partecipare a ogni CPSE, che ci auguriamo migliori sempre più». Oltre al CPSE 2013 del 29 Ottobre/1° Novembre, vi saranno una serie di eventi organizzati in parallelo, tra cui l'11° Samsung China Public Security Forum, il Global Security Grand Cerimony 2013 (CPSE Golden Excellence Awards) e la conferenza GSIA (Global Security Industry Alliance). L'Expo non sarà soltanto un luogo in cui vengono esposti i prodotti: promuoverà una serie di attività per lo scambio di informazioni tecniche avanzate e per accedere ai più recenti sviluppi e dinamiche, attivandosi per lo sviluppo dell'internazionalizzazione del mercato e promuovere il commercio e lo scambio nel settore della sicurezza tra il mondo e la Cina. «Il China Public Security Expo è una grande piattaforma di comunicazione comune per l'industria della sicurezza. Il motivo per cui sponsorizziamo China Public Security Forum è la promozione delle nostre attrezzature di sicurezza in tutto il mondo e siamo felici del suo grado di professionalità», dice SungSik Kim, direttore generale di Tianjin Samsung Electronics Co., Ltd. Come sempre CPSE 2013 lavora a stretto contatto con i più alti enti governativi cinesi del settore della

sicurezza, avvantaggiandosi del sostegno del governo come delle più avanzate forme di ricerca per raggiungere il massimo livello di qualità. Nel 2011, il direttore del comitato Science and Technology del Ministero della Pubblica Sicurezza Li Runsen, il Vice Presidente del Science Research Institute del Ministero dei Trasporti, il Vice-Presidente dell'Associazione cinese per la Scienza e la Tecnologia, il Vice Sindaco di Shenzhen sono stati tra i visitatori del CPSE. Anche nel 2013 sono attesi per una serie di eventi e la loro presenza non fa che accrescere l'importanza dell'Expo.

Rappresentanti delle associazioni di categoria e delegazioni provenienti da molte delle principali aziende di tutto il mondo saranno presenti al CPSE 2013. Sono state ricevute conferme da Germania, Brasile, Emirati Arabi Uniti e da molti altri paesi e regioni che mostrano grande interesse e determinazione a partecipare. Si ipotizza un incremento di oltre il 25% annuale nel comparto dell'industria cinese della sicurezza con relativo incremento di espositori d'oltremare, visitatori e opportunità di business per la capitale della sicurezza mondiale. Ormai da tempo Shenzhen ha un ruolo fondamentale come centro di produzione mondiale per il settore della sicurezza. Sostenuto da massicci e ambiziosi progetti di sviluppo in infrastrutture come Città Sicura e dai futuri programmi di Smart City, il settore della sicurezza cinese sta conoscendo un rapido sviluppo e ha di fronte a sé ancora un enorme potenziale di mercato. In questo contesto, CPSE il 2013 è soprattutto un luogo ideale per costruire e migliorare la partnership e reti commerciali internazionali.

CPSE2013
THE 14TH CHINA PUBLIC SECURITY EXPO
Oct 29 - Nov 1, 2013 | SHENZHEN CHINA
www.cpse.com.cn

ESSECOME A CPSE 2013

Sarà, in assoluto, la prima volta che una rivista italiana della sicurezza viene ospitata con uno stand a disposizione a **CPSE**, la più importante rassegna settoriale in Cina che, in questo momento, rappresenta il principale mercato mondiale per la sicurezza fisica. L'iniziativa è stata definita nell'ambito del progetto di espansione internazionale della presenza e delle relazioni di Essecome Security & Safety nei principali mercati mondiali, a supporto dell'industria italiana della sicurezza.

La collaborazione con gli organizzatori della manifestazione di Shentzen si pone tre obiettivi: far conoscere agli operatori italiani una manifestazione che può rappresentare un'importante opportunità di relazioni bilaterali per l'export in Cina di soluzioni e prodotti fortemente identificati come "made in italy"; incontrare sul posto produttori locali per stabilire forme di partnership; far conoscere agli operatori cinesi interessati all'Italia, Essecome e www.securindex.com, due testate prestigiose con le quali presentare i propri brand e prodotti.

