

## INT-TSI. Nata per sorprendere.



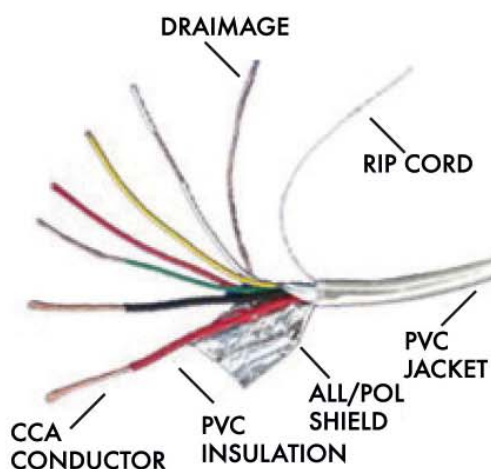
LA TASTIERA TOUCH SCREEN  
CHE RISPONDE A QUALSIASI ESIGENZA.

Completa integrazione con il TVCC  
e totale configurabilità nelle icone,  
nelle funzioni e nell'aspetto grafico.  
Ora creare scenari complessi e personalizzati  
ha solo il limite della fantasia.



**Satel**®  
— ITALIA —

[www.satel-italia.it](http://www.satel-italia.it)



# CAVO DI **ALTA QUALITÀ** **E BASSO COSTO**

...il nuovo nato in casa ELAN

# Galaxy<sup>®</sup> Flex



## Galaxy<sup>®</sup> Flex - Da oggi ancora più potente!

Innovativa, intuitiva e facile da usare, Galaxy Flex è una centrale antintrusione ibrida disponibile in tre contenitori per applicazioni residenziali e commerciali. La versione più recente di Galaxy Flex può essere gestita da smartphone e tablet grazie alla App Galaxy "GX Remote Control". Flex include caratteristiche di sicurezza presenti in prodotti di categoria superiore. Per un maggiore comfort di utilizzo

dispone della modalità di inserimento notturno. **Galaxy Flex<sup>®</sup>, la centrale antintrusione flessibile, scalabile, semplice e veloce da installare.**

## Honeywell



Per ulteriori informazioni su Galaxy<sup>®</sup> Flex per il vostro prossimo progetto visita [www.galaxyflex.com](http://www.galaxyflex.com) o chiama al 02 4888 051



© 2014 Honeywell International Inc. All rights reserved.  
Tutti gli altri nomi di società e prodotti sono nomi commerciali,  
marchi o marchi registrati delle rispettive società.



VIDEOTREND

## DISTRIBUTORI UFFICIALI PER L'ITALIA

**Doppler**  
security & automation

Distributore  
Piemonte  
Doppler

**dsa**  
brianza

Distributore  
Monza e Brianza  
DSA Brianza

**Vitekna**

Distributore  
Campania  
Vitekna

**AST**  
AUTOMAZIONE E SICUREZZA

Distributore  
Toscana  
AST

**B&B**  
Tecnosystems

Distributore  
Padova, Verona, Rovigo  
B&B  
Tecnosystems

**Sicurtel**

Distributore  
Como  
Sicurtel

**digitalsystem**  
SICUREZZA - AUTOMAZIONE

Distributore  
Puglia  
Digital System

**decibel**

Distributore  
Palermo, Agrigento e  
Trapani  
Decibel

**NIBRA**  
Security Solutions

Distributore  
Milano Nord Est  
Nibra

**COM.PAC**

Distributore  
Brescia e Bergamo  
Com.pac.

**PAMITRON**  
see the world

Distributore  
Trentino Alto Adige  
Pamitron

**CHECKPOINT**  
Sicurezza e Automazione per la Rete

Distributore  
Roma e provincia  
Checkpoint

**EACC**

Distributore  
Calabria  
ACC

**DSAMED**

Distributore  
Emilia Romagna  
DSAMED

**its**  
Teleselezione

Distributore  
Abruzzo - Molise  
ITS

**Sacchi**  
Elettronica

Distributore  
Lecco  
Sacchi

**VOYAGER**

Distributore  
Emilia Romagna  
Voyager

**TECNOCITY**

Distributore  
Milano Nord Ovest  
Tecnocity

**SCS**

Distributore  
Palermo  
SCS

Telecamere HD-SDI, IP Megapixel, HDCVI, Analogiche. Speed Dome. Videoregistratori di Rete, Digitali. Monitor LCD. Video wall. Armadi Rack. Fibre e Convertitori Ottici. Switch di Rete. Ottiche. Matrici Video. Custodie. Illuminatori IR. Gruppi di continuità. Sistemi di trasmissione WiFi. Accessoristica Professionale.



**Videotrend S.r.l.**

Distributore ufficiale Dahua

Tel. 0362 1791300

[www.videotrend.net](http://www.videotrend.net) / [info@videotrend.net](mailto:info@videotrend.net)



# i ♥ HDCVI

High Definition Video Composite Interface (HDCVI) è una tecnologia innovativa nella videosorveglianza, che consente la trasmissione in Alta Definizione (HD) fino a 500MT (720P) su cavo coassiale, completando così l'offerta esistente IP e HD-SDI ma a costi decisamente inferiori.

### Caratteristiche

- High Definition ( 720p o 1080p)
- Lunga distanza di trasmissione su coassiale
- Video in tempo reale
- 3 segnali (Video / Audio / RS485) su ogni canale/cavo coassiale

### modelli raccomandati:



4/8/16 All Channel 1080P  
2U Standalone DVR



4/8 All Channel 720P Mini  
1U Standalone DVR



720P/1080P Water-proof IR  
HDCVI Mini Dome Camera



720P/1080P Water-proof  
IR HDCVI Camera



1.3Mp HD HDCVI  
IR PTZ Dome Camera



1.3Mp HD HDCVI  
PTZ Dome Camera

CE FC © ® ISO 9001:2000

**DAHUA TECHNOLOGY CO., LTD.**

No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053

Tel: +86-571-87688883 Fax: +86-571-87688815

Email: [overseas@dahuatech.com](mailto:overseas@dahuatech.com)

[www.dahuasecurity.com](http://www.dahuasecurity.com)



# GLI EVENTI DI ESSECOMA A MEDITEXPO

Pastorano (CE), 16-17 maggio 2014

## 16 MAGGIO ORE 11.30 · AGORÀ REGGIA

### Il workshop di casamiasicura: il motore di ricerca B2C e la piattaforma di servizi B2B

Presentazione del motore di ricerca B2C [www.casamiasicura.it](http://www.casamiasicura.it), ideato per promuovere in modo efficace e economico l'incontro degli operatori (installatori di sistemi di sicurezza, istituti di vigilanza, rivenditori di infissi di sicurezza e casseforti) con gli utenti privati, per offrire soluzioni per la casa. Verranno presentate la **piattaforma di servizi B2B** riservata ai Vendor e al loro canale, le **convenzioni assicurative e le soluzioni di consulenza legale e tecnica** rivolte ai Partner.

## 16 MAGGIO ORE 15.00 · AGORÀ MASCHIO ANGIOINO

### La tavola rotonda di Vigilanza & Dintorni: L'applicazione del DM 269, a che punto siamo?

modera *Raffaello Juvara*

L'applicazione del DM 269, a oltre 3 anni dalla sua entrata in vigore, come sta procedendo? I requisiti minimi imposti dal DM sono condivisi e riconosciuti da tutti gli stake-holders? I controlli e le sanzioni da parte delle Autorità tutorie sul rispetto dei requisiti minimi sono applicati in tutta Italia allo stesso modo?

Qual è il rapporto tra servizi di vigilanza armata e servizi fiduciari?

**Questi sono i principali interrogativi sui quali i rappresentanti delle associazioni di categoria e dei sindacati del lavoratori si confronteranno, per comprendere quali potrebbero essere gli scenari prossimi venturi della categoria.**

*Invitati Rappresentanti del Ministero dell'Interno.*

## 17 MAGGIO ORE 10.00 · AGORÀ CONVITTO NAZIONALE

### I talk show di Security for Retail Forum (SRF)

Questa sessione di SRF riprende i temi di maggior attualità per la sicurezza dei PDV: la gestione intelligente e in sicurezza del denaro e la trasformazione della security da centro di costo a centro di profitto in due distinti momenti di esposizione e di confronto.

**1° talk show: Cash Management e Cash Handling, quali soluzioni per la gestione intelligente e sicura del denaro** con i rappresentanti dell'utenza, produttori di tecnologie e fornitori di servizi per confrontare le esigenze e le soluzioni per la messa in sicurezza degli esercizi commerciali sottoposti al rischio di reati predatori.

**2° talk show: Integrazione tra sistemi di loss prevention, gestione magazzino e inventari**, con una rassegna delle soluzioni viste a **Euroshop 2014** interpretate per il mercato italiano **del retail**.

#### PARTNER



#### ENTI PATROCINANTI



# Se crolla Internet, ovvero come far diventare freddo il caffè

**M**etti una domenica mattina di uscire presto a prendere il giornale, di tornare a casa con i cornetti appena usciti dal forno per la colazione e di goderti il momento in cui ti siedi a tavola, con una tazza di caffè caldo in una mano e l'altra per sfogliare le pagine della politica (uffa, che barba), della cronaca (ma per piacere!), dell'economia (non parliamone, almeno oggi) cercando di arrivare, con calma, allo sport. Ma prima di raggiungere gli anticipi del sabato e le prove della MotoGP, devi passare per le forche caudine delle pagine della cultura. E qui, tu che lavori nella sicurezza, ti devi fermare, in questa domenica di aprile.

Hai trovato un articolo dal titolo/cazzotto in faccia  
**“SE CROLLA INTERNET - La Rete ha ormai**

**miliardi di utenti. Troppi: il rischio di blackout è concreto. Per questo lo scienziato Dan Dennett lancia l'allarme e un piano per sopravvivere a un nuovo Medioevo”** (\*)

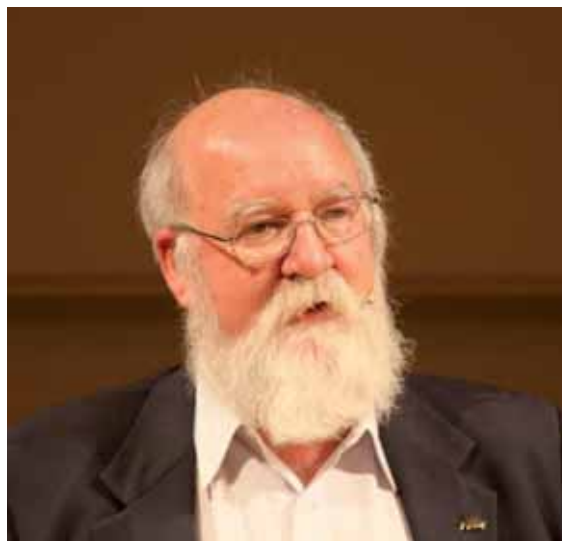
Sposti la tazza del caffè e leggi, il tema è troppo importante. Fra tutto, ti colpisce un'affermazione di Dennett: «La gente non si rende conto che oggi tutto dipende dalla rete, nessuna funzione vitale può continuare se si blocca Internet. Dappertutto si spegnerebbero tv e cellulari, si fermerebbero bancomat, supermercati, distributori di benzina. Ecco perché il maggior pericolo sarebbe il panico, il folle panico delle 48 prime ore, quando la gente non sa cosa fare, non ha notizie, non ha istruzioni, non ha mai fatto un'esercitazione per prepararsi».

Altro che cazzotto in faccia! Tutti i giorni arrivano in redazione comunicati che attestano le “meravigliose sorti e progressive” (\*\*) dei sistemi di sicurezza in rete, che permettono di far dialogare elementi eterogenei per dare informazioni organiche e unitarie a operatori remoti che devono gestire un attacco terroristico alla centrale elettrica, spegnere il principio d'incendio nel tunnel in autostrada, salvare la vita del cardiopatico telemonitorato, bloccare il rapinatore nella bussola della banca e altre simili amenità. Pensi anche alle tante app sviluppate negli ultimi tempi, per rendere più amichevole l'impianto di allarme di casa, per “smartfonizzarlo” almeno un po'...

Cerchi di pensare a cosa succederebbe a tutti quei sistemi di sicurezza se, improvvisamente, crollasse Internet. Molte difese cadrebbero e tanti malintenzionati potrebbero approfittare della situazione; molte persone si troverebbero “fuori” da un luogo nel quale non potrebbero entrare, forse tante quanto quelle rimaste “dentro” luoghi dai vorrebbero uscire eccetera, eccetera...

Ma poi pensi che gli effetti globali della caduta di Internet sarebbero talmente devastanti per il mondo intero, da far passare in secondo piano anche quelli sui sistemi di sicurezza che lavorano in rete.

A quel punto, giri pagina, arrivi allo sport. Riprendi la tazza del caffè, è diventato freddo.



(\*) Federico Rampini (La Repubblica, 13 aprile 2014); Daniel Clement Dennett, Direttore del Center for Cognitive Studies Tufts University - Boston

(\*\*) Giacomo Leopardi - La ginestra (v. 51)

## News

### INTERVISTA

- 8** Il ruolo degli standard per la crescita del mercato della sicurezza

### SCENARI

- 10** Euroalarm, il libro bianco della sicurezza europea - Ultima puntata

### EVENTI

- 15** La città come infrastruttura critica

### SCENARI

- 19** Cosa serve per la sicurezza delle IC?  
**20** Le recinzioni perimetrali - 1ª puntata  
**21** Chi forma i formatori? - 4ª puntata

### INTERVISTA

- 23** L'integrazione secondo Samsung Techwin

### EVENTI

- 24** Incontro concessionari e installatori autorizzati HESA

## Technologies

### SCENARI

- 26** "Insider attack": americanata o problema reale?

### INTERVISTA

- 30** Con Atik arriva la nuova distribuzione

### CASE HISTORY

- 34** Uno PSIM per Berco (ThyssenKrupp)

### INTERVISTA

- 38** Allegion, c'è del nuovo anzi di antico...  
**42** 4 Power Srl: sicurezza IP e innovazione  
**45** Lo storage secondo WD Purple

### CASE HISTORY

- 48** Sistemi integrati Eyeon di Videotrend al Golf Club di Manzano

### ZOOM PRODOTTO

- 50** Milestone - Axis  
**53** Siemens sbarra la porta agli intrusi con Magic Mirror  
**55** INT-TSI Tastiera Touch 7"  
Sicurezza e Domotica senza limiti con Satel  
**58** Da TSEC i più piccoli contatti magnetici di Grado 3 sul mercato

## Money

### INTERVISTA

- 60** La via di Mondiapol per la tutela delle banche clienti



**Dove trovi la sicurezza che cerchi**



## Goods

## CASE HISTORY

- 64** Milestone e AXIS insieme per la sicurezza di Paul Smith

## INTERVISTA

- 68** Il barometro dei furti nel retail offerto da Checkpoint

## SCENARI

- 70** Retail, come proteggere dispositivi, dati e reti con PCI - DSS 3.0

## Security Services

## INTERVISTA

- 74** ANIVP, quando le associazioni sono al servizio delle imprese

## SCENARI

- 76** Nemici per la pelle ma uniti contro il DM 269

## Fiere

## INTERVISTA

- 78** Medity Expò, lo snodo naturale per il centro-sud

## FIERE

- 82** Security Essen, la regina delle fiere della sicurezza
- 84** Sicurezza 2014 in crescita
- 86** Golfo e Medio Oriente a Dubai per Oil & Gas Security Summit
- 89** L'inconsapevolezza di oggi, la crisi di domani

REDAZIONALI TECNOLOGIE  
91-92-93-94

## in copertina...



Grazie al grande schermo touch da 7" INT-TSI assicura la comodità di gestione riservata finora soltanto agli smartphone e ai tablet. La possibilità di usare i widget interattivi sulla schermata permette con un solo tocco di comandare l'illuminazione, il riscaldamento, il sollevamento e l'abbassamento degli avvolgibili e perfino l'irrigazione delle piante.

Quando è necessaria l'autorizzazione di una operazione mediante la password dell'utente, al posto delle icone viene visualizzata la finestra con tastiera numerica per digitare la password e il sistema seleziona a sorte il posto della visualizzazione della tastiera, allo scopo di impedire di indovinare la password.

La funzionalità della nuova tastiera INT-TSI non consiste solamente nel comandare il sistema di allarme e i dispositivi dell'automazione: grazie alla possibilità di visualizzare le immagini delle videocamere digitali della sorveglianza, svolge la funzione di un vero centro di protezione, riunente le principali funzioni responsabili della sicurezza.

# Il ruolo degli standard per la crescita del mercato della sicurezza

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

## **Qual è il market share di ONVIF nel mercato globale della sicurezza fisica?**

È molto difficile per ONVIF misurare il market share perché lo scenario globale degli standard è molto complesso e frammentato. Misuriamo piuttosto il successo dal numero dei nostri membri che sono leader del mercato. Attualmente aderisce a ONVIF la maggioranza se non la totalità dei principali produttori del settore video IP, ai quali si stanno aggiungendo anche i maggiori produttori di controllo accessi.

## **Siete in grado di stimare la quota di mercato in Europa e in Italia?**

Se controllate la provenienza dei nostri associati, all'incirca un quarto viene dall'Europa. Una buona parte sono società globali che operano anche in Italia. A questo punto, circa la metà del totale dei nostri associati proviene dall'Asia e il rimanente 25% dalle Americhe.