Essecome Security & Safety sarà presente a **CPSE 2013** con il key account per il mercato cinese signor **Hao Ming Geng**, che potrà fornire direttamente informazioni e assistenza agli operatori italiani interessati agli scambi con la Cina (cn.keyaccount@securindex.com)

Sicherheits Expo München supera tutte le aspettative

a cura della Redazione

La 10ª Sicherheits Expo si è conclusa con un bilancio positivo, per la soddisfazione degli espositori: «Abbiamo avuto ottimi contatti a livello comunitario e governativo, oltre che con molti partner. L'enorme potere d'acquisto degli investitori della Germania del sud è risultato evidente in questa fiera», ha detto Michael Schenkelberg, Responsabile Vendite e Marketing di Schneider Intercom. «Sicherheits Expo ha confermato la sua posizione di leader tra le fiere dedicate ai prodotti della sicurezza della Germania del sud e delle nazioni confinanti», ha detto Juergen Schneider di Nedap NTP. La qualità e il numero crescente di visitatori riflettono il successo della fiera per la safety e la security. Quest'anno 3.100 sono stati i visitatori della manifestazione tenutasi a Monaco di Baviera. Con una superficie di 5.500 m², il padiglione 4 del MOC di München-Freimann era tutto esaurito. Dopo il discorso di apertura Joachim Herrmann, ministro dell'Interno del land bavarese ha consegnato la medaglia d'onore conferita dall'Associazione bavarese per la sicurezza nell'economia (BVSW eV) all'ex capo della polizia nazionale, Waldemar Kindler. Il 3° convegno Fire protection, moderato da Wolfgang Friedl, è stato seguitissimo. In particolare è stato molto apprezzato dai partecipanti il tour tecnico dell'Allianz Arena. «Ottima organizzazione, perfetta moderazione, un buon programma, un valido mix di lezioni», ha commentato Joachim Roth della RVM Insurance Company. Il 6° convegno Door + Gate, sotto la direzione di Otto Meier Bielmeier e Günter Thomas ha avuto anch'esso molto successo. «Eccellente: informazioni molto interessanti sulle ultime norme e regolamenti», ha affermato Jürgen Portz, Direttore Rundoor Türautomatik. L'11° SicherheitsExpo si terrà dal 2 al 3 luglio 2014 presso il MOC Event Center di München-Freimann.

Essecome conferma la propria media partnership a Sicherheits Expo, ponendosi a disposizione degli operatori italiani interessati a partecipare all'edizione 2014 per promuovere nel modo più opportuno i prodotti nell'importante mercato della Germania del sud.

SIPS
03-09-13 **05-09-13** Krasnodar, Russia

SecurityUser Expo
17-09-13 **19-09-13** Copenhagen, Danimarca

ISAF
19-09-13 **22-09-13** Istanbul, Turchia

Asis International
24-09-13 **27-09-13** Chicago, USA

InfoSecurity
25-09-13 **27-09-13** Mosca, Russia

SIPS Siberia
25-09-13 **27-09-13** Novosibirsk, Russia

SECPROTEC East Africa
25-09-13 **27-09-13** Nairobi, Kenya

CIPS Central Asia
08-10-13 **10-10-13** Tashkent, Uzbekistan

Sectech 2013
22-10-13 **23-10-13** Stoccolma, Svezia

Libya Security & Defence Summit
24-10-13 **25-10-13** Londra, UK

CPEXPO – Community Protection
29-10-13 **31-10-13** Genova, Italia

CPSE 2013
29-10-13 **01-11-13** Shenzhen, Cina

A+A 2013
05-11-13 **08-11-13** Düsseldorf, Germania

Sfitex
12-11-13 **15-11-13** San Pietroburgo, Russia

Transport Security Expo
13-11-13 **14-11-13** Londra, UK

Wise 2013
19-11-13 **22-11-13** Varsavia, Polonia

All-over IP
20-11-13 **21-11-13** Mosca, Russia

9 th Middle East Energy Security Forum
25-11-13 **27-11-13** Dubai

Securtex 2013
26-11-13 **28-11-13** Tripoli, Libia

Intersec 2014
19-01-14 **21-01-14** Dubai

TB Forum
11-02-14 **14-02-14** Mosca, Russia

Sicur 2014
25-02-14 **28-02-14** Madrid

Security Expo 2014
27-02-14 **02-03-14** Roma, Italia

Security Expo
19-03-14 **22-03-14** Sofia, Bulgaria

European Security Conference & Exhibition
01-04-14 **03-04-14** L'Aia, Paesi Bassi