## **Ci può descrivere il ruolo degli standard in una fase in cui sistemi eterogenei (videosorveglianza, controllo accessi, fire etc.) devono essere sempre integrabili?**

Se non ci fossero gli standard, il ritornello dei produttori sarebbe "costruiscilo una volta e non cambiarlo mai". Sistemi integrati costruiti con interfacce personalizzate tra prodotti specifici sono dipendenti dalla continuità del supporto di ogni singolo produttore, che deve mantenere e aggiornare le integrazioni. I sistemi disegnati in base a uno standard

di interfaccia comune di collegamento, tuttavia, saranno molto più longevi perché sono basati su una piattaforma condivisa che rimarrà costante per tutta la vita del sistema

Un sistema video costruito con NVR conformi a



ONVIF è un forum pubblico di settore creato allo scopo di sviluppare uno standard globale per l'interfaccia dei prodotti di sicurezza fisica IP-based, che ha come obiettivo in particolare di rendere interoperabili sistemi realizzati da aziende differenti.

La compatibilità si attua concretamente tramite la standardizzazione di:

- protocolli di comunicazione;
- rilevamento dei dispositivi;
- assegnazione degli indirizzi IP;
- controllo e configurazione dei dispositivi remoti;
- protocolli dei flussi audio-video;
- visualizzazione e registrazione dei flussi audio-video.

Gli obiettivi principali dell'organizzazione sono i seguenti:

- standard di comunicazione tra i dispositivi di sicurezza fisica IP-based;
- interoperabilità tra prodotti di sicurezza fisici IP indipendentemente dal produttore;
- adesione aperta a tutte le società e organizzazioni.

Fondato nel 2008 da Axis, Bosch e Sony, il forum si è subito imposto all'attenzione degli operatori del settore ed è oggi approvato da alcuni dei principali produttori al mondo di prodotti video IP.

L'organizzazione stabilisce delle specifiche (aggiornate periodicamente) a cui i produttori possono aderire volontariamente.

I dispositivi che rispettano le specifiche possono richiedere la certificazione ONVIF.

ONVIF e telecamere IP fisse, per esempio, potrà continuare a funzionare anche se le telecamere venissero sostituite da telecamere PTZ di un diverso produttore, purché conformi a ONVIF. Lo stesso vale anche per sistemi più complessi, con l'integrazione tra sistemi di controllo accessi e di videosorveglianza.

**Può spiegarci gli obiettivi del nuovo Profilo C?**

L'intento del Profilo C è portare la stessa interoperabilità attualmente goduta dal comparto video al settore del controllo accessi, tradizionalmente più chiuso. Abilitando un'interfaccia comune di collegamento tra una piattaforma di gestione del controllo accessi e una varietà di sensori di porta over IP e lettori di badge di costruttori diversi, la vedremo diventare il driver di una continua evoluzione tecnologica e dell'arrivo

di nuovi player nel settore del controllo accessi.

**In termini legali, formali e sostanziali, quali sono le differenze tra standard privati come ONVIF e le norme emessi da organismi pubblici come ISO o CEN/CENELEC?**

Sul piano formale, ONVIF è un'alleanza tecnica che produce de facto standard che vengono utilizzati dai produttori su base volontaria. In genere, sono le dinamiche del mercato – la domanda o la popolarità – che portano ad adottare questi standard. Le norme emesse da organismi come ISO o CEN/CENELEC o altri enti che determinano i requisiti dei sistemi di rilevazione incendi, elettrici o salvavita per un particolare paese o giurisdizione, esprimono più spesso i requisiti legali per la sicurezza delle persone voluti da quella giurisdizione.



# Euroalarm, il libro bianco della sicurezza europea

## Ultima puntata

a cura di Cristina Isabella Carminati

**N**ella primavera del 2013 EUROALARM 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 EUROALARM 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. In questo numero presentiamo l'ultima parte del documento tradotto in italiano. Il pdf dell'originale in lingua inglese è postato in [www.securindex.com/library](http://www.securindex.com/library)

### 3. Garantire i massimi livelli di security e sicurezza antincendio per tutti

Il maggiore interesse pubblico europeo riguardante i prodotti e i servizi antincendio e di security riguarda la fornitura di soluzioni affidabili, che tutelino la vita e la proprietà, e la possibilità di funzionamento sociale e di resilienza. A questo proposito, esaminando in generale l'attuale agenda dell'UE al di fuori della politica industriale per il settore della sicurezza, Euralarm ritiene che vi siano diverse aree nelle quali esiste una sicura opportunità di migliorare la safety e la security dei cittadini UE a breve termine, in particolare:

- allarmi pubblici e notifiche di massa;
- sicurezza antincendio degli alberghi;

- efficienza energetica e ristrutturazione degli edifici.

### A. Utilizzo dei sistemi di security e antincendio per gli allarmi pubblici e notifiche di massa per raggiungere più cittadini

Gravi eventi che mettono a rischio la vita e la proprietà su larga scala in genere richiedono l'intervento delle autorità di protezione civile, che a loro volta si affidano a una serie di allarmi pubblici e privati, comunicazioni e servizi di intervento per rispondere in modo efficace a tali eventi. Euralarm sostiene pertanto la Commissione europea nel suo sforzo di installare un sistema di allarme pubblico paneuropeo.

I vari progetti di ricerca nell'ambito del Settimo programma quadro (7° PQ) stanno evidenziando argomenti quali l'allerta alla popolazione su vasta scala se si verifica un incidente, noto anche come sistema di allarme pubblico, grazie al quale la popolazione è informata da una serie di comunicazioni, tradizionalmente tramite i media radiotelevisivi.

Anche i settori privato e pubblico hanno predisposto sistemi di notifiche di massa, che forniscono informazioni e istruzioni alle persone in tempo reale in un edificio, area o installazione tramite comunicazioni vocali intelligibili e segnali visibili, testi e grafica.

Sulla base della sua lunga esperienza nell'allertare e guidare l'evacuazione delle persone dalle zone pericolose negli edifici, il settore industriale rappresentato da Euralarm può dare un considerevole contributo a questo importante sforzo.



Pertanto Euralarm si è impegnata, in collaborazione con il progetto 7° PQ “Alert4All”, a dimostrare la possibilità dell’integrazione dei sistemi di safety & security nonché dei sistemi di notifica di massa e di allarme pubblico. Il progetto dimostrativo Euralarm PEARS (Public Emergency Alert & Response System) sarà illustrato nel quarto trimestre del 2013 insieme alla “Alert4All”. Sulla base dell’esperienza vissuta negli Stati Uniti, Euralarm è fiduciosa che la dimostrazione sarà un successo.

Attualmente soltanto pochi paesi europei hanno adottato normative in questo campo. Sebbene le dimostrazioni e altri progetti abbiano diffuso best practice e protocolli, ciò non è sufficiente. I tempi sono maturi per adottare standard paneuropei per una soluzione comune e quindi integrata sia per le notifiche di massa che per i sistemi di allarme pubblico.

**B. Migliorare la safety per milioni di viaggiatori tramite una direttiva europea sulla sicurezza antincendio degli alberghi**

La Commissione europea sta attualmente riesaminando la Council Recommendation on fire safety in existing hotels del 1986. Così com’è questo strumento non crea obblighi giuridici vincolanti per i governi degli Stati membri o per proprietari di hotel/operatori. Ma la consultazione della Commissione sulla sua possibile revisione ha generato una vasta gamma di osservazioni e pareri sulla fattibilità e l’opportunità di una revisione delle raccomandazioni, che ha portato la Commissione europea ad ammettere l’assenza di un consenso sulla via da seguire per migliorare la sicurezza antincendio negli alberghi. Di fronte a questa situazione la Commissione europea ha deciso di estendere la fase di consultazione sulla sicurezza antincendio degli alberghi e di includere la sicurezza antincendio in un Green Paper sulla safety dei servizi previsto per il 2013.

Euralarm deplora il ritardo nella messa in sicurezza di tutti coloro che viaggiano nell’Unione europea ed è pronta a collaborare con la Commissione e le altre parti interessate per accelerare il processo e giunge-

re a conclusioni soddisfacenti.

Euralarm crede ancora che soltanto il passaggio a requisiti giuridicamente vincolanti a livello UE potrà garantire un adeguato livello di safety negli alberghi. A questo proposito Euralarm si è anche impegnata a sostenere attivamente lo sviluppo degli standard necessari a conformarsi a un futuro strumento giuridico. Per tali caratteristiche tecniche, gli organismi di normalizzazione CEN e CENELEC sarebbero i più adeguati a coordinare i contributi delle parti interessate.

### **C. Ristrutturazione degli edifici: un'opportunità per migliorare la security e la protezione antincendio**

Ai sensi della Direttiva UE sul rendimento energetico degli edifici (EPBD/2010/31/EU) e della Direttiva sull'efficienza energetica più recentemente adottata (EED/2012/27/EU), un gran numero di edifici - tra questi molti pubblici - sarà ristrutturato per migliorarne l'efficienza energetica. Ciò è un'opportunità per il miglioramento della safety e della security.

Per soddisfare i requisiti della legislazione UE, la ristrutturazione degli edifici dovrebbe tenere conto delle esigenze di security e sicurezza antincendio, al

fine di garantire la migliore protezione possibile.

- La natura di questo lavoro apre la possibilità di ripensare anche le strategie di sicurezza e di aggiornare simultaneamente gli allarmi antincendio e altri sistemi a costi inferiori.
- D'altra parte tale ristrutturazione non può essere autorizzata se come conseguenza si ha lo smantellamento parziale o totale dei vecchi sistemi di sicurezza senza la loro sostituzione.

In questo contesto Euralarm si aspetta da parte delle autorità policy-making che il livello attuale di protezione degli edifici sia mantenuto o migliorato, anche nel caso di una ristrutturazione EPBD (Energy Performance of Buildings Directive, NdR).

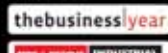
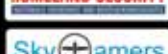
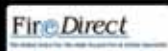
Oltre alle raccomandazioni sopra indicate, le seguenti azioni possono portare e un ulteriore sviluppo dell'industria antincendio e della security.

### **4. La responsabilità illimitata verso terzi è una minaccia per la tecnologia innovativa**

Le società europee di security hanno sperimentato il problema della limitazione delle responsabilità negli USA dopo gli attacchi terroristici dell'11 settembre. Poco dopo, gli appaltatori del governo



Supporting Associations



THE  
 EMERGENCY MANAGEMENT &  
 CRISIS RESPONSE SUMMIT  
 MIDDLE EAST

DAY 1



AVIATION

DAY 2



INFRASTRUCTURE

DAY 3



OIL & GAS

10<sup>th</sup> - 12<sup>th</sup> June 2014 in Dubai, U.A.E.

non hanno più potuto accettare il grave rischio di diffusione delle tecnologie della security e formule offerte per i contratti correlati, dato che ciò costituiva una potenziale minaccia per le aziende. Come risposta a questo problema il governo degli Stati Uniti ha promulgato la Safety Act (Support Anti-terrorism by Fostering Effective Technologies Act). Il Safety Act assicura che ci sia un'adeguata assicurazione per compensare legittime rivendicazioni. Questa protezione non è limitata alle società statunitensi sebbene sia valida soltanto all'interno del sistema giudiziario americano. L'Unione europea non ha ancora affrontato la questione. La mancanza di una protezione delle responsabilità simile in Europa contribuisce a una base industriale più debole, ostacola gli investimenti e riduce la distribuzione di nuove e innovative tecnologie e servizi di security in Europa.

A questo proposito Euralarm accoglie con favore l'iniziativa della Commissione di trovare soluzioni a queste lacune. In qualità di fornitori di soluzioni di security, abbiamo tutto l'interesse a proteggere i cittadini e la società, incoraggiando allo stesso tempo l'innovazione e la diffusione di tecnologie che affrontino le attuali minacce. Euralarm raccomanda di considerare il rispetto degli standard EN come quadro di riferimento per la valutazione dei contenziosi in materia di 1) responsabilità verso terzi, 2) responsabilità per l'interoperabilità del sistema, e 3) responsabilità per l'integrità del sistema.

## 5. Promozione dei prodotti e servizi di safety

È di vitale importanza per lo sviluppo di una vivace industria europea della security che il mercato globale della security rimanga aperto e accessibile. Molti dei più importanti player europei sviluppano una quota significativa della propria attività al di fuori dell'UE. Questa diversificazione consente di coprire i costi di sviluppo e genera economie di scala per

le imprese interessate. L'UE dovrebbe, quindi, fare pieno uso delle sue politiche commerciali per mantenere e, ove possibile, migliorare l'accesso al mercato internazionale attraverso l'apertura reciproca, il riconoscimento e la standardizzazione dei prodotti e di tutte le modalità dei servizi.

Considerazioni di politica commerciale:

- riduzione delle tariffe sui prodotti per la safety;
- promozione degli standard EN a livello internazionale;
- richiesta di valutazioni della performance negli appalti pubblici in modo che

le apparecchiature debbano soddisfare i criteri evidenziati nelle richieste di offerta.

L'esportazione di prodotti e servizi di safety di altissima qualità contribuirà alla crescita dell'industria e dell'occupazione.

## 6 . La strada da percorrere

Come è stato ripetutamente affermato in questo White Paper, vi è un urgente bisogno di un cambiamento di rotta: da

un approccio nazionale delle politiche di security a un approccio europeo e internazionale.

È certamente soltanto attraverso un'azione a livello comunitario che saremo in grado di affrontare la frammentazione endemica che sta attualmente minando il potenziale di crescita e la competitività dell'industria europea della security. Affrontare questo problema andrà a beneficio della società europea nel suo insieme, tenendo conto del valore sociale dei prodotti e dei servizi di security, che consiste nella tutela della vita e della proprietà che essi forniscono. Il cammino verso un vero e proprio mercato interno europeo per la security e un'industria europea della security realmente competitiva a livello mondiale è appena iniziato e c'è molto lavoro da fare. Euralarm guarda avanti per contribuire a questo ambizioso sforzo e lavorare a stretto contatto con tutte le parti interessate per aiutarle a trovare la strada da percorrere.





# La città come infrastruttura critica

di Barbara Ferraris di Celle – Co-founder Reputation Agency

**C**on il Patrocinio del Senato della Repubblica e della Camera dei Deputati, nella splendida cornice del Palazzo dei Gruppi Parlamentari, a Roma, si è svolto il 25 marzo il convegno “La città come infrastruttura critica”, organizzato dall’Associazione HI CARE, da AIAS Security & Safety, dall’ANMIL e dalla Fondazione Italiana per la Legalità e lo Sviluppo. L’importante consesso è stato caratterizzato da un parterre eccezionale e dalla testimonianza di Joseph F. Bruno, Commissioner Office of Emergency Management di New York.

Il convegno intendeva sottolineare l’importanza dell’interazione tra pubblico e privato nella prevenzione e nella gestione di eventi critici, in particolare in quelle città, come Roma o Milano, in cui una crisi può provocare danni a livello sistemico e che pertanto devono essere tutelate come infrastrutture critiche.

Per gestire i rischi in modo efficace e costruire la resilienza ai loro impatti, sono necessari sforzi maggiori per

comprendere, misurare e prevedere l’evoluzione delle interdipendenze, integrando gli strumenti tradizionali di gestione dei rischi con nuovi concetti pensati per ambienti incerti. La cooperazione tra pubblico e privato, la condivisione delle informazioni, la semplificazione delle norme e la definizione di regole chiare in tema di security, sono alcuni degli elementi da porre in campo per garantire la sicurezza nelle città, a partire da Roma. La prima parte del convegno è stata coordinata da Giuseppe Fausto Milillo, Presidente della Fondazione Italiana per la Legalità e lo Sviluppo, che ha sottolineato come in questo momento di crisi sia ancor più importante parlare di sicurezza e lotta alla criminalità nelle città.

Significativi gli interventi in apertura di Rossella Matarazzo, Vice Capo di Gabinetto con delega alla Sicurezza del Comune di Roma e di Gianna Detoni, Presidente Hi Care, che hanno sottolineato l’importanza della condivisione di informazioni e della cooperazione tra pubblico e privato, auspicando che Roma sia soltanto



Gianna Detoni



*Giuseppe Fausto Milillo e Gianna Detoni*

la prima città di una lunga serie in cui vengono trattati i temi della security dei territori e della città come infrastruttura critica.

Joseph F. Bruno, Responsabile dell'OEM di New York, ha illustrato come vengono gestite le emergenze nella città di New York e ha descritto il modello di partnership pubblico/privato per la gestione delle emergenze, la prevenzione dei rischi e il mantenimento della sicurezza nella città. Dopo la sua nomina avvenuta nel mese di aprile 2004, Bruno è stato incaricato dall'allora sindaco Michael Bloomberg di creare e implementare il Sistema di Gestione Citywide Incident (CIMS), che ha definito ruoli e responsabilità per la città, lo stato, gli enti governativi, le organizzazioni non-profit, il settore privato e tutti quei soggetti coinvolti nella gestione e nella risposta alle emergenze. Oggi CIMS è ormai lo standard di NYC universalmente accettato per rispondere e gestire le crisi. Il commissario Bruno, nel presentare il modello dell'Office of Emergency Management di New York City, ha più volte ribadito l'importanza della partnership con il settore privato, che va inserito all'interno del Comitato di Crisi della città e coinvolto in tutte le fasi della pianificazione di emergenza, preparazione, risposta e recupero. Organizzare la prevenzione, effettuare test sul territorio che coinvolgano anche i privati e coordinare le aziende sui comportamenti da tenere in caso di crisi, sono attività fondamentali per garantire la sicurezza della cittadinanza e delle infrastrutture territo-

riali. A questo proposito Joseph F. Bruno ha dichiarato: «Ho insistito molto sull'importanza della prevenzione e del dialogo costante tra enti governativi e privati. Dopo l'11 settembre abbiamo realizzato chiaramente che è necessario preparare la cittadinanza a eventi critici e che uno degli strumenti più efficaci per raggiungere questo scopo è decisamente la partnership pubblico-privato. Per questo motivo a New York i rappresentanti del tessuto economico e sociale della città partecipano con noi alle esercitazioni e - durante una crisi - hanno accesso alle stesse informazioni che ho io, nello stesso momento. Pianificare e sfruttare le sinergie con il settore privato aiuta a reagire meglio e a garantire un ritorno alla normalità molto più rapido dopo un'emergenza. Coinvolgere i privati è fondamentale e necessario».

New York è una città complessa dove le emergenze - sia naturali che causate dall'uomo - sono purtroppo comuni, come dimostrano le numerose crisi che si sono verificate nel corso degli ultimi dieci anni. La città è composta da 8,3 milioni di abitanti per una superficie di 302 chilometri quadrati su tre isole e una penisola. I canali di comunicazione utilizzati abitualmente dall'Office of Emergency Management - compresi i social media, le notifiche di emergenza, le chiamate in conferenza con i numerosi partner del settore privato e la tradizionale divulgazione via mass-media - permettono all'agenzia di condividere le informazioni e fare sistema contro la crisi.

# BMHP



DIGI  
TAL

## Loro dialogano, il tuo cliente sta sicuro.



Falsi allarmi addio. Da oggi prova le BM HP, l'avanzata gamma di barriere digitali da esterno con portata variabile da 60 a 200 metri che AVS Electronics ha creato per le tue esigenze di sicurezza. Pratiche da installare, flessibili da utilizzare, le BM HP sono veramente uniche, con la loro innovativa funzione WIND UP, che ti permette di modulare come vuoi l'area protetta, senza preoccuparti delle interruzioni accidentali. E per te che non ami i compromessi, le BM HP offrono la speciale funzione "scandaglio", che ti permette di rilevare l'intruso a grande distanza. BM HP: quando loro dialogano, la sicurezza è garantita.

100%  
MADE IN ITALY

**AVS electronics**® AVS ELECTRONICS S.p.A. Via Valsugana, 63, 35010, Curtarolo, (PD), Italy.  
Tel. +39049 9698 411 - Fax +39049 9698 407 avs@avselectronics.com www.avselectronics.com



Stimolati dalla relazione di Joseph Bruno, i protagonisti della successiva tavola rotonda hanno sollevato interessanti spunti di riflessione.

Il Senatore Giuseppe Marinello, Presidente Commissione Territorio, Ambiente e Beni Ambientali del Senato, ha centrato il suo intervento sul ruolo fondamentale che gioca il cittadino consapevole dell'impatto di ogni sua azione sul territorio e sugli altri. I rischi che devono essere quotidianamente fronteggiati in una città come Roma derivano non solo dalle calamità naturali ma anche dall'azione dell'uomo (attività criminose e non). Fabrizio Curcio, Direttore dell'Ufficio di Gestione delle Emergenze del Dipartimento di Protezione Civile Nazionale, ha invece individuato nelle tecnologie, nelle risorse e nelle normative i tre elementi fondamentali che devono necessariamente sussistere per poter procedere nella collaborazione tra pubblico e privato.

Domenico Vulpiani, Coordinatore del Centro Elaborazione Dati Ministero dell'Interno ha parlato specificamente della città di Roma, delle sue criticità e delle modalità con le quali viene garantita la continuità operativa delle infrastrutture in situazioni di emergenza, anche grazie alla cooperazione con le aziende che si occupano di *security*.

Significativa anche la presenza delle aziende: Pierluigi Pelargonio, Responsabile Vigilanza e Security di ATAC S.p.A., Tommaso Profeta, Responsabile Security di Finmeccanica S.p.A., Umberto Saccone, Corporate Security Officer di ENI S.p.A. e Damiano Toselli, Corporate Security Officer di Telecom Italia S.p.A.

Elemento comune a tutti gli interventi è la consapevolezza della necessità di creare modelli di collaborazione fra soggetti privati e soggetti pubblici che si occupano

di *security*. La condivisione di conoscenze e di informazioni consente, con risorse ottimizzate, un risultato migliore nel prevenire i rischi e garantire la sicurezza nell'ambito delle infrastrutture critiche.

Soddisfatti gli organizzatori della manifestazione. Gianna Detoni, Presidente dell'Associazione HI CARE, ha dichiarato: «L'opinione dell'Associazione HI CARE è che città come Roma e Milano - per citare soltanto due esempi - debbano essere considerate delle vere e proprie infrastrutture critiche, da proteggere e tutelare in modo particolare per evitare danni al Sistema Paese. Il nostro modello di riferimento è l'Office of Emergency Management di New York City, che nella propria mission cita esplicitamente la partnership tra pubblico e privato quale strumento di prevenzione delle crisi sul territorio. L'Istituzione che in Italia ha fatto di più in questo senso è sicuramente il Dipartimento di Protezione Civile, ma troppo spesso quando si parla di aziende chiamate a partecipare ai tavoli di coordinamento ci si riferisce solo alle public utilities. Con questo convegno invece abbiamo provato ad affrontare il tema in maniera più ampia: all'appello mancano ancora diversi attori del settore privato, bisogna migliorare la comunicazione tra pubblico e privato ed è necessario attivare una collaborazione costante, soprattutto nella fase di preparazione alle crisi. L'Associazione HI CARE si propone quindi di discutere di questi temi per realizzare qualcosa di simile all'Office of Emergency Management di New York nelle principali città italiane, adattando il modello alle caratteristiche del nostro tessuto economico e sociale. Solo così saremo in grado di esercitare al meglio la prevenzione, che è il miglior strumento di gestione di una crisi sul territorio».



Gianna Detoni e Joseph F. Bruno

# Cosa serve per la sicurezza delle IC?

a cura della Redazione



**L**a quantità e la diversità dei siti e delle strutture fisiche (per esempio centrali elettriche, ferrovie, aeroporti, gasdotti, server farm etc.) o virtuali come internet, la pluralità dei rischi a cui sono esposte (incidenti industriali, calamità naturali, azioni volontarie a fini terroristici o predatori) e soprattutto l'importanza strategica che rivestono per la politica, le economie, l'ambiente e la salute dei componenti delle comunità alle quali afferiscono, fanno sì che, a livello globale, le **Infrastrutture Critiche (IC)** rappresentino uno dei più importanti capitoli per la sicurezza nazionale di ogni singolo paese.

Nel decennio 1996-2006 sono stati registrati oltre

2500 attentati in tutto il mondo, riconducibili direttamente o indirettamente a organizzazioni terroristiche ma, storicamente, hanno provocato molti più danni alle IC gli incidenti e le calamità rispetto agli atti volontari, con esclusione delle guerre. Pensando soltanto alle centrali nucleari, le IC per eccellenza dell'era moderna, **Three Mile Island** (USA, 1979), **Chernobyl** (URSS, 1986) e **Fukushima** (Giappone, 2011) sono luoghi che l'immaginario collettivo ha memorizzato come sinonimi di disastro assoluto.

Tutto ciò ha causato l'aumento progressivo degli investimenti per la sicurezza delle IC da parte dei governi di tutti i Paesi, facendo ricorso alle più avanzate soluzioni tecnologiche e alle migliori competenze di risk management. Di conseguenza, le IC costituiscono la più ampia palestra di esercitazione delle conoscenze in sicurezza, in ogni sua declinazione: safety, cyber security, physical security, fire.

**Essecome security & safety** inizia da questo numero una rassegna di tecnologie applicate alla IC, presentando analisi, case history e approfondimenti, ospitando il contributo di aziende leader nei rispettivi ambiti, per offrire ai professionisti che si occupano dell'argomento informazioni e spunti di approfondimento.

La prima puntata è dedicata alle recinzioni perimetrali intelligenti e l'ospite è **DEA Security**.



# Le recinzioni perimetrali

## 1<sup>a</sup> puntata

di Alessandro Del Rosso – DEA Security

I sistemi antintrusione per recinzioni prodotti da DEA Security fanno parte di quelle protezioni perimetrali elettroniche che, come detto, rivestono oggi un ruolo sempre più importante nella sicurezza multi-strato delle IC. I sistemi DEA si trovano installati in diverse IC italiane ed estere, tra le quali si annoverano centrali elettriche, complessi petrolchimici e aeroporti.

Alcuni recenti progetti che contemplano l'impiego dei sistemi DEA Security consistono nella protezione perimetrale di siti ad alto rischio con perimetri anche molto estesi. Tra questi progetti c'è anche quello di un importante aeroporto internazionale d'oltreoceano, per la protezione della cui recinzione è stato proposto il sistema antintrusione con intelligenza distribuita SERIR P2P.

SERIR P2P impiega speciali rivelatori piezodinamici che, dotati di unità di analisi integrata e protetti da un involucro in poliammide, si installano direttamente sul pannello di rete per mezzo di un sistema di fissaggio antirimozione. I sensori percepiscono le vibrazioni a cui è sottoposta la recinzione durante un tentativo di intrusione, discriminando tra differenti tipi di attacco: taglio, arrampicamento e sfondamento della struttura. Ciascun sensore è univocamente identificato, così da permettere la precisa individuazione del punto in allarme, e include dispositivi contro le manomissioni termiche e magnetiche.

Ciò che ha portato lo studio di progettazione dell'aeroporto a prendere in considerazione SERIR P2P è soprattutto la sua elevata immunità ai disturbi ambientali, come quelli generati da condizioni climatiche avverse, brusche variazioni termiche o automezzi in manovra, la compatibilità con la vegetazione, che in certi tratti del perimetro lambisce o avvolge (piante rampicanti) la recinzione e



la capacità di coprire fino a 1.500 metri di perimetro (per un totale di 500 sensori) con una sola unità di controllo, riducendo al minimo l'infrastruttura di cablaggio in campo.

L'altro fattore determinante è stata la possibilità di proteggere, grazie ad apposite appendici in metallo, anche la concertina che sormonta la recinzione per la sua intera lunghezza.

Nel progetto, SERIR P2P si integrerà con il sistema di videosorveglianza IP sia a livello di rete fisica, condividendo le fibre ottiche già in campo, sia a livello di software di supervisione: in caso di allarme, il software DEA MAP sfrutterà le informazioni fornite dai rivelatori sulla recinzione per attivare automaticamente le telecamere di pertinenza. Tramite speciali moduli I/O, SERIR P2P potrà inoltre raccogliere le segnalazioni provenienti da altri dispositivi di terze parti, quali per esempio i contatti magnetici dei cancelli.

# Chi forma i formatori?

## 4<sup>a</sup> puntata

*a cura di Cristina Isabella Carminati*

Essecome continua 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.

In questa terza puntata incontriamo AVS Electronics e Samsung Techwin.

*a colloquio con Fabio Baro, Amministratore Delegato AVS Electronics  
a cura di Cristina Isabella Carminati*

### **Quali sono gli obiettivi della proposta formativa di AVS?**

AVS è stata tra le prime aziende italiane ad aver proposto un calendario di formazione mirata alle esigenze del professionista della sicurezza. Una scelta, parliamo degli anni '70-'80 del secolo scorso, che nasceva dalla consapevolezza dell'arretratezza della formazione in questo settore. Da allora, ovviamente, molte cose cambiate e anche gli obiettivi della proposta formativa si sono evoluti e affinati. Oggi il nostro focus è quello di far conoscere tutte le potenzialità e quindi offrire un'elevata preparazione su tutte le caratteristiche dei nostri prodotti. Per un'azienda produttrice e distributrice come AVS il vero patrimonio da coltivare è un cliente informato e aggiornato, capace di far proprie tutte le innovazioni che il prodotto offre, sfruttando a pieno le sue caratteristiche. Il cliente che frequenta i nostri corsi è dunque sicuro di ottenere almeno tre vantaggi: è vincente quando fa la proposta commerciale al proprio cliente perché conosce nel dettaglio ciò che va a proporre, è sicuro di utilizzare i prodotti sfruttandone al massimo le caratteristiche e, avendo ricevuto un'opportuna formazione, risparmia riducendo i costi di installazione e di intervento.

**I vostri corsi sono rivolti solamente ai clienti AVS (concessionari, installatori autorizzati) o sono**



### **aperti a tutti gli operatori?**

I corsi sono riservati esclusivamente a clienti AVS perché intendiamo, così, non soltanto fidelizzare il rapporto con l'azienda ma contribuire anche ad aumentare il valore aggiunto che ogni nostro cliente può offrire al mercato.

**Organizzate corsi anche in collaborazione con enti di normativi o di certificazione?** Fino a oggi, per la tipologia di corsi attivati, abbiamo utilizzato principalmente formatori aziendali di grande esperienza tecnica e operativa, visto che molta della

formazione erogata è pratica. In questo momento stiamo comunque valutando la possibilità di attivare alcune collaborazioni esterne con enti normativi o di certificazione.

## Che tipo di attestati vengono rilasciati al termine

*a colloquio con Carmen Palumbo, Marketing Executive Italy & France Samsung Techwin Europe Limited  
a cura di Cristina Isabella Carminati*

### Quali sono gli obiettivi della proposta formativa di Samsung Techwin per il 2014?

Visto il successo del corso "Introduzione alla VideoSorveglianza IP Samsung", Samsung Techwin ha pensato di trasformare il training rendendolo itinerante, organizzando una serie di giornate formative, in collaborazione con i Distributori Certificati Samsung Techwin.

La giornata di corso, completamente gratuita, vuole dare una panoramica sulle soluzioni IP di VideoSorveglianza di Samsung e fornire le nozioni necessarie per progettare, installare e configurare, in modo corretto, sistemi basati su tecnologia IP Full HD. Il target di riferimento è rappresentato da tecnici installatori professionisti.



### dei corsi?

Viene rilasciato un certificato di partecipazione che indica i temi approfonditi dal corsista. Un certificato che risulta obbligatorio conseguire e ogni anno rinnovare nel caso l'installatore faccia parte del progetto "Installatore di Qualità Certificato AVS".

### Quali sono le date e le sedi dei vari appuntamenti di questo "Samsung in tour"?

Le date (a oggi pianificate) e le città/zone in programma sono:

- 2 aprile > Roma
- 3 aprile > Milano
- 15 aprile > Verona
- 13 maggio > Palermo
- 14 maggio > Palermo
- 29 maggio > Chieti
- 3 giugno > Ascoli Piceno
- 5 giugno > Napoli
- 1 luglio > Roma
- 3 luglio > Padova

### Sono previsti incontri anche presso la sede di Milano?

Samsung Techwin ha messo a calendario due giornate di approfondimento tecnico sulle nuove soluzioni per la VideoSorveglianza IP Full HD c/o la sede di Milano. Con l'introduzione delle nuove telecamere IP Full HD della famiglia WiseNetIII, oggi è ancora più semplice e immediato poter realizzare un sistema di VideoSorveglianza con immagini di qualità e servizi di analisi video e audio più accurati. Durante la giornata sarà illustrata anche la piattaforma Samsung Security Manager (SSM) che consente una gestione integrata di telecamere IP, NVR e DVR analogici sotto un unico sistema. Le prossime date disponibili sono il 22 maggio e il 26 giugno. Come parte del Samsung Smart Partner Programme, abbiamo inoltre organizzato un programma di training (Samsung IP Institute-SIPI) sulle tematiche della VideoSorveglianza IP targata Samsung. Il training, della durata di 2 giorni, è indirizzato a personale con skill tecnico, e, per i nostri Partner Certificati, è rilasciato a titolo gratuito. Le prossime date disponibili sono 8/9 maggio e 9/10 giugno.



# L'integrazione secondo Samsung Techwin

*a colloquio con Fabio Andreoni, Country Manager Samsung Techwin Italy  
a cura della Redazione*

**Samsung Techwin è uno dei leader globali del mercato della videosorveglianza. Qual è la vostra visione, in termini di tendenze tecnologiche, nel breve/medio periodo?**

La nostra vision si basa su 4 elementi fondamentali che guidano lo sviluppo delle nostre soluzioni: qualità dell'immagine, ottimizzazione delle risorse, facilità d'uso e flessibilità di integrazione. I quattro "pillars" rispondono perfettamente al nostro intento di offrire ai nostri utenti un "Total Cost of Ownership" interessante e adeguato ai budget disponibili. Nel 2014 tutto ciò è enfatizzato anche dalle partnership tecnologiche in essere con i partner VMS, che ci consentono di fornire flessibilità e possibilità di scelta ai nostri Clienti.

**Accanto al processo di migrazione dai sistemi analogici a quelli in rete, è partito il processo di integrazione intersistemica, con tecnologie in grado di ottimizzare la gestione dei dati, come VMS e PSIM. Come vi proponete a questo proposito?**

La migrazione da tecnologie analogiche a tecnologie IP è in corso ed è ormai un processo consolidato. I due ambiti coesistono e offrono, con caratteristiche diverse, opportunità di business interessanti. Samsung prosegue nello sviluppo anche di prodotti innovativi per il mercato analogico, sfruttando novità tecnologiche che offrono maggiore qualità rispetto al passato. In Samsung crediamo fermamente al concetto di partnership con altri operatori di mercato per offrire soluzioni sempre più integrate e funzionali. Ci saranno importanti novità da questo punto di vista che saranno annunciate nel prossimo futuro.

**Un altro mega-trend a livello globale è l'integrazione tra prodotti e servizi (SaaS e VsaaS).**

I tempi sono maturi per queste applicazioni e per posi-



zionare videosorveglianza e sicurezza fisica in generale in modo diverso rispetto al passato, più come servizio che come acquisto di un bene. Le tecnologie che Samsung mette a disposizione si sposano perfettamente per operare anche in questi ambiti.

**Quali tipologie di prodotto prevedete di presentare nel mercato italiano nel 2014?**

La nostra mission è basata sull'impegno di portare sul mercato prodotti che rispondano ai nostri quattro cardini della nostra vision. Tutti i nuovi prodotti del 2014 rientrano all'interno di questa filosofia. Elencarne ora i dettagli sarebbe un po' dispersivo, ma in generale possiamo anticipare che abbiamo lavorato sull'aumento della qualità delle immagini e delle risoluzioni e sul concetto di Open Platform già anticipato nelle risposte precedenti. Nel 2014 abbiamo anche lavorato per consolidare la partnership con il nostro canale, ottimizzando la politica commerciale e distributiva. Oggi possiamo contare su una rete sul territorio ben radicata, capillare e in grado di offrire servizi di eccellenza. Stiamo allargando il nostro team, con l'inserimento di nuove figure professionali per supportare i nostri obiettivi di crescita, che, come da DNA della nostra azienda, sono sempre ambiziosi e competitivi.

# Incontro concessionari e installatori autorizzati HESA

*a cura della Redazione*

**T**orna il 27 maggio prossimo a Villa La Valera di Arese l'appuntamento annuale dei concessionari e degli installatori autorizzati HESA, la rete dei migliori professionisti italiani della sicurezza che, in continua espansione, è oggi composta da 187 aziende: 74 concessionari e 113 installatori autorizzati.

Questi professionisti sono in grado di distinguersi ogni giorno nel mercato della sicurezza e di soddisfare al meglio le esigenze degli utenti finali con soluzioni studiate su misura, avvalendosi delle migliori tecnologie oggi disponibili e favoriti dai servizi esclusivi offerti loro da HESA. Per l'Incontro Nazionale del 2014, nel 40° anniversario del passaggio dalla storica Ditta Individuale Enzo Hruby a HESA S.p.A., l'azienda ha in

serbo per i concessionari e gli installatori autorizzati interessanti nuovi prodotti che si vanno ad aggiungere a quella che è la più completa offerta di sistemi professionali per la sicurezza antintrusione, la videosorveglianza e l'antincendio. Uno in particolare, progettato per rispondere con la massima affidabilità alle particolari esigenze di sicurezza del mercato italiano, verrà reso disponibile in esclusiva per i Concessionari e gli Installatori Autorizzati proprio in occasione dell'Incontro Nazionale. Oltre alle novità di prodotto, come di consueto questo appuntamento è anche l'occasione per fare un bilancio dell'attività, presentare le prospettive per il futuro in un mercato in costante evoluzione e riunire in un clima sereno e conviviale i più qualificati professionisti della sicurezza.





[www.hesa.com](http://www.hesa.com)

È sempre  
più difficile  
rimanere competitivi

# **DIVENTA INSTALLATORE AUTORIZZATO HESA**

Scopri i vantaggi di appartenere al più esclusivo gruppo di professionisti della sicurezza:  
HESA S.p.A. - Via Triboniano, 25 - 20156 MILANO - Tel. 02.380361 - [www.hesa.com](http://www.hesa.com)

# “Insider attack”: americanata o problema reale?

*Luca Salgarelli, Presidente e Amministratore Delegato TSEC*

**L**a progettazione dei sistemi anti-intrusione o, più correttamente, di un allarme antifurto prevede sempre una definizione di rischio basata sulla divisione dello spazio in zone d’azione. Ad alto livello, tali zone sono l’area da proteggere (zona interna), e la zona a essa complementare, ovvero quella esterna, con un perimetro a fungere da confine tra le due.

Nei casi più semplici, per esempio negli impianti residenziali medio/piccoli, questo tipo di architettura è già sufficiente per definire la struttura dell’impianto, con dispositivi funzionali alla protezione perimetrale (barriere, contatti magnetici, sensori inerziali, etc.),

spesso coadiuvati, almeno negli impianti più importanti, da dispositivi complementari che proteggono la zona interna (sensori volumetrici, etc.).

L’architettura degli impianti più complessi, come quelli dedicati alla protezione dei centri commerciali, delle residenze prestigiose o degli edifici bancari, è certamente più articolata, e spesso prevede ulteriori suddivisioni degli spazi in sottoinsiemi omogenei per funzione, livello di accesso e rischio. Rimane comunque valida almeno ad alto livello, anche in questi impianti complessi, la nozione di divisione dello spazio in due macro zone: quella interna al perimetro protetto e quella esterna.





Allo stesso modo possiamo raggruppare le persone che operano all'interno o nelle vicinanze di un'area protetta da un allarme antifurto nelle seguenti tre categorie:

- categoria A: gli occupanti legittimi dell'edificio. Nel caso residenziale si tratta naturalmente di chi dimora nell'edificio, comprese le persone che hanno titolo per soggiornarvi (amici, parenti, etc.). Negli altri casi del personale di un'azienda, di una banca, etc.
- categoria B: i visitatori, ovvero tutte quelle persone che possono essere presenti nelle aree protette, ma soltanto in particolari condizioni, come i clienti

di un supermercato negli orari di apertura, i correntisti di una banca, etc.

- categoria C: gli attaccanti, quindi tutte le figure che hanno l'intenzione di violare l'area protetta, di solito per commettere un furto o un crimine di altra natura.

In tutti i casi, dal più semplice al più complesso, la definizione di zone dell'impianto e, in maniera complementare, del perimetro che le divide ha la primaria funzione di separare le persone che interagiscono con l'impianto stesso in almeno due gruppi: gli insider, ovvero gli occupanti legittimi (categoria A), e gli outsider, ovvero gli attaccanti (categoria C).

I visitatori, la categoria B, trovano collocazione tra gli insider e gli outsider a seconda dello stato del sistema: per esempio, in un sistema di allarme a protezione di un supermercato, un cliente durante le ore di apertura sarà necessariamente un insider, dato che occupa durante gli acquisti una zona interna del sistema che verrà allarmata alla chiusura del negozio. Questa separazione tra insider e outsider è alla base della filosofia costruttiva degli impianti di allarme antifurto: scopo primario del sistema, almeno ad alto livello, è segnalare con un allarme la presenza di un outsider in una zona interna dell'area protetta.

La divisione così netta degli attori di un sistema trova un fondamento particolarmente rilevante negli impianti residenziali, dove nella stragrande maggioranza dei casi i visitatori (categoria B) sono assimilabili agli occupanti legittimi (categoria A), e sono quindi da ritenersi benigni. Il sistema d'allarme in questo caso si trova a operare in condizioni ideali: può espletare la sua funzione di separatore tra insider e outsider nel migliore dei modi, dato che tutti gli insider si trovano nella zona interna (all'interno del perimetro protetto) e sono benigni, mentre gli outsider, potenziali attaccanti, si trovano nella zona esterna. In questo caso il rischio principale dal quale l'impianto di sicurezza è chiamato a proteggerci è l'outsider attack.

Il problema diventa però presto complesso se si analizzano le situazioni tipiche degli impianti dedicati alla

protezione di edifici non residenziali. Qui concorrono due fattori di primaria importanza nel modificare radicalmente il rischio. Il primo è che i membri della categoria B, i visitatori, possono spesso mascherare un membro della categoria C: si pensi, per esempio, al caso di un ladro che inizi la perlustrazione di un esercizio commerciale durante le ore di apertura al pubblico, per poi sferrare il suo attacco nottetempo. Il secondo fattore è dovuto alla natura umana: in questo scenario anche i membri della categoria A possono infatti nascondere o coadiuvare qualcuno che rientra in categoria C. Per esempio, un dipendente che si sentisse maltrattato potrebbe decidere di aiutare un ladro nell'esecuzione di un furto, predisponendo dall'interno una qualche forma di sabotaggio dell'impianto. Questi due fattori, già importanti se considerati singolarmente, insieme formano una miscela esplosiva per l'innalzamento del livello di rischio. In questi casi infatti il rischio principale può arrivare dall'interno del perimetro protetto: il vettore primario del rischio diviene l'insider attack.

È altrettanto chiaro che un insider attack porta l'attaccante ad aver accesso alle parti vitali del sistema di sicurezza, facendo quindi in modo che le sue azioni possano avere una efficacia molto superiore al caso dell'outsider attack. Nel caso di un insider attack, il sistema non può più operare nelle condizioni ottimali che abbiamo descritto sopra nel caso



residenziale semplice, ovvero di divisione tra insider e outsider: in questo caso, l'insider cessa di essere benigno, e il sistema di sicurezza dovrebbe reagire di conseguenza.

La normativa statunitense negli scorsi anni è stata rivista in maniera estremamente significativa proprio dopo la scoperta di ripetuti furti in edifici appartenenti al dipartimento di stato: l'analisi forense dopo questi episodi rivelava vettori primari di insider attack, come per esempio il mascheramento preventivo dei sensori volumetrici, o quello magnetico dei contatti (rilevatori di apertura varco), anche per modelli ad alta sicurezza, grazie ai quali i sistemi anti-intrusione erano stati violati con sforzi relativamente contenuti. L'insider attack è passato in breve tempo da leggenda metropolitana a uno scottante problema per tutte le zone ad alta sicurezza. La questione ha provocato una revisione profonda delle norme e, di conseguenza, della tecnologia e del modus operandi dei professionisti. In particolare, nel 2009 è stato introdotto un nuovo livello di sicurezza nella norma statunitense UL 634, il Livello 2, specificatamente pensato per le aree a rischio di insider attack. Negli Stati Uniti, i dispositivi e i sistemi di sicurezza, per essere certificabili al Livello 2 (il più alto possibile), devono oggi contenere tecnologie esplicitamente progettate per renderli resistenti all'insider attack.

Purtroppo la normativa Europea, quindi quella in vigore anche nel nostro paese, ovvero il compendio di norme EN 50131, seppur recentemente rivisto, non contempla nemmeno questo tipo di problemi. La EN 50131 specifica quattro gradi di sicurezza, dal Grado 1 (il più basso), al 4 (il più alto), basandosi esclusivamente sulla raffinatezza tecnica dell'attaccante come parametro per la definizione del grado di sicurezza. In altre parole, un impianto di Grado 1 è pensato per i casi nei quali si prevede che l'attaccante abbia «una conoscenza bassa» del sistema anti-intrusione, e che disponga «di una limitata gamma di attrezzi fa-

cilmente reperibili». All'altro capo dello spettro, un impianto di Grado 4 è idoneo, sempre secondo la EN 50131, quando si ha a che fare con attaccanti che «abbiano la capacità o le risorse per pianificare in dettaglio un'intrusione o una rapina e che dispongano di una gamma completa di attrezzature, compresi i mezzi di sostituzione dei componenti di un impianto di sicurezza».

Nella normativa europea la distinzione tra attacchi che provengono dall'esterno del perimetro protetto e quelli che invece provengono dall'interno non è nemmeno considerata come parametro essenziale per l'assegnazione di un grado di sicurezza a un impianto. È quindi chiaro che i progettisti, i costruttori di apparati e gli installatori, pur rispettando la normativa, si trovano a dover combattere una battaglia impari. Da un lato i rapinatori, ben consci della potenza che un insider attack può avere nei loro piani di crimine, stanno sempre di più affinando questi vettori d'attacco, e recenti, molteplici casi eclatanti avvenuti anche nel nostro paese ne sono la prova. Dall'altro lato i professionisti del nostro settore si trovano loro malgrado a dover combattere questa guerra con un'arma tecnologicamente spuntata, perché non in grado, a partire dalle principali normative di riferimento, di rispondere in maniera opportuna a un vettore d'attacco così dirompente.

È auspicabile che, partendo dalle associazioni di categoria per arrivare ai comitati tecnici, venga intrapresa una strada di revisione delle norme in modo da recepire quanto di utile ci possa essere nelle norme statunitensi su questo tema. Questa sembra a chi scrive un'azione dovuta, quantomeno per permettere alla catena del valore europea nel settore dei sistemi di sicurezza di poter competere ad armi pari con quella che proviene da oltre oceano. E, non meno importante, per permettere a chi usufruisce di un sistema anti-intrusione di potersi difendere al meglio, almeno in futuro.



# Con Atik arriva la nuova distribuzione

*a colloquio con Roberto Esposito, Atik Consulting  
a cura della Redazione*



**Parliamo di [www.setik.biz](http://www.setik.biz), il primo sito per la commercializzazione on-line di sistemi di sicurezza. È un sito B2B o B2C, è rivolto cioè agli installatori o agli utenti finali?**

È nato come sito B2C che però ha avuto subito un forte riscontro tra i professionisti del settore, che hanno una maggior competenza e sono quindi gli interlocutori ideali soprattutto per tutte quelle installazioni che presentano un maggior coefficiente tecnico. Oggi possiamo dire che il 30% della nostra attività è rappresentato dal B2B e il 70% dal B2C, ma a partire da quest'anno ci aspettiamo una forte crescita sul B2B, sia in ambito nazionale, ma ancora di più in chiave internazionale: il mercato estero è più ampio e pronto del nostro soprattutto per quanto riguarda l'online.

**Quali sono i vantaggi che le due diverse categorie di utenti possono trovare nell'acquisto on-line**

**rispetto alle modalità tradizionali, rivolgendosi rispettivamente ai distributori e agli installatori?**

Abbiamo cercato di prendere il meglio del mondo tradizionale e portarlo sull'online; il nostro approccio alla vendita online è molto atipico, provo a sintetizzarlo evidenziandone i fattori principali:

- prima di tutto la qualità del servizio; sembrerà banale o scontato, ma noi vogliamo evidenziare la qualità, riteniamo vitale che ogni cliente rimanga soddisfatto, ogni feedback dato rappresenta sempre un motivo per migliorare. Siamo molto attenti a questo fattore; consideri che oggi abbiamo oltre il 99% di feedback positivi su quasi 4.000 giudizi totali, giudizi pubblici dati da ogni nostro cliente, il tutto alla luce del sole, e questo dà un senso di fiducia non percepibile sul tradizionale;
- siamo tra i pochissimi che mettono a disposizione un numero telefonico per informazioni tecniche; la maggior parte degli store online vivono di "form" o



mail, senza un recapito telefonico; abbiamo inoltre optato per una soluzione con numero verde, così da dare il massimo della comodità, oltre a una chat gratuita online dove rispondiamo dal lunedì al sabato;

- abbiamo oltre il 90% della merce a catalogo in pronta consegna con disponibilità elevate, spediamo il giorno successivo al pagamento dell'ordine in tutta Italia con corriere espresso, permettendo così consegne entro 24/48 ore. Inoltre spediamo in tutta Europa entro 72 ore. Questo permette di avere "virtualmente" una disponibilità immediata su tutto il nostro catalogo da parte di ogni cliente, cosa decisamente rara oggi, e possiamo continuare a farlo grazie a un'elevatissima rotazione di magazzino, considerando che attualmente effettuiamo circa 800 spedizioni al mese;
- siamo sempre aperti tranne la domenica, inclusi il periodo natalizio e quello estivo, chiudiamo soltanto nei giorni festivi, così da andare incontro anche a chi lavora (e oggi sono molti) in agosto e nel periodo di Natale;
- ci siamo dati regole interne rigidissime; abbiamo un sistema informatico che permette di controllare



qualsiasi comunicazione in uscita dall'azienda, entro 24 ore è richiesto tassativamente al personale di rispondere a ogni richiesta ricevuta via mail, sia essa commerciale o tecnica, e stiamo introducendo in questi giorni un sistema di ticketing che permetterà a ogni cliente di avere uno storico di tutte le richieste fatte;

- tutto il personale è estremamente preparato (copriamo 4 lingue: italiano, inglese, francese e spagnolo), quasi tutti laureati, sia i tecnici (al momento 4 su rotazione) che i commerciali (al momento 4 su rotazione) hanno una preparazione su tutti i prodotti, così da dare consigli il più possibile precisi e utili; periodicamente

teniamo corsi interni sui nuovi prodotti e le nuove tecnologie, il personale è giovane e affiatato, sembra banale ma ritengo sia oggi una delle nostre più importanti carte vincenti;

- importiamo l'80% del catalogo; questo ci garantisce di ridurre drasticamente i passaggi, con costi estremamente competitivi e disponibilità delle novità del mercato quasi in tempo reale; i nostri numeri ci permettono di ottenere un canale privilegiato con i produttori e ciò è indispensabile soprattutto in un mercato difficile come quello europeo.



**Ci sono riferimenti a livello internazionale di vendita on-line di sistemi di sicurezza, tipologia che risulta molto innovativa per il mercato italiano, dove l'utente finale è abituato al rapporto con l'installatore o, meglio, con l'impiantista di fiducia?**

La figura del tecnico in questo ambito è indispensabile: gli impianti di videosorveglianza e d'allarme richiedono spesso valutazioni tecniche che l'utente finale non è in grado di fare, la nostra scelta è quindi quella di "spingere" molto sugli installatori. Setik non realizza installazioni, sempre più spesso i clienti ci chiedono di seguirli anche in questo ma purtroppo per noi è al momento impossibile. Per questo motivo oggi stanno nascendo i primi "Setik partner" ovvero installatori da noi autorizzati e verificati che seguono specifiche regole sia nella vendita che nell'installazione, che copriranno non soltanto il territorio italiano ma anche tutta Europa. Proprio in questi giorni stiamo lavorando sulla loro selezione. Essi stessi saranno sottoposti a giudizio da parte dei nostri clienti, di fatto saranno la nostra prima interfaccia verso il pubblico. Crediamo moltissimo in questo progetto, come amiamo definirlo si tratterà del nostro "esercito sul territorio".

**Quali servizi post-vendita fornite agli utenti finali?**

Prima di tutto offriamo 24 mesi di garanzia, come previsto dalla legge, certo, ma la garanzia vale anche per i rivenditori e non è un aspetto da poco in quanto siamo gli unici, che io sappia, in questo settore. Abbiamo un'assistenza via mail gestita dai 4 tecnici con tempi di risposta entro le 24 ore e stiamo attualmente integrando un sistema di ticketing, il tutto rigorosamente gratuito. Abbiamo poi un'assistenza telefonica a pagamento che, oltre a dare supporto, ci permette di collegarci (ovviamente previa richiesta e autorizzazione del cliente) sull'apparato remoto in modo tale da supportare in diretta il cliente nella configurazione. Inoltre, stiamo introducendo 3 ulteriori utili funzioni: la possibilità di effettuare direttamente la configurazione dell'impianto, inviando così al cliente la merce già configurata; la possibilità di effettuare sopralluoghi e relativi preventivi (tramite i nostri partner); la possibilità di richiedere degli interventi post-vendita da remoto su appuntamento. Eventuali interventi sul posto invece sono delegati ai nostri partner, e direi che tutto ciò è molto di più di quanto è offerto da qualsiasi azienda che non vende online.



**Quali sono state le reazioni del mercato alla vostra proposta?**

Dobbiamo fare delle distinzioni. Siamo una realtà giovane, consideri che abbiamo poco più di un anno di vera attività: siamo nati a giugno 2012 in modo assolutamente sperimentale, siamo partiti in modo organizzato soltanto nel 2013, e oggi a poco più di un anno registriamo crescita nell'ordine del 15% a trimestre; ci aspettiamo quest'anno di raddoppiare il fatturato rispetto al 2013, quindi un po' di fastidio sul mercato l'abbiamo sicuramente creato.

Dai clienti i riscontri sono stati ottimi, tranne un primo periodo dove i margini per il B2B erano piuttosto bassi; oggi abbiamo invece riadeguato i listini e sono decisamente più interessanti. Diverso è invece il discorso per quanto riguarda la concorrenza: inizialmente abbiamo avuto la processione di concorrenti che ci venivano a trovare per "educarci" su come dovevamo lavorare in questo settore, ci veniva richiesto di alzare i margini verso il B2B e di uniformarci agli altri; devo dire che in Italia soltanto un'azienda si è comportata in modo intelligente sposando la nostra iniziativa e supportandoci, traendone sicuramente profitto e diventando l'unico nostro fornitore in Italia, mentre per il resto importiamo tutto.

**I prodotti e i servizi acquistabili on-line sul vostro sito sono assimilabili a quelli distribuiti attraverso i canali tradizionali o avete innovato anche i contenuti tecnici?**

Una delle cose che più ci contraddistingue è la velocità con la quale introduciamo nuove tecnologie, questo perché riteniamo fondamentale differenziarci e per farlo il nostro obiettivo è avere sempre una marcia in più degli altri. Facciamo molta ricerca e siamo continuamente impegnati a testare nuovi prodotti; qualora ritenessimo il partner interessante ci impegniamo con lui anche nella parte di sviluppo, introducendo funzioni e necessità tipiche del mercato italiano. Alcuni esempi? Siamo stati i primi a vendere online la nuova tecnologia HD-CVI, i primi a introdurre i nuovi chipset Sony Effio-V ed Effio-A, i primi a introdurre sul mercato italiano in accordo con Western Digital i nuovi dischi Purple. Sono moltissime le novità che introduciamo mensilmente, credo che in pochi dedichino così tanto tempo alla ricerca di nuovi prodotti. Inoltre tramite il nostro blog tecnico presentiamo spesso test, consigli tecnici, guide, tutorial e molto altro.

**Dal vostro punto di vista come evolverà complessivamente il mercato della sicurezza in Italia?**

Credo che oggi ci sia molta più consapevolezza, in quanto avvicinandosi sempre più all'informatica il mondo della videosorveglianza ha attirato a sé una clientela diversa, che oggi vuole qualcosa di più. Questo qualcosa in più richiede specializzazione, competenza e professionalità, soltanto chi sarà disposto a investire anche su se stesso potrà trarne giovamento. La videosorveglianza secondo me è un settore in forte espansione, uno dei pochi in questo periodo di crisi, e l'online rappresenta una nuova era; tutto il nostro approccio è estremamente moderno, crediamo nell'online e riteniamo che sia un mercato forte, ma oggi rappresenta ancora una percentuale decisamente minima del mercato Italiano, non più del 6%-8%. Per questo motivo riteniamo fondamentale spingere anche sul canale tradizionale, saremo quindi molto presto presenti con uno store fisico che diventerà anche la nostra nuova sede e, se l'esperimento funzionerà, ci saranno molte novità che ritengo potranno ulteriormente rivoluzionare il mercato, con caratteristiche che almeno qui in Italia non sono ancora presenti.



# Uno PSIM per Berco (ThyssenKrupp)

di Bruno Fazzini, presidente e ad Citel

**B**erco, leader di mercato per cingoli per grandi macchine di movimentazione in cantiere e per uso militare, che ha la maggior parte delle risorse di produzione in Italia, appartiene al gruppo tedesco ThyssenKrupp, tra i principali operatori

mondiali nel settore degli acciai speciali e prodotti derivati. La società, già dotata da anni di singoli sistemi antintrusione, antincendio, controllo accessi, rilevazione presenze in due diversi stabilimenti, ha deciso di razionalizzare l'operatività dei vari sistemi integrandoli in un sistema di gestione unico



multifornitore e multifunzione salvaguardando gli investimenti fatti in passato e sostituendo soltanto ciò che risultava obsoleto o non integrabile. I vincoli esistenti erano la salvaguardia e integrazione dei sottosistemi anti-intrusione UTC Aritech Master e anti-incendio Notifier. La società aveva inoltre la necessità di ottenere una gestione proceduralizzata, immediata e tracciabile di eventi generati dalla correlazione di input diversi.

Le strutture da proteggere erano molteplici: lo stabilimento di Copparo, lo stabilimento di Castelfranco Veneto, fonderia, carpenteria, magazzino, i parcheggi dipendenti. Era necessario garantire inoltre la protezione perimetrale di 2 km per la sede principale e la safety di 3000 dipendenti totali.

BERCO ha adottato un sistema di gestione integrata della sicurezza fisica in logica PSIM (Physical Security Information Management) scegliendo la piattaforma aperta multifornitore CENTRAX di Citel Spa.

Centrax è il sistema di gestione informatizzata della sicurezza fisica pienamente aderente a tutti i requisiti PSIM; è il più diffuso in Italia, con una presenza iniziata tra i grandi utenti come Poste e banche da oltre 10 anni e una rapida diffusione anche nel settore manifatturiero e del retail, sia per soluzioni interne che per servizi esterni, anche in forma cloud, e quindi sostenibili per qualsiasi dimensione aziendale.

Il progetto di Citel è stato scelto da BERCO sulla base delle referenze presentate su progetti tecnicamente assimilabili e per le competenze progettuali e realizzative dimostrate in questi ultimi anni nella realizzazione di sistemi di protezione integrata in ambito industriale. Un ulteriore elemento di peso nella scelta è stato il coinvolgimento di Zucchetti-Axess da parte di Citel, per la copertura di tutte le esigenze di controllo accessi, rilevamento presenze, gestione dei flussi di personale nelle mense.

Citel ha proposto come partner specializzato Zucchetti-Axess per la sistemistica di gestione accessi, anche in virtù di una sinergia ormai consolidata in ambito ENI e Saipem, dove entrambe le aziende sono qualificate e certificate e dove l'integrazione

tecnico-funzionale ha raggiunto quel livello di eccellenza che è irrinunciabile per gli ambienti critici delle multinazionali dell'energia.

Il principale aspetto innovativo è il fatto che il progetto sia stato ideato in logica di sistema informatico per la sicurezza fisica, integralmente aderente ai requisiti PSIM e con la valorizzazione dei sottosistemi esistenti. Sono state previste l'integrazione e correlazione dei sottosistemi di protezione degli asset aziendali per ottenere un cruscotto unificato di gestione degli eventi, nonché la gestione per eventi e non soltanto per allarmi, quindi un data collection di segnali di tipo qualsiasi, atti a generare – anche per gruppi di correlazione – eventi qualificati per grado di attendibilità, localizzati con la precisione,

e aggiornati in tempo reale anche ai fini del "situation management" della sicurezza fisica, della safety, dell'integrità dell'impiantistica.

Le sostituzioni/nuove implementazioni hanno riguardato il sistema di controllo accessi e rile-

vamento presenze, il sistema di videosorveglianza intelligente con moduli di videoanalisi a bordo di telecamere IP Axis, basati su soluzioni Technoaware (perimetro, parcheggio esterno, magazzino esterno e parcheggio dirigenti), il sistema di controllo veicoli in entrata e uscita e monitoraggio flotta aziendale, il sistema di rilevamento uomo a terra tramite rete GPS e Wifi e la gestione delle 4 mense aziendali tramite sistemi di prenotazione e consumo della Zucchetti.

Il team di Progetto è stato così costituito:

- main contractor Citel Spa;
- controllo accessi Zucchetti – Axess;
- rilevamento presenze Zucchetti – Axess;
- gestione mense Zucchetti;
- video management Citel - CVM (Centrax Video Manager);
- tecnologia video Axis;
- analisi dell'immagine e moduli per la protezione perimetrale Technoaware – Genova;
- rilevamento e gestione "uomo a terra" Salute & Innovazione;
- attività di impiantistica specializzata Intecom Srl.



## Integrazioni e interoperabilità

sotto-sistema	tecnologia	tipo di integrazione e interazione
Videosorveglianza e video analisi	CVM + Axis + Technoaware	Il modulo integrato di Centrax, CVM (Centrax Video Manager), gestisce 50 telecamere IP, 38 delle quali dotate di algoritmi di videoanalisi di Technoaware per rilevare intrusioni, scavalcamenti, avvicinamenti anomali alle barriere fisiche.
Sottosistema Intrusione	UTC Aritech Master	Normalizzazione, mediante il modulo Gemina di Citel, del protocollo proprietario della centrale Master in protocollo pubblico CEI per l'interazione bidirezionale di segnalazioni e comandi su rete IP.
Sottosistema Incendio	Notifier AM 6000	Normalizzazione, mediante il modulo Gemina di Citel, del protocollo proprietario della centrale AM6000 in protocollo pubblico CEI per l'interazione bidirezionale di segnalazioni e comandi su rete IP.
Controllo Accessi / Rilevamento presenze	X@tlas di Zucchetti Axess TMC	Interazione diretta server-to-device per la ricezione immediata delle anomalie da diagnostica del device e delle segnalazioni di tentativi di effrazione o di esclusione dei varchi.
Mensa	Zucchetti Mensa Web	Interazione con il sistema di gestione delle prenotazioni dei singoli dipendenti per 4 mense aziendali con relativi terminali di consumo disposti presso ciascuna linea di distribuzione. L'interazione ha lo scopo di ricevere segnalazioni diagnostiche a fini manutentivi e con il gestionale aziendale per la corretta contabilizzazione.
Sistema di rilevamento uomo a terra	Salute & Innovazione	Integrazione del sistema su server Centrax per la ricezione dei dati legati alla geo-localizzazione tramite GPS piuttosto che da triangolazione Wi-fi con relativi strumenti di comunicazione implementati su Centrax.

## Conformità ai 7 requisiti PSIM

n	requisito PSIM come da definizione IHS	conformità del progetto ai requisiti
1	<b>Connettività e integrazione</b>	Il PSIM di BERCO è installato e configurato per ricevere e correlare segnalazioni e transazioni da tutti i sottosistemi: intrusione di Ge Security-UTC incendio di Notifier, connessi via LAN. È quindi in grado di attivare comandi specifici in funzione del tipo di evento risultante dalla correlazione e dalla sua dinamica.
2	<b>Gestione Real Time e configurazione controllata</b>	Gli eventi vengono tutti generati in real time e presentati immediatamente in una coda, dalla quale si attiva il cruscotto contestualizzato di gestione.

3	<b>Correlazioni e Verifiche</b>	le correlazioni principali coinvolgono accessi, incendio, intrusione, videoanalisi.
4	<b>Visualizzazione per la cognizione immediata, oggettiva e completa della situazione</b>	Lo scenario completo dell'evento viene ottenuto su planimetria animata, pop-up di videoispezione contestualizzato a chi deve gestire l'evento un'idea anche complessiva della natura dell'evento, del contesto locale e dell'ampiezza della minaccia.
5	<b>Processo di gestione eventi basato su procedure guidate</b>	Avvio immediato dell'operatore su un percorso guidato passo-passo, basato su procedure mirate al contenimento o al contrasto della minaccia, monitorizzando progressivamente l'esito delle attività svolte sul posto.
6	<b>Affidabilità e Resilienza</b>	Il sistema è predisposto sia per la business continuity in locale che per il disaster recovery da remoto. Una volta entrato in esercizio, il sistema sarà completato con una soluzione di Disaster Recovery in una diversa località.
7	<b>Reportistica e Riesame post-evento</b>	La reportistica viene generata automaticamente o semi-automaticamente da Centrax, senza lasciare spazio alla soggettività dell'operatore. Ai report sono allegabili, nel corso della gestione dell'evento, files multimediali di tipo snap-shot che video-clip. I report non sono modificabili, ma soltanto integrabili da un responsabile di livello superiore; sono archiviabili anche in black-box remotizzate e tracciabilità della gestione e verbalizzazione non soggettiva e documentata della gestione dell'evento facilitano la ricostruzione – anche criminologica – dell'accaduto e della sua gestione.



Gruppo di appartenenza e committente



Main-contractor e sistemistica di integrazione utilizzata



Partners di soluzioni integrate  
Impiantistica specializzata



Altre integrazioni  
(incendio e intrusione)

# Allegion, c'è del nuovo anzi di antico...

*a colloquio con Giovanni Miti, Amministratore Delegato CISA, e Alberto Andrini, Product Manager Hospitality Solutions EMEIA a cura della Redazione*

**Allegion è un nuovo marchio che si presenta nel panorama mondiale della sicurezza fisica degli accessi ma, in realtà, è un gruppo globale di aziende presenti in tutto il mondo, alcune delle quali con storie secolari. Ci parli di Allegion.**

*Giovanni Miti, Amministratore Delegato CISA*

A partire dal 2 dicembre 2013 la divisione sicurezza di Ingersoll Rand è stata resa autonoma per creare una nuova società globale denominata Allegion PLC. Allegion è a tutti gli effetti un'azienda indipendente, quotata presso la borsa di New York (NYSE: ALLE) e rappresentata da un gruppo di marchi leader nel mercato della sicurezza. Si può affermare che pur essendo un'azienda nuova Allegion vanta un patrimonio consolidato e in continuo sviluppo di soluzioni per la sicurezza. CISA è parte del nuovo gruppo e da subito si è impegnata per dare valore ad Allegion confermando il proprio ruolo nel mercato dei sistemi di chiusura e controllo accessi. CISA in Italia conta 770 dipendenti distribuiti nelle sedi di Faenza (Ravenna) e di Monsampolo del Tronto (Ascoli Piceno),

polo di riferimento per la produzione dei cilindri.

**Tra i marchi del gruppo figura anche l'italiano CISA, un'azienda che ha letteralmente fatto la storia della sicurezza fisica degli accessi e di cui Paolo Tura, il fondatore di Essecome, era stato direttore commerciale fino al 1979. Qual è il ruolo affidato a CISA nella strategia globale di Allegion?**

*Giovanni Miti, Amministratore Delegato CISA*

La storia di CISA è "costellata" da eccellenze e professionisti come Paolo Tura, che ho avuto la fortuna e il piacere di conoscere, che nel tempo hanno contribuito a rendere il nostro marchio tra i più importanti nel settore. Tornando alle origini, permettetemi di citare il nostro fondatore Luigi Bucci, che nel 1926 ha creato a Firenze Costruzioni Italiane Serrature Affini, brevettando la prima serratura elettrocomandata che rivoluzionò il principio di azionamento dei portoni e dei cancelli.

Quasi un secolo di sviluppo che ha portato oggi CISA a essere nella rosa dei cinque marchi strategici a li-



*Giovanni Miti*



*Alberto Andrini*





vello mondiale di Allegion. Lo storico logo CISA continua a essere punto di riferimento nel mercato dei sistemi di chiusura e controllo accessi, contribuendo così a dare valore al nuovo gruppo.

Si tratta di una sinergia strategica; basti pensare che il catalogo CISA contiene oltre 30 mila articoli: cilindri, serrature per le varie tipologie di porte, maniglioni antipanico e sistemi per uscite d'emergenza, chiudiporta, casseforti, serrature elettroniche e sistemi per il controllo accessi. Prodotti e servizi che rispondono ai più elevati standard previsti dalle normative.

**La sicurezza fisica oggi integra sempre più le componenti passive (porte, serrature) con quelle attive di controllo accessi, utilizzando tutte le tecnologie disponibili, biometria e RFID compresi. Qual è la visione di CISA su questo tema e quali prodotti presenta sul mercato integrando componenti meccaniche ed elettroniche?**

*Alberto Andrini, Product Manager Hospitality Solutions EMEIA*

Le soluzioni elettroniche CISA per il controllo accessi consentono da sempre una facile integrazione con prodotti di terze parti (per esempio soluzioni per la sicurezza fisica, gestione della camera intelligente o borsellini elettronici), grazie a interfacce "aperte" che garantiscono elevati standard di sicurezza e semplicità d'uso. Ne sono la riprova i numerosi casi di partnership con aziende del settore.

Le tecnologie utilizzate per l'integrazione si sono naturalmente evolute nel tempo e CISA segue attentamente questa evoluzione, sviluppando prodotti che integrano lo stato dell'arte in fatto di standard tecnologici; un esempio su tutti è la nuova serratura eSIGNO, compatibile con lo standard di comunicazione a corto raggio NFC, che consente lo scam-

bio di informazioni con dispositivi mobili compatibili (smartphone, tablet) e, nella versione wireless, con il protocollo di comunicazione ZigBee™ tramite il quale è possibile il controllo centralizzato della serratura senza la necessità di cablaggi strutturali.

**E quali sono le soluzioni per rendere interoperabili gli accessi nell'ambito di sistemi di sicurezza in rete (over IP)?**

*Alberto Andrini, Product Manager Hospitality Solutions EMEIA*

Il sistema di controllo accessi elettronico per hotel e ambienti comunitari CISA eSIGNO include un kit di sviluppo software completo di documentazione tecnica e codice d'esempio, con il quale è possibile integrare, tra gli altri, anche sistemi di sicurezza IP. A tal proposito CISA offre supporto tecnico agli sviluppatori della società partner al fine di realizzare soluzioni affidabili e integrate, pur garantendo autonomia di funzionamento. In gergo tecnico questo aspetto viene definito "fault tolerance": l'eventuale malfunzionamento di uno dei due sistemi non ha effetto sull'altro, funzionalità chiave in un contesto di elevata sicurezza.

**A quali segmenti del mercato italiano sono rivolti principalmente i vostri prodotti?**

*Alberto Andrini, Product Manager Hospitality Solutions EMEIA*

CISA è stata tra le prime al mondo a integrare nelle proprie serrature la tecnologia delle smart card fino ad arrivare a soluzioni contactless, sviluppando prodotti innovativi per gli ambienti comunitari tra cui l'alberghiero. Tra le novità più rivelanti CISA propone la serratura contactless eSIGNO che unisce l'eccellenza del design italiano a prestazioni di sicurezza



avanzate: la sua configurazione elegante e compatta risponde in modo completo ed efficace alle esigenze specifiche del mondo dell'ospitalità, dalle catene alberghiere alle strutture a conduzione familiare.

Grazie alla tecnologia contactless la serratura si apre in modo intuitivo avvicinando la tessera al lettore. CISA eSIGNO funziona a batterie, evitando lavorazioni invasive sulla porta e semplificando l'installazione anche nei casi di sostituzione di sistemi preesistenti. La serratura elettronica è dotata inoltre di segnalazione a led per la funzionalità "do-not-disturb", che indica allo staff la presenza in camera dell'ospite. La nuova serratura è disponibile anche wireless ed è inoltre compatibile con la tecnologia Near Field Communication (NFC): memorizzando i dati di accesso nel proprio telefonino basta avvicinarlo alla serratura

per entrare in camera.

La gamma CISA eSIGNO comprende anche la nuova cassaforte pensata per hotel. Si contraddistingue per il design moderno Made in Italy, progettato per adattarsi a ogni ambiente. Grazie all'apertura a 90° e a cerniere a sbalzo che portano lo sportello fuori ingombro è consentita l'introduzione di un PC portatile da 14" ed è prevista una presa di alimentazione interna per ricaricarlo. La cassaforte funziona con quattro batterie che consentono alla serratura motorizzata l'apertura automatica dello sportello a basso consumo, testata da 8000 cicli apri-chiudi.

L'offerta CISA per il mondo hotel è un network completo di informazioni e approfondimenti, con il sito internet [cisahotels.com](http://cisahotels.com), il canale dedicato su YouTube e la possibilità di twittare con CISA @CISALocks.



WiseNet III

SAMSUNG  
SAMSUNG TECHWIN

# WISENETIII... A PROVA DI FUTURO!



## ...E RISPARMIA CON I PRODOTTI IP WISENETIII

In Samsung sappiamo bene che decidere quando e come migrare a una soluzione di sicurezza IP è un'operazione complessa, condizionata da molteplici fattori. La nostra nuova gamma di telecamere IP WiseNetIII permette di avere un controllo completo e una totale flessibilità nello scegliere la soluzione che meglio si adatta alla tua azienda. Puoi integrare WiseNetIII nel tuo attuale sistema analogico! Con Samsung puoi adeguare il tuo impianto di videosorveglianza, senza, necessariamente, buttare via l'investimento fatto in precedenza.

Contattaci per maggiori informazioni!

E [stesecurity@samsung.com](mailto:stesecurity@samsung.com)

W [www.samsung-security.it](http://www.samsung-security.it)

# 4Power Srl: sicurezza IP e innovazione

*a colloquio con Pasquale Pirozzi, direttore generale 4Power Srl  
a cura della Redazione*

**4**Power nasce dall'incontro tra professionisti provenienti dai settori protezione elettrica, networking, cablaggio strutturato. Obiettivo comune: creare una impresa ad alto valore aggiunto con una offerta di prodotti a 360° per tre settori fondamentali: protezione e continuità elettrica, sicurezza e networking, cablaggio strutturato. Tutti i fondatori concordavano sulla necessità di offrire un servizio per supportare la clientela nel ridurre i tempi e le energie necessarie alla gestione dei fornitori: differenti condizioni di vendita e pagamento, sistemi di assistenza disomogenei e prodotti di varie marche a volte non completamente compatibili tra loro. D'altra parte se i fornitori sono molti è difficile che riescano ad avere un quadro completo delle problematiche del cliente e quindi a supportarlo efficacemente.

L'intenzione era di anticipare quella che oggi è una evidente richiesta da parte del mercato: la necessità di formazione e di assistenza pre e post vendita. Il cliente ideale cerca un affiancamento nella scelta dei prodotti per ottimizzare i costi di manutenzione e gestione, desidera soluzioni stabili e durature, oltre che un rapporto qualità prezzo competitivo.

## **Perché avete deciso di entrare nel settore della sicurezza?**

La sicurezza è un ambito quasi naturale per 4Power. Uno dei fondatori proveniva proprio da questo settore, ma con l'affermarsi delle tecnologie IP possiamo dire che cablaggio strutturato, networking e continuità elettrica sono ambiti specifici della sicurezza IP, sia che venga intesa in senso stretto (sorveglianza, controllo accessi, anti intrusione, etc.) che in senso lato (affidabilità delle installazioni, possibilità di prestazioni elevate anche in situazioni



critiche, etc.). Negli ultimi anni il settore sicurezza ha avuto una crescita interessante, in parte legata alla sensazione di "insicurezza" nella vita quotidiana, in parte dovuta alla convergenza delle periferiche sulle piattaforme informatiche e reti IP; tutto ciò ha semplificato le installazioni e reso accessibili funzioni che fino a pochi anni fa erano disponibili soltanto a costo di grossi investimenti.

## **Come siete attualmente organizzati sul territorio?**

La rete di 4Power sul territorio è organizzata prevalentemente in agenzie di vendita indiretta e funzionali tecnico commerciali, oltre che agenzie

plurimandatarie affiancate dai nostri specialisti di divisione. Avere prevalentemente funzionari diretti è una scelta strategica: se non vi è perfetta intesa tra produzione, magazzino, assistenza e funzionari vendite, è facile entrare in spirali pericolose che possono produrre ritardi, problematiche tecniche non risolte e insoddisfazione dei clienti. Tutte cose che in una prospettiva di lungo periodo si trasformano in perdite di fatturato o maggiori costi.

## Quali sono le vostre idee e proiezioni per il futuro?

Le modalità operative e le strette relazioni con la rete dei clienti e distributori hanno cambiato il modo in cui guardiamo al mercato. Possiamo riassumere questa influenza nel consolidarsi di due concetti, apparentemente banali.

Il primo è che chiaramente i problemi su uno degli anelli della catena di distribuzione si ripercuotono su tutti, sino a noi produttori, per cui diventa normale, quando pensiamo a una strategia o a un prodotto, considerare come interesse strategico dell'azienda non soltanto la vendita ma tutti gli effetti generati dalla stessa sul sistema.

In seconda battuta consideriamo l'ampliamento dell'orizzonte temporale: quando pensiamo a un prodotto o a una strategia, diventa necessario considerare gli effetti e le possibili conseguenze a lunga scadenza, piuttosto che concentrarsi sull'immediatezza della vendita.

Il cliente deve fidarsi e sapere che quando si rivolge a noi per un supporto o una informazione i consigli e suggerimenti sono dati nell'interesse di tutti. Due modi di pensare che fino a poco tempo fa erano ad appannaggio di pochi "visionari" della sostenibilità e dell'ambientalismo, ma che oggi stanno entrando nel vocabolario quotidiano di molte aziende.

Come azienda per prossimi anni abbiamo fissato alcuni obiettivi: incrementare il livello qualitativo del supporto tecnico, potenziare la formazione e sviluppare prodotti personalizzati. Come asse trasversale abbiamo deciso di porre la massima attenzione al risparmio energetico e alla Green Technology.

## Qual è il pensiero di 4power a proposito dei concetti "sostenibile", "green" e "smart"?

Tre concetti che si stanno affermando nelle imprese, rafforzati da fatti concreti come il crescente costo dell'energia, le frequenti notizie di disastri ambien-



tali che mettono in crisi intere economie e gli effetti del cambiamento climatico. Tutti fattori che sottolineano come non sia possibile sottrarsi alle conseguenze di comportamenti produttivi scorretti o non sostenibili.

Lasciando da parte l'uso di queste parole per vuote strategie di marketing, il mondo della Green Economy offre vere e proprie fonti di guadagno. Non soltanto, ma spinge anche verso modalità produttive non predatorie e realmente sostenibili sul lungo periodo: in altre parole con il giusto guadagno per tutti e per l'ambiente.

## Come si pone 4power nei confronti della formazione?

Dal 2013 abbiamo incrementato gli investimenti nel settore formazione e rafforzato l'offerta diretta verso i distributori e gli installatori. È chiaro che parte della



mancata ripresa e del trend negativo dell'economia Italiana è legata anche a un diffuso deficit di competenze. Le tecnologie si evolvono rapidamente e molti faticano a stare dietro all'innovazione. Per questo, dopo una opportuna sperimentazione, abbiamo deciso di decentrare la nostra offerta formativa realizzando corsi di formazione e aggiornamento anche presso le sedi dei distributori o dei clienti che lo richiedono. Questa strategia offre un doppio beneficio: la formazione fatta "a casa propria" permette a più persone della stessa azienda di partecipare, riducendo tempi e costi e creando un sapere condiviso, ma anche di consolidare l'autorevolezza del distributore o del partner verso i suoi clienti, che vengono invitati ai corsi.

### **Ci può parlare della personalizzazione dei prodotti?**

Il rapporto costante con la clientela ci fornisce informazioni importanti per lo sviluppo di nuovi prodotti e servizi per risolvere problematiche o necessità specifiche. Nel 2013, dopo un lungo periodo di progettazione e test, abbiamo messo in produzione e lanciato sul mercato due apparati innovativi, dedicati al settore domotica e sicurezza: DOMO, un UPS miniaturizzato installabile su guida DIN in quadri elettrici e INTEGRA, uno switch con porte LAN e SFP, risultato di una integrazione delle tecnologie UPS e PoE.

Altro settore in crescita è quello del networking e sicurezza IP con alimentazione fotovoltaica. In questo

ambito stiamo promuovendo il sistema Wi-Fi a isola basato sull'innovativo switch BSP-300 della Planet Technology, progettato specificamente per reti con alimentazione fotovoltaica. Questo coniuga in un unico apparato switch e tecnologie per la ricarica e gestione delle batterie.

In questi prodotti si concentra la nostra proiezione futura: innovazione, integrazione e risparmio energetico.



# Lo storage secondo WD Purple

*a colloquio con Davide Vento, Business Manager Italy WD  
a cura della Redazione*

**Parliamo di WD, leader mondiale nell'archiviazione, che propone soluzioni innovative per lo storage delle immagini di videosorveglianza.**

WD ha lanciato di recente i nuovi WD Purple, una famiglia di dischi specificamente pensati per le applicazioni di videosorveglianza (in ambiente CCTV). Già dal 2011 WD ha sviluppato un approccio al mercato incentrato sul concetto che un hard disk non vada bene per tutte le applicazioni, proponendo una gamma di prodotti ampia, con caratteristiche distinte per diverse applicazioni. Come una city car non è la soluzione migliore per un agente di commercio che percorre, per esempio, 70.000 km/anno sulle autostrade italiane, anche l'hard disk per un uso comune all'interno di un personal computer non è la migliore soluzione per chi deve installarlo, per esempio, all'interno di un sistema di videosorveglianza o un sistema di archiviazione dati acceso 365 giorni all'anno 24 ore su 24. Il WD Blue è l'ideale per le applicazioni da ufficio, il WD Green come sistema secondario d'archiviazione, il WD Black per gli utenti che cercano la massima prestazione in ambiente gaming e professionale (video editing per esempio), il WD RED per sistemi NAS (fino a 5 alloggiamenti) i WD SE per sistemi NAS oltre i 6 alloggiamenti, i WD RE per sistemi di archiviazione, ad alta affidabilità, il WD XE per applicazioni "mission critical", i WD VelociRaptor per workstation.

**Quali sono le caratteristiche peculiari di WD Purple e a quali tipologie di utenti finali si rivolge?**

Semplificando al massimo, le caratteristiche principali dei WD Purple sono le seguenti:



- 3 anni di garanzia;
- progettato per utilizzo 24/7;
- firmware All Frame technology per ridurre al minimo le immagini "pixelate";
- cache sbilanciata in scrittura per ottimizzare l'acquisizione dati (immagini);
- supporto fino a 32 Videocamere HD (alta risoluzione);
- ideale per sistemi DVR/NVR fino a 8 baie (8 hard disk in raid);
- certificato dai principali produttori di DVR e NVR mondiali.





Il WD Purple è il prodotto ideale per sistemi di video sorveglianza home/small medium business in sistemi DVR/NVR fino a 8 dischi e con un massimo di 32 telecamere in alta risoluzione collegate. Secondo analisi di mercato del 2012 (fonti esterne) il WD Purple può essere identificato come il disco rigido ideale nel 93% delle installazioni di sistemi di video sorveglianza.

### **Secondo WD, quali sono le prospettive di fusione dei sistemi video in rete nel mercato residenziale, SOHO e Small Business?**

WD considera il mercato della videosorveglianza come una nuova opportunità molto interessante. Sempre più spesso ci si preme di installare impianti di videosorveglianza anche in ambito residenziale e la semplificazione dell'installazione aiuta sicuramente a far sì che il mercato possa potenzialmente crescere in modo esponenziale. Molti degli installatori si approvvigionano (anche per gli hard disk) non dal canale informativo, ma da fornitori di componenti elettronici quali interruttori, cavi, etc. WD vuole comunicare a tali

operatori che possono anche comprare dai loro fornitori abituali ma facendo la scelta giusta per il tipo di applicazione in cui viene integrato il disco fisso. Negli obiettivi di WD il WD Purple potrebbe avere lo stesso successo riscontrato negli ultimi 18 mesi dal WD RED nell'ambiente storage/NAS prosumer (fino a 5 slot per 25-30 utenti).

### **La migrazione da analogico a IP è data come cosa fatta sul piano teorico ma non ancora in termini quantitativi e non in tutti i mercati. Quali sono le vostre valutazioni in materia?**

Personalmente penso che questa migrazione non sia ancora avvenuta al 100%, motivo per cui siamo un po' in ritardo rispetto ad altri paesi europei. La semplificazione degli impianti e le soluzioni "chiavi in mano" sicuramente potranno aiutare ad accelerare tale migrazione. Oltre il 60% del mercato dei DVR mondiale in termini di fatturato è fatto da player medio piccoli (con meno dell'1% di quote di mercato); questo vuol dire che in prospettiva ci sono molteplici opportunità da poter cogliere. Per il lancio dei WD Purple abbiamo dato i nostri dischi ai principali produttori di DVR e NVR per fare in modo





che già al lancio gli utenti potessero verificare sui siti dei vendor di DVR/NVR e su quello di WD la piena compatibilità e certificazione, in modo da integrare i nostri dischi in modo sereno, sapendo che gli stessi sono stati già testati e approvati da questi produttori.

**Quali solo le vostre previsioni sul mercato globale della sicurezza nel breve/medio termine come evoluzione dei prodotti e delle strategie di marketing?**

Noi pensiamo che il mercato CCTV possa essere una nuova opportunità per tutti. Fare training, corsi, la partecipazione di WD agli eventi di sicurezza in Italia e in Europa, indica per noi che questo mercato è sicuramente in crescita e potenzialmente nuovo. Riteniamo sia un'opportunità di crescita non indifferente e la strategia marketing è quella di essere il più vicino possibile a chi usa realmente i dischi, a chi li installa. Da qui la nostra volontà di stringere collaborazioni direttamente con i primari operatori del mercato italiano, per aiutarli a capire (ove necessario) qual è il prodotto giusto per ogni singola installazione CCTV. Un impianto con 100 videocamere HD, per esempio, è progettato diversamente da un impianto da 20 videocamere HD, e di conseguenza i dischi fissi integrati per l'archiviazione immagini devono essere diversi. È questo che WD intende spiegare agli operatori del mercato della videosorveglianza che, forse, non hanno mai riflettuto in modo approfondito su tali aspetti.



**Switch Gigabit Managed con SFP e DI/DO**



Linea ethernet METRO, rame/fibra:  
8 Porte SFP 100/1000X + 2 Porte 10/100/1000T  
2 ingressi digitali (DI) e 2 uscite (DO) - per collegare sensori ed attuatori di allarme al sistema  
Trasferimento allarme alla rete IP via SNMP

**Switch Gigabit industriali rame/fibra**



Switch Ethernet gestito 8 porte 10/100/1000Base-T  
2 porte SFP 100/1000F massima flessibilità, adatto a condizioni gravose: IP30 slim (-40 a +75°C)  
Staffa per montaggio su guida DIN

**Access Point per esterni Wi-Fi a 5Ghz**



AP Wireless IP55 multifunzione con antenna integrata (Flat Panel 16dBi)  
2 connettori RP-SMA per antenna Esterna 300Mbps IEEE 802.11a/n. 5GHz, IP 55, alimentazione PoE/DC/AC



www.4power.it  
info@4power.it



# Sistemi integrati Eyeon di Videotrend al Golf Club di Manzano

*a cura della Redazione*

**L**e colline cortonesi richiamano da sempre un gran numero di turisti italiani e stranieri, attratti dalle bellezze della nota cittadina toscana. A pochi chilometri da Cortona si sta sviluppando il progetto del Manzano Golf & SPA Resort, che sarà il primo Golf Resort di Cortona, si estenderà per circa 80 ettari e includerà un campo da golf disegnato dallo studio

del famoso progettista Gary Player, un hotel a 4 stelle lusso e ben 36 unità abitative.

La realizzazione del progetto è stata sviluppata interamente con prodotti Eyeon per il controllo domotico e dell'automazione alberghiera.

Ogni appartamento della struttura viene allestito con moduli intelligenti interconnessi tra loro.

Il collegamento delle camere con la centrale di su-





pervisione garantisce il controllo e la gestione di ogni utenza.

I servizi tipicamente implementati sono il controllo accessi, le presenze, il risparmio energetico, la gestione ottimale del personale e delle utenze elettriche oltre alla supervisione generale di zone comuni e aree tecnologiche.

Una nota particolare va al modulo touch da 2.8" che rappresenta la soluzione ideale per la gestione completa dell'appartamento in un sistema di automazione alberghiera.

Grazie al suo pannello touch screen può racchiudere al suo interno tutte le funzionalità di tutti i moduli utilizzabili all'interno, oltre a fungere da lettore di tessere o transponder, da termostato digitale per la gestione della climatizzazione e da gestore di messaggistica personalizzata per l'ospite, quali le info Hotel e della località che lo ospita.

La postazione di supervisione è stata alloggiata nella parte hotel del complesso ed è composta da una base Pc embedded con sistema E-Life nativo.

Gli apparati sono modulari e montati in un apposito quadro RACK che garantisce anche l'alloggio del backup di sicurezza elettrico oltre che quello softwa-

re completo di tutte le informazioni dell'impianto in modo da garantire il suo funzionamento in mancanza di rete.

È possibile anche connettersi con l'impianto antintrusione o a quello di videosorveglianza a circuito chiuso. Le periferiche intelligenti I/O sono distribuite e autoalimentate su linea CAN BUS installata all'interno dei centralini di camera o quadri di zona.

La parte di supervisione è in grado di sostenere tutti gli apparati necessari alla struttura con possibilità di futuri ampliamenti, mentre le unità remote di controllo camera sono montate in appositi moduli DIN.

## CONTATTI

VIDEOTREND SRL  
(+39) 0362 1791300  
[www.videotrend.net](http://www.videotrend.net)  
[www.aion.it](http://www.aion.it)

# STANNO PER ARRIVARE



L'innovativa serie di videoregistratori di rete (NVR) Milestone Husky™ fornisce soluzioni di videosorveglianza personalizzate completamente integrate. Questa serie di NVR state-of-the-art può essere personalizzata per soddisfare le esigenze di qualsiasi impianto di sorveglianza, da una abitazione o una piccola azienda, a un impianto di sorveglianza complesso con più siti e centinaia di telecamere.



The Open Platform Company

# La combinazione perfetta

## Milestone Husky

Il premiato software di gestione video Milestone, assieme con hardware ad alte prestazioni. Milestone Systems offre la serie Milestone Husky™, disponibile in tre modelli. Utilizzare uno da solo, “stand alone” o collegare più modelli e scegliere tra più di 50 opzioni per una soluzione veramente personalizzabile e scalabile.



### Milestone Husky™ M10

Piccolo, elegante e configurato per efficaci prestazioni e affidabilità.  
Ideale per la videosorveglianza entry-level.



### Milestone Husky™ M30

Progettato per installazioni di workstation con esigenze di sorveglianza generale.  
Personalizzabile per rispettare il budget e scalabile quando il vostro business cresce.



### Milestone Husky™ M50

Il Top, la soluzione rack con la massima archiviazione, memoria e potenza di CPU.  
Il Milestone Husky M50 è ricco di funzionalità e personalizzabile con opzioni illimitate, rendendolo perfetto per le installazioni avanzate con sofisticate esigenze di sorveglianza.

# Perché Milestone Husky?

## Ottime Prestazioni

- ▶ Pre-installato il software di gestione video Milestone (VMS) con dimostrata semplicità e affidabilità in migliaia di installazioni in tutto il mondo
- ▶ La perfetta integrazione del software di gestione video Milestone (VMS) e hardware ad alte prestazioni
- ▶ Progettato, costruito e testato per affidabilità e durata

## Personalizzazione e scalabilità

- ▶ Collegare modelli Milestone Husky per l'efficacia dei costi e scalabilità illimitata per soddisfare le crescenti esigenze di sorveglianza
- ▶ Utilizzare Milestone Interconnect™ per collegare modelli Milestone Husky in siti remoti con XProtect®
- ▶ Corporate per la centrale di comando e controllo\*
- ▶ Collegare più Milestone Husky M30 o Milestone Husky M50 con una configurazione master / slave e guardare il video da tutte le telecamere collegate semplicemente collegando al server master. Installare marche e modelli diversi di telecamere in base alle vostre esigenze: compatibile con la più ampia selezione di telecamere (supporta ONVIF™ e dispositivi compatibili PSIA)
- ▶ Integrare add-on XProtect e integrazioni di Terze Parti, come il controllo accessi e video analisi, con i modelli Milestone Husky M30 e Milestone Husky M50

## Semplicità

- ▶ Software preinstallato e attivato automaticamente con l'hardware
- ▶ Facile set-up in pochi minuti - procedure guidate di configurazione, attivazione automatica della licenza e ricerca del dispositivo automatico (ad esempio telecamere)
- ▶ Facile manutenzione e sostituzione, l'hardware possono essere spediti prima di rispedire l'hardware da riparare
- ▶ Non richiede formazione sul software

\* Richiesto per Husky M10.

Specifiche e caratteristiche possono essere variate.



# Siemens sbarra la porta agli intrusi con Magic Mirror

a cura della Redazione

**S**ecurity Products di Siemens presenta lo stato dell'arte dei rilevatori di movimento da interno, i nuovi "Magic", disponibili nella versione con grandangolo da 12 o 18 metri, PIR e a doppia tecnologia, con o senza antimascheramento.

Questi nuovi dispositivi utilizzano la tecnologia "Magic Mirror", un brevetto esclusivo Siemens che fissa nuovi standard nella sensibilità di rilevazione e nell'affidabilità, perfezionando nel contempo gli algoritmi Visatech e Machtech per una attendibilità e immunità da falsi allarmi senza rivali.

L'innovativa compattezza del design e delle soluzioni installative, inoltre, li rende unici assicurando una perfetta integrazione in ogni contesto di utilizzo.

Magic Mirror è l'evoluzione della famosa tecnologia Black Mirror di Siemens, cui è stata apportata una serie di importanti miglioramenti. L'innovativo specchio aumenta la lunghezza focale dei rilevatori, rendendo la sensibilità di rilevazione più omogenea, soprattutto per le aree più estese. Un nuovo sistema di filtraggio della luce bianca riduce i falsi allarmi dovuti alla presenza di fonti di luce esterne, come lampade o fari di eventuali vetture.

Naturalmente sono disponibili versioni dotate di tecnologia integrata antimascheramento.

I vari modelli poi, condividendo il medesimo case a profilo ribassato, non consentono di identificare il tipo di rivelatore installato, caratteristica questa che si è dimostrata un ulteriore ed efficace deterrente.

È possibile utilizzare la stessa staffa per il montaggio a parete o a soffitto per tutti i modelli disponibili.

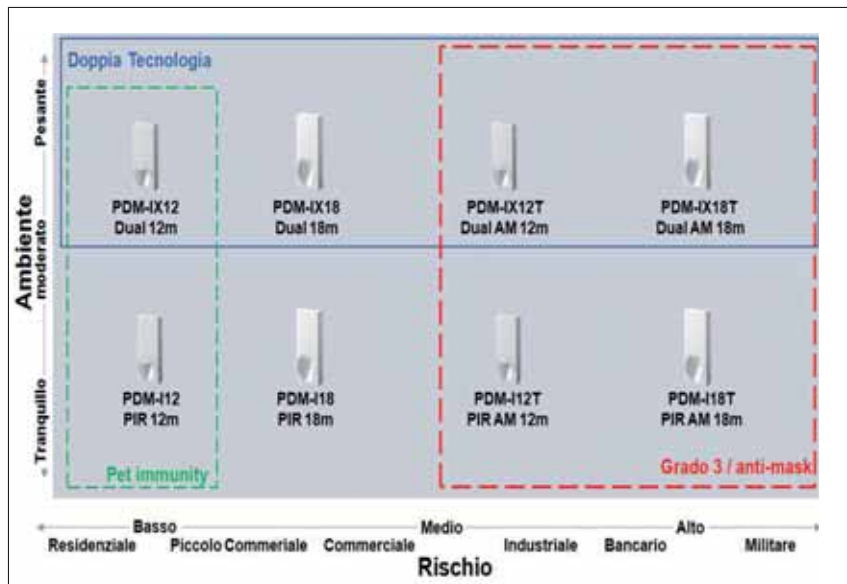
L'adattamento ai vari modelli di centrale antintrusio-



ne è semplice, rapido e non comporta difficoltà.

Naturalmente, il collegamento alle centrali Siemens SPC, come alle altre attualmente a listino, è semplice, veloce e intuitivo. Per utilizzare i rilevatori Magic con altri tipi di centrale, invece, è sufficiente sostituire le resistenze esistenti con le versioni specifiche (l'installazione è immediata e non richiede l'uso di viti di serraggio).

Grazie all'elettronica ad alta efficienza energetica, tutti i rilevatori Magic Mirror consumano significati-



vamente meno energia rispetto ad altri modelli. Nel 2013, ancora prima del lancio ufficiale sul mercato e quindi in fase di prototipo, i rivelatori Magic Mirror di Siemens sono stati premiati con il prestigioso premio “Red Dot Award: product design” per il loro design innovativo e accattivante.

**In sintesi... Magic: un nome che nasce da...**

### Filtri multipli a protezione del sensore

Una matrice di filtri protegge il sensore dalle interferenze causate dalla presenza fortuita e indesiderata di luce bianca, favorendo la massima immunità ai disturbi.



### Imaging avanzato delle zone di rilevazione

La tecnologia a doppio specchio crea delle zone di rilevazione a sensibilità costante, per garantire una copertura omogenea e prestazioni di rilevazione affidabili.

### Grandi prestazioni di rilevazione

La garanzia di prestazioni uniformi in tutta l'area di copertura e l'impiego di un algoritmo di rilevazione avanzato (Visatec, Matchtec) massimizza la sensibilità senza compromettere l'affidabilità di rilevamento delle intrusioni.

### Ottica anti-mascheramento integrata

La funzione anti-mascheramento integrata nello specchio MAGIC garantisce la massima protezione della finestra di rilevazione.

### Design compatto

L'impiego di un doppio specchio ne riduce le dimensioni, a vantaggio della compattezza della custodia, che si presenta eccezionalmente sottile e di piccole dimensioni.

## CONTATTI

Security Products di Siemens  
 (+39) 02 24365358  
[www.magic-detector.com](http://www.magic-detector.com)  
[www.siemens.it/securityproducts](http://www.siemens.it/securityproducts)



# INT-TSI Tastiera Touch 7” Sicurezza e Domotica senza limiti con Satel

a cura della Redazione



**U**n'azienda che da anni investe in ricerca e sviluppo in maniera tanto significativa non poteva che lanciare sul mercato delle tastiere touch così innovative. L'obiettivo primario per SATEL è sempre stato quello di rendere all'utente un servizio pressoché unico, e cioè di dargli la possibilità di interagire con il suo sistema di allarme in modo semplice e fluido. La strada da percorrere è stata aperta dai produttori di smartphone e tablet e Satel ha voluto cogliere questa ondata di tecnologia affiancando alle tastiere tradizionali un nuovo standard di livello qualitativo altissimo sugli organi di comando. Da questa idea innovativa è nata INT-TSI. INT-TSI è un vero e proprio centro di controllo intelligente del sistema INTEGRA. Grazie alla sua tecnologia spinta e a un'attraente interfaccia grafica, INT-TSI è in grado di soddisfare gli utenti e gli installatori più esigenti. Le innumerevoli possibilità di configurazione offerte dai sistemi INTEGRA richiedono una gestione all'altezza delle potenzialità della centrale. INT-TSI introduce quindi una nuova qualità di utilizzo dei sistemi di allarme.

## Intuitiva, facile, piacevole

La INT-TSI racchiude una tecnologia avanzata: un efficiente processore garantisce un funzionamento fluido dell'estesa interfaccia grafica e i componenti di alta qualità utilizzati consentono le azioni con una scorrevolezza unica, semplicemente sfiorando lo schermo in vetro. Il potente software TSI-BUILDER offre la possibilità di configurare un sistema che associa sicurezza e home automation con standard di massima professionalità. Le soluzioni futuristiche applicate nell'INT-TSI offrono all'installatore progettazioni illimitate dell'interfaccia utente. Tale personalizzazione rende l'utilizzo quotidiano unico, intuitivo, facile e piacevole.

## Operazioni complesse rese semplici: l'aiuto dei widget

INT-TSI è stata pensata per garantire, in modo comodo e facile, la gestione quotidiana del sistema. In fase di progettazione abbiamo pensato di presentare le funzioni disponibili con icone dai colori vivaci, widget attraenti per garantire una vera interazione



tra l'utente e il sistema. I widget della INT-TSI possono: eseguire scenari, essere tasti di controllo del sistema di sicurezza e automazione, indicare lo stato dei singoli elementi, agire da pulsanti interattivi che cambiano di stato al verificarsi di un comando. Allo schermo inoltre possiamo aggiungere dei widget con la visualizzazione immediata di ora, data e temperatura. È possibile assegnare icone personalizzate alle singole funzioni al fine di rendere più facile l'uso della tastiera. I singoli widget possono essere posizionati e replicati in schermate differenti che possono essere aperte facilmente utilizzando la barra laterale delle funzioni. Grazie a questa particolarità i widget possono essere raggruppati a piacimento, rendendo così più facile trovare le funzioni richieste. Quando è necessaria l'immissione del codice utente, le icone vengono sostituite automaticamente da una finestra con tastierino numerico per inserire la password.

### Facile accesso agli elementi di base

Lo schermo base è stato pensato per essere organizzato in modo tale che l'utente possa accedere velocemente ai tasti preposti all'accensione e allo spegnimento dell'allarme, avere l'accesso a funzioni aggiuntive, così come lanciare velocemente una "richiesta di soccorso": è sufficiente infatti sfiorare l'icona che indica il tipo di minaccia.

### Home automation

La caratteristica che rende INT-TSI ideale per un sistema domotico è la possibilità di eseguire con un solo tocco sequenze di azioni attraverso ogni widget. Per esempio, il comando "film" può abbassare le tapparelle, far scendere lo schermo di proiezione e regolare la luce ideale per la visione.

Gli scenari permettono anche un controllo degli impianti di riscaldamento, aria condizionata, tende, porte di ingresso e garage, nonché l'irrigazione del giardino. Grazie alla completa integrazione tra la centrale INTEGRA e il protocollo domotico KNX è anche possibile controllare tutti dispositivi KNX attraverso i widget della INT-TSI.

### Visualizzazione immagini delle telecamere

Le funzionalità di INT-TSI non si fermano al solo controllo del sistema di allarme e automazione, ma offrono la vera integrazione con i sistemi TVCC. Grazie alla possibilità di visualizzare le immagini delle telecamere, INT-TSI rappresenta il nuovo centro di controllo della sicurezza. In un colpo d'occhio l'utente ha sempre tutto sotto controllo.

È possibile visualizzare sullo schermo immagini video relative, per esempio, alla telecamera installata vicino al cancello per verificarne l'apertura o in caso di allarme per accertare la presenza di estranei.



### Modalità tastiera virtuale

La modalità terminale simula il funzionamento di una tastiera INTEGRA tradizionale. Tale soluzione è comoda per quelle persone che sono abituate al funzionamento tradizionale del sistema. Al fine di garantire la massima sicurezza il tastierino si posiziona in modo casuale sullo schermo per evitare l'individuazione della password tramite le impronte.