ISNR Abu Dhabi
01-04-14 **03-04-14** Abu Dhabi

MIPS 2014
14-04-14 **17-04-13** Mosca, Russia

Ifsec Sud Africa
13-05-14 **15-05-14** Johannesburg, Sudafrica

Ifsec 2014
17-06-14 **19-06-14** Londra, UK

Security 2014
23-09-14 **26-09-14** Essen, Germania

Sicurezza 2014
12-11-14 **14-11-14** Milano, Italia

4POWER S.R.L.
(+39) 081 8193441
www.4power.it

Videosorveglianza e wi-fi con alimentazione fotovoltaica

Lo switch industriale PoE BSP–300 della Planet Technology è un apparato all-in-one (switch Gigabit LAN, alimentatore PoE e carica batterie) per realizzare reti di comunicazione alimentate con pannelli fotovoltaici.
Progettato per ridurre al minimo i consumi e ottimizzare l'energia disponibile, permette di risparmiare la carica delle batterie mantenendo la massima affidabilità e sicurezza. Dispone di 3 Prese RJ45 di cui due PoE Gigabit, uscita alimentazione +24v per periferiche aggiuntive, contenitore alluminio pesante, ampia temperatura operativa. Protocolli PoE IEEE802.3at e af. Gestione batterie completamente configurabile.
A volte è necessario installare videocamere in luoghi dove allacciarsi alla rete elettrica non è né semplice né economico. Con il BSP-300 è possibile creare rapidamente soluzioni di videosorveglianza wireless permanenti o portatili, totalmente autonome per: controllo accessi; videocamere e ripetitori wi-fi in cantieri, porti e pontili di ormeggio, campi fotovoltaici e aree industriali; installazioni su edifici, parchi naturali, aree pubbliche, fiere o eventi.

FRACARRO S.p.A
(+39) 0423 7361
www.fracarro.it

FLY 2 DNS per collegare i DVR Fracarro a Internet

La gestione da remoto dei DVR è resa possibile attraverso connessioni internet che spesso comportano per l'installatore procedure complesse di collegamento.
A ogni accesso alla rete, infatti, tutti i dispositivi vengono identificati da un indirizzo IP dinamico, rendendo molto difficoltosa la connessione da remoto, a meno che non si disponga di un indirizzo IP statico (opzione a pagamento, peraltro non fornita da tutti i provider).
I DVR Fracarro risolvono questo problema con il servizio FLY 2 DNS, grazie al quale è possibile la connessione gratuita a internet direttamente dal menu del dispositivo, senza necessità di registrarsi a servizi esterni come No-IP o DynDNS e senza bisogno di utilizzare il PC.
FLY2DNS consente infatti l'accesso da remoto al DVR da rete esterna, identificando univocamente il dispositivo anche in presenza di indirizzi IP dinamici. A ogni collegamento del DVR a internet, l'IP ottenuto verrà trasmesso al servizio DNS, che aggiornerà di conseguenza il record associato al dispositivo.

INIM ELECTRONICS S.R.L.
(+39) 0735 705007
www.inim.biz

SmartLink Advanced: connettività avanzata

Un avvisatore telefonico, ma anche un risponditore, nonché un generatore di linea di riserva. Tutto in un unico dispositivo: SmartLink Advanced di Inim Electronics. SmartLinkAdv genera una linea di riserva quando richiesto dall'applicazione e opera come avvisatore telefonico vocale su linea PSTN e su rete GSM con 100 messaggi preregistrati e riprogrammabili. Inoltre, è sia un avvisatore SMS, sia un avvisatore digitale su linea GSM, GPRS e PSTN che utilizza i protocolli più diffusi degli istituti di vigilanza, come il Contact-ID o lo standard SIA-IP. Per le attivazioni da remoto (fino a 200 numeri telefonici), SmartLinkAdv diventa un risponditore con guida vocale che consente di attivare scenari ed effettuare operazioni domotiche e anti-intrusione. Attivazioni possibili anche mediante l'invio di SMS. SmartLinkAdv è programmabile da remoto, via Internet, attraverso il canale GPRS. Evoluzione di SmartLink, SmartLink Advanced di Inim Electronics rappresenta una vera innovazione nel mondo degli avvisatori.

RISCO GROUP S.R.L.
(+39) 02 66590054
www.riscogroup.it

RISCO Cloud: la soluzione di facile gestione

L'infrastruttura Cloud apre le porte a beneficio della sicurezza, dando la possibilità ai professionisti di fornire la più avanzata e dinamica soluzione sul mercato. Le possibilità sono molteplici: dall'avanzato sistema di controllo accessi Axesplus alle centrali di nuova generazione Agility3 completamente Wireless e presto la nuova versione di LightSYS, centrale ibrida controllabile via App. Agility™ 3 è un sistema di sicurezza radio bidirezionale che include la verifica video degli eventi e il controllo remoto tramite applicazioni per Smartphone e Web che sfruttano il RISCO Cloud. Grazie al Cloud: gli utenti possono usare le Applicazioni Web e Smartphone per controllare le proprie abitazioni e/o uffici; gli installatori possono usufruire delle funzioni di configurazione e di aggiornamento del sistema da remoto; gli Istituti di Vigilanza Privata possono usare le applicazioni web per gestire il proprio database clienti e i servizi a loro offerti. Gli utenti e gli installatori non hanno alcun costo per l'utilizzo del Cloud di proprietà di RISCO.

SICURIT ALARM ITALIA S.P.A.
(+39) 02 33405231
www. sicurit.net

Esclusivo doppia tecnologia da interno Tower 30®

Power G® Visonic è uno dei più innovativi sistemi di sicurezza via radio, grazie alla comunicazione bi-direzionale e alla trasmissione del segnale su frequenze variabili. Anche dal punto di vista della sensoristica Power G® non si fa mancare nulla, dai contatti magnetici per porte e finestre a dispositivi quali NextCam®, il sensore infrarosso con telecamera e Led IR incorporati per la video verifica degli allarmi, alle sirene e tastiere touch screen sempre via radio. Ora la famiglia Power G® si arricchisce di un esclusivo sensore da interno a doppia tecnologia, nome in codice WPMDT32AM, composto da una sezione a infrarossi con tecnologia a specchio e da una a microonda, il tutto con un sofisticato e affidabile sistema antimasking.
Rilevazione brevettata con Black Mirror Technology® per immunità a forti luci combinata alla tecnologia a specchio ellittico/parabolico esclusiva VISONIC. Ideale per chi vuole il massimo dell'affidabilità, riducendo ulteriormente la possibilità di falsi allarmi. Distribuito in esclusiva per l'Italia da SICURIT.

TSEC S.R.L.
(+39) 030 5785302
www.tsec.it

Sensori inerziali magnetici CLIC

TSEC introduce sul mercato un nuovo membro della famiglia di sensori per sistemi di allarme CLIC: i rivoluzionari sensori inerziali magnetici serie V. Estremamente compatti, in un involucro di soli 9mm di diametro si adattano all'incasso a scomparsa in tutte le situazioni installative grazie anche all'accessoristica dedicata. Basati su un nuovo principio ibrido inerziale/magnetico, gli inerziali CLIC non sono soggetti a vincoli di posizionamento, e possono quindi essere installati nelle zone dei serramenti dove il pericolo di scasso è più alto. Nel contempo garantiscono una lunga vita di funzionamento esente da falsi allarmi. La loro sensibilità è paragonabile a quella della migliore sensoristica oggi disponibile sul mercato, il che li rende compatibili con le schede di analisi più comunemente usate dai maggiori produttori. Nuovi inerziali CLIC: un'altra rivoluzione da TSEC nella sensoristica per sistemi di allarme professionali.

VENITEM
(+39) 041 5740374
www.venitem.com/

Venitem costruisce la tua sicurezza

Mose: prima sirena vocale ad alta qualità presente sul mercato, con precisi messaggi vocali permette di discriminare il tipo di intrusione in modo immediato, garantendo un intervento rapido. Il suo innovativo sistema di illuminazione a led ad alta luminosità illumina la zona violata, rendendone immediata la localizzazione. Il sistema è attivabile anche separatamente dall'allarme e trasforma Mose in un'elegante lampada da esterno. Tra le novità, la sirena per uso interno Mini Hola, che grazie a un led integrato può funzionare anche da comoda luce di emergenza. Sirena piezoelettrica in grado di emettere diversi tipi di suono associabili a diversi tipi di allarme e preallarme, con indicazione on/off che permette di monitorare in qualsiasi momento lo stato dell'impianto. E ancora l'ambitissima sirena/centrale Doge CT3, la prima in grado di funzionare anche da centrale d'allarme, concepita per la protezione di piccoli ambienti quali mini appartamenti, garage, piccole imbarcazioni, ponteggi e cantieri. Fornita in comodo kit di sicurezza, è in grado di gestire fino a tre zone ed è abbinabile a sensori di movimento per interno ed esterno.