### Gli sfondi e il design

Anche lo sfondo della tastiera può essere liberamente scelto dall'utente, a seconda dei suoi gusti e della sua immaginazione, da una libreria di immagini già pronte o può essere personalizzato con una foto. Questa tastiera dal design accattivante e moderno è disponibile in due colorazioni per adattarsi a tutti gli stili d'interno. Lo spessore di soli 22 mm le permette una perfetta e discreta integrazione con l'ambiente.

### Personalizzazione totale: il PLUS per utenti e installatori

Finalmente è giunto il momento in cui l'installatore può domandare al suo utente cosa vuole visualizzare sulla tastiera, quali icone gli facilitano i comandi e quali informazioni vuole leggere.

Oggi l'installatore ha finalmente il modo di far valere la sua professionalità, con INT-TSI è in grado di proporre all'utente un'interfaccia grafica intuitiva e facile, non deve più spiegarne ripetutamente il funzionamento perchè è la tastiera stessa che lo suggerisce. Una caratteristica unica di INT-TSI è quindi la possibilità di

personalizzare l'interfaccia individualmente per ogni utente - sia in termini di funzionalità che di icone proposte. Per esempio, per chi utilizza esclusivamente le funzioni di base, la tastiera visualizzerà soltanto quelle, mentre gli utenti più avanzati potranno utilizzare la versione estesa dell'interfaccia.

La possibilità di personalizzazione di INT-TSI non si limita soltanto alle icone o ai widget. Il software di configurazione infatti consente di utilizzare uno dei tre temi grafici predefiniti, che offrono tre stili di visualizzazione completamente diversi anche sulle barre degli strumenti.

**Con INT-TSI si può liberare la creatività per un look unico!**

#### CONTATTI

SATEL ITALIA SRL  
 (+39) 0735 588713  
[www.satel-italia.it](http://www.satel-italia.it)

# Da TSEC i più piccoli contatti magnetici di Grado 3 sul mercato

a cura della Redazione

**F**in dalla loro introduzione sul mercato alla fine del 2012 i CLH-101 e 111 hanno attirato l'interesse di installatori e clienti finali per le loro caratteristiche uniche.

Si tratta di contatti magnetici anti-mascheramento costruiti interamente in Italia con tecnologia Magnasphere®. Quest'ultima merita una breve presentazione poiché rappresenta un vero e proprio cambiamento epocale nella protezione perimetrale dei varchi. I classici contatti basati su tecnologia Reed sono facilmente attaccabili. È infatti

semplice mascherare l'assenza del magnete di riscontro di un contatto Reed, ovvero l'apertura della porta, con l'applicazione di un magnete all'esterno del varco anche ad allarme inserito, e avere quindi accesso indisturbato.

## Principio di funzionamento della tecnologia Magnasphere®

In applicazioni ad alta sicurezza la soluzione è stata fino a oggi l'impiego di sensori a "triplo bilanciamento magnetico", seppure con un notevole ag-





gravio in termini di costi e dimensioni installative. I CLH-101 e 111 hanno dimensioni davvero contenute, 15x15x50 mm e si caratterizzano per il design elegante ed essenziale. Altra prerogativa importante è la robustezza in quanto il cuore del sensore è metallico e non in vetro. La completa resinatura ne garantisce l'assoluta impermeabilità (classe ambientale IV).

I sensori possono essere forniti con resistenze di doppio bilanciamento già integrate; questa caratteristica li rende ottimali in situazioni in cui è richiesto un grado di sicurezza elevato facilitando notevolmente il lavoro dell'installatore e riducendo drasticamente i tempi di installazione.

Rispetto ai contatti tradizionali a triplo bilanciamento, i CLH-101 e 111 non hanno distanza minima di installazione tra sensore e magnete, vero punto debole dei contatti ad alta sicurezza tradizionali, e quindi, se correttamente posizionati, conferiscono una maggiore sicurezza al controllo del varco.

Dallo scorso anno tutti i sensori della linea CLH hanno ottenuto da IMQ la certificazione al Grado 3

secondo la norma EN 50131.

Ultima caratteristica, ma non per questo meno importante: il prezzo molto competitivo è un indubbio fattore del successo ottenuto dai CLH-101 e 111 presso i più importanti utilizzatori nel settore bancario e della grande distribuzione.

#### CONTATTI

TSEC SRL  
 (+39) 030 5785302  
 www.tsec.it

# La via di Mondialpol per la tutela delle banche clienti

*a colloquio con Fabio Marchesi, ad Mondialpol Facility  
a cura di Raffaello Juvara*

**Mondialpol Group è uno dei principali operatori italiani del trasporto valori. Quali sono le dimensioni attuali del gruppo e come è dislocato sul territorio?**

I due parametri essenziali per delineare le dimensioni di un operatore di questo settore sono il fatturato e il numero dei dipendenti. Il fatturato aggregato del Gruppo Mondialpol è stato di circa 200 milioni nel 2013, con una crescita dell'11% rispetto all'anno precedente. Dal 2009 al 2013 la crescita costante del fatturato (CAGR) è stata del 14%, ottenuta sia per linee interne che per effetto di acquisizioni e di aperture di nuove business unity. I dipendenti complessivi sono circa 1500. La presenza sul territorio è diversa in funzione dei servizi svolti: nel trasporto valori viene garantita la copertura totale del territorio italiano in forma diretta e indiretta, con esclusione di Calabria e Sicilia, la contazione è assicurata in forma diretta nelle regioni settentrionali, centrali e Sardegna; la vigilanza nelle province in cui opera storicamente il gruppo.

**Il gruppo è da tempo un operatore di 1° livello, in grado cioè di stipulare direttamente i contratti con le banche e gli altri grandi clienti e di distribuire fasi di lavorazione a propri corrispondenti sul territorio. Come viene gestita e controllata la regolarità di queste lavorazioni delegate a terzi?**

È appena il caso di ricordare che attraverso Mondialpol Network e Mondialpol Service possiamo agire con mandato su tutto il territorio nazionale. Queste società sono autorizzate come "Agenzia di



affari" in virtù di una specifica licenza – ex art. 115 del TULPS - e, come tali, abilitate a ricevere mandati con e senza rappresentanza.

**Come nasce l'attribuzione delle attività di audit a una realtà come Mondialpol Facility?**

Mondialpol Facility è un'azienda del Gruppo Mondialpol Service Group composta totalmente da



professionisti certificati ai sensi della norma UNI 10459:1995 e dislocati sul territorio nazionale, coordinati operativamente dal sottoscritto.

Le attività che svolge sono essenzialmente di risk assessment, risk analysis, risk management e fraud management, attraverso la costante acquisizione e analisi di dati, valutazioni preliminari, check list e altri strumenti.

Nel momento in cui i vertici di Mondialpol Service Group hanno inteso avviare l'attività di verifica e audit presso i centri di contazione valori, la scelta di affidare il compito a Mondialpol Facility è stata "naturale".

Tuttavia si è reso necessario un lungo periodo di formazione e test prima che l'attività partisse a pieno regime.

**Quali sono i controlli che effettua Mondialpol Facility?**

Sono numerosi: si va dall'esame del contesto operativo generale (ordine e pulizia dei locali, situazione logistica interna) alla verifica del sistema gestionale, cioè della corretta tracciatura delle banconote presunte false, di quelle macchiate o danneggiate,

e della chiara evidenza nei tabulati della divisione delle banconote per tipologia (buone, logore, false, danneggiate), dal controllo dell'applicazione del provvedimento della Banca d'Italia del 14 febbraio 2012 (Disposizioni relative al controllo dell'autenticità e idoneità delle banconote in euro e al loro ricircolo, NdR) all'accertamento sulla formazione (presenza di funzionigrammi, organigrammi e registri di attività di formazione) e sull'adeguatezza alle normative delle apparecchiature per la selezione e l'autenticazione delle banconote, compresa la presenza dei manuali d'uso, dei contratti di manutenzione e di aggiornamento. Attenzione particolare viene dedicata alla sicurezza (verifica della funzionalità del controllo accessi, degli impianti di videoregistrazione, degli allarmi) e alla lavorazione e spedizione degli assegni (utilizzo dei lettori, confezionamento e archiviazione delle immagini).

Fondamentale, naturalmente, è il puntuale controllo della coerenza tra contante e assegni e delle evidenze contabili con la conseguente certificazione della giacenza riscontrata. Il nostro audit non si limita soltanto a una valutazione indipendente, a una "fotografia" del centro contazione. È, in un certo

senso, dinamico, in quanto uno dei nostri obiettivi primari è quello di fare presente all'istituto di credito eventuali criticità, indicando anche ipotesi di soluzioni.

Mondialpol agisce in estrema trasparenza e comunica al cliente ogni attività svolta e il modo in cui è stata svolta. L'audit si conclude con una check list di tutte le verifiche effettuate, alla quale si aggiunge un report per la banca con le considerazioni conclusive e un giudizio sulla conoscenza della normativa da parte del personale intervistato. Da questo la banca cliente può capire se ci sono aspetti che devono essere migliorati. Perché quando si tratta di denaro non ci si può fermare a un formale adeguamento alla normativa, occorre agire nella massima sicurezza e trasparenza, anche per prevenire comportamenti scorretti.

#### **L'audit viene quindi ad avere una finalità di prevenzione di possibili "inconvenienti"?**

Certamente sì, perché permette da un lato di sensibilizzare e concorrere alla formazione e all'aggiornamento degli operatori, mentre dall'altro permette di cogliere alcuni cosiddetti "segnali deboli" o elementi oggettivi di criticità su cui basare interventi di varia entità e natura, fino alla risoluzione del rapporto, a tutela e garanzia dell'Istituto Bancario per cui conto è condotto l'audit.

**Recenti episodi di diversa gravità hanno fatto comprendere come il sistema del trasporto valori sia una infrastruttura critica a tutti gli effetti, essendo il gestore della logistica del contante. Il default improvviso di un elemento della supply chain può quindi determinare effetti molto gravi sulla collettività. Come si può affrontare la continuità nel trasporto valori? Quali sono le scelte di Mondialpol Group?**

È un tema di estrema attualità, che deve essere affrontato in modo responsabile da tutte le parti interessate. Per questo motivo Mondialpol ha costituito la prima rete d'impresa del settore Trasporto, Contazione e Custodia Valori assieme al gruppo Fidelitas di Bergamo. "Continuità Valori" è il nome scelto per questa prima rete d'impresa per rispondere efficacemente alle richieste, da parte delle istituzioni e della clientela, di garanzia della continuità operativa a seguito di eventi che possano provocare gravi interruzioni di servizio. Il mercato di riferimento del nostro settore può contare su questa nostra iniziativa, che ha lo scopo di garantire a tutta la clientela – cittadini, aziende, banche, enti pubblici – non soltanto la continuità operativa in caso di eventi critici, che abbiamo visto aumentare negli ultimi mesi, ma anche la qualità e la sicurezza dei processi di lavorazione dei valori e, in generale, di affidabilità di impresa e di professionalità nei servizi.





# Security for Retail Forum · SRF



## 64 Milestone e AXIS insieme per la sicurezza di Paul Smith

*a cura di Cristina Isabella Carminati*

## 68 Il Barometro dei furti nel retail offerto da Checkpoint

*a colloquio con Alberto Corradini, Sales Director di Checkpoint Systems  
a cura della Redazione*

## 70 Retail, come proteggere dispositivi, dati e reti con PCI - DSS 3.070

*un libro bianco di Ergonomic Solutions  
prefazione di Chris Field, Fieldworks Connections*

**AON** BENFIELD

  
ASSOVALORI

**CTS**

**GUNNEBO**  
For a safer world.

 nedap | retail

**tyco**

# Milestone e AXIS insieme per la sicurezza di Paul Smith

a cura di Cristina Isabella Carminati

**E**ntro il 2015 la famosa catena inglese di abbigliamento Paul Smith installerà nei propri negozi in 35 Paesi nel mondo sistemi video IP centralizzati a Nottingham, con il VMS di Milestone e le camere di Axis.

Paul Smith è uno dei principali retailer di moda del Regno Unito, con uffici e showroom nelle città chiave della moda mondiale, tra cui Londra, Milano, New York, Parigi, Amsterdam, Anversa, Düsseldorf e Sydney, e store in 35 paesi nel mondo. Attualmente conta 24 punti vendita nel solo Regno Unito. La crescita della società negli Stati Uniti e in Europa continua: il progetto è di aprire almeno cinque nuovi negozi ogni anno per i prossimi cinque anni. L'azienda ha un fatturato annuo superiore a 400 milioni di sterline. Il fondatore, Sir Paul Smith ha aperto il suo primo negozio nella nativa Nottingham nel 1970, all'età di 24 anni, ed è ormai affermato come uno tra i più grandi stilisti inglesi.

Il software di gestione video IP open platform Milestone XProtect® Corporate (VMS) con XProtect® Smart Client e le telecamere di rete di Axis Communications sono stati distribuiti in tutti i 45 store Paul Smith e rappresentano l'inizio dell'azione di rinnovamento IT dell'azienda britannica.

Inizialmente il nuovo sistema video digitale verrà usato ai soli fini di loss prevention ma Paul Smith ha già previsto che, dopo aver completato l'installazione in tutti i negozi nel mondo entro la fine del 2015, sarà impiegato anche per la business intelligence a supporto della gestione operativa delle vendite.

Paul Smith è uno dei primi utilizzatori di IP e di ser-



Lee Bingham

vizi cloud-based. Nel 2001 è stata la prima grande azienda britannica a migrare verso la telefonia IP installando una rete Cisco IPT. Aprendosi alle più recenti tendenze della gestione IT, compreso l'impiego di sistemi ad architettura aperta su base Microsoft, il gruppo ha potuto mantenere il team dedicato ai servizi di rete di dimensioni relativamente piccole, malgrado una crescita davvero rapida. Paul Smith è

presente con punti vendita in 35 Paesi.

Questo approccio spiega il fatto che quando si presentano nuove sfide IT, il direttore della sezione IT di Paul Smith, Lee Bingham, cerchi soluzioni standard-based scalabili rapidamente ed efficacemente. Bingham specifica che i nuovi sistemi e servizi devono durare per almeno 10 anni, semplicemente perché non ci sono personale e budget sufficienti per sostenere continue sostituzioni di dispositivi e software.

Il CCTV preesistente di Paul Smith è cresciuto organicamente man mano che il gruppo ha aperto store in tutto il mondo. Quando al settore IT è stato chiesto di gestire i sistemi video, Lee Bingham ha insistito per migrare al video IP e ha preteso che il sistema video fosse visibile sulla rete corporate: «Se non è IP allora non è IT, e quindi non aveva senso spostare la sua gestione dal team Facility Management all'IT department, a meno che il sistema CVTT fosse accessibile in rete sui desktop dei manager».

La società ha approvato il piano triennale presentato dal reparto IT per la migrazione totale dalla TVCC analogica al video IP. L'installazione e la messa in rete della nuova piattaforma video fanno parte dell'ag-

giornamento globale in corso delle infrastrutture IT, insieme all'apertura di nuovi punti vendita (POS) e alla pianificazione delle risorse (ERP).

Il reparto IT di Paul Smith ha cercato sul mercato una soluzione hardware e software di video IP robusto e scalabile. Dopo un accurato processo di valutazione, la scelta è caduta sul software di gestione video Milestone XProtect Corporate e sulle telecamere di rete Axis. Sono stati scelti anche i codificatori video Axis per portare alcune telecamere analogiche esistenti sulla rete aziendale, in attesa dell'aggiornamento completo IT e video IP.

Lee Bingham, responsabile del reparto IT di Paul Smith ha dichiarato: «Il fatto che Milestone XProtect sia costruito su una piattaforma ad architettura aperta che utilizza Microsoft Active Directory rende possibile un rapido roll-out, come il controllo dei costi di manutenzione e di supporto. Scegliendo Milestone ci possiamo permettere di far migrare l'intero parco TVCC su una sola piattaforma consolidando uniformità e coerenza».

«Milestone si adatta perfettamente al nostro modello», continua Bingham. «La piattaforma ad architettura

**ASSA ABLOY**  
leader mondiale  
nei sistemi di sicurezza  
vi aspetta a  
ELF Convention 2014

**ELF Convention 2014**  
The annual Congress of the European Locksmith Profession

Palazzo degli Affari, Firenze  
23 - 24 maggio

**ASSA ABLOY**  
The global leader in  
door opening solutions

[www.assaabloy.it](http://www.assaabloy.it)



ra aperta consente la scalabilità e l'aggiunta di nuovi servizi. Possiamo controllare che i nostri gestori possano vedere le telecamere in negozio attraverso le nostre tecnologie IT standardizzate. Possiamo effettuare il login tramite il front-end Milestone XProtect Smart Client per visualizzare video in diretta e video registrati dalle telecamere in tutto il mondo. Se c'è un problema, in linea di massima lo possiamo risolvere tramite la rete da Nottingham, senza salire su un aereo. Ciò consente di risparmiare sui tempi di gestione e riduce le emissioni di anidride carbonica della nostra azienda».

Per il futuro Bingham prevede che i diversi manager di ciascuna area specialistica, come per esempio il visual merchandising, accederanno in modo proattivo alle telecamere per valutare se il layout concordato degli store sia rispettato e funzioni bene per i clienti. Ci sarà anche un aumento della domanda di accesso tramite dispositivi mobili ai video che Milestone Mobile è in grado di fornire .

«Il nostro obiettivo, dato che i sistemi video basati