ERRATA CORRIGE

Abbiamo attribuito per errore la qualifica di Technical manager di Crisma Security a Barbara Farulli che è invece Amministratore. Ce ne scusiamo con la sig.ra Farulli e i nostri lettori.

essecome
security&safety

n. 04 luglio-agosto 2013

ISSN: 2282-5770

Anno XXXIII - I
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE
Cristina Isabella Carminati

COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

REDAZIONE
Cristina Isabella Carminati - Raffaello Juvara

HANNO COLLABORATO A QUESTO NUMERO
Maurizio Barbo, Andrea Caragnano, Lorenzo P. Luini,
Marco Scorzelli, Valerio Weinberger

SEGRETERIA DI REDAZIONE
redazione@securindex.com

GRAFICA/IMPAGINAZIONE
Elisabetta Nasuti
info@enasuti.it

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Bozzini, 3
Milano - Via Keplero, 38
tel. 02/36757931 - fax 02/36757944

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

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

STAMPA
Grafiche G7 sas
Via Marconi, 18A - 16010 Savignone (GE)
tel. +39 010 9761488 - fax +39 010 9761482
graficheg7@graficheg7.it

Partner Essecome

4POWER	www.4power.it	69, 91
AICC	www.infrastrutturecritiche.it	28-31
ASSOSICUREZZA	www.assosicurezza.it	13-15
CE.S.I	www.cesi-italia.org	40
CITEL	www.citel.it	32-36
COMNET	www.comnet.net	59-61
CP EXPO	www.cpexpo.it	II COP, 41-45
CPSE	www.chinaexhibition.com	53, 87-89
DIAS	www.dias.it	50-52
DRÄGER	www.draeger.it	71-73
ERMES ELETTRONICA	www.ermes-cctv.com	47-48
EURISPES	www.eurispes.eu	39
FLIR	www.flir.com	56-58
FRACARRO	www.fracarro.it	91
Gazzoli Engineering	www.gazzoli.it	20-22
GUNNEBO	www.gunnebo.it	IV COP
HESA	www.hesa.it	18-19
INIM ELECTRONICS	www.inim.biz	91, III COP
ISAF 2013	www.isaffuari.com	23
JVC	www.jvcitalia.it	62-63
LBM	www.lbm-italia.com	79
MILESTONE SYSTEMS	www.milestonesys.com	I COP, 24-27
RISCO GROUP	www.riscogroup.com/italy	92
SATEL	www.satel-italia.it	11
SECPROTEC	www.secproteceastafrica.com	46, 85-86
SIA	www.sia.eu	64-66
SICHERHEIT EXPO	www.sicherheitsexpo.de	90
SICURIT ALARMITALIA	www.sicurit.it	92
TSEC	www.tsec.it	9, 92
VENITEM	www.venitem.com	93
VIDEOTREND	www.videotrend.net	1
WISE	www.wise-warsaw.pl	37, 83-84

AVVISATORE TELEFONICO ANTINTRUSIONE ALL-IN-ONE

INIM.BIZ

AVVISATORE SMARTLINK ADVANCED.
IL FUTURO DELLA TECNOLOGIA TI CHIAMA.

Lasciati rapire dal fascino della connettività avanzata.
Arriva l'avvisatore telefonico vocale, via SMS e digitale SmartLink Advanced. È programmabile in modo simile alle centrali SmartLiving, anche tramite internet. Opera su rete telefonica terrestre, GSM e GPRS. Genera una linea di backup. Gestisce il protocollo SIA-IP. Tutto in uno. Avanti in tutto.

inim ELECTRONICS


Ideale:
elegante, compatto,
personalizzabile.
Perfetto:
robusto, sicuro,
facile da integrare.
Gradevole:
silenzioso, discreto,
anche per disabili.
...e il Servizio?
Flessibile, rapido,
affidabile.
In una parola:
SpeedStile
il Varco per il controllo degli accessi
Soluzioni che creano valore
• CONTROLLO ACCESSI
• TRATTAMENTO DENARO
• SICUREZZA FISICA
• SICUREZZA ELETTRONICA
www.gunnebo.it
GUNNEBO
For a safer world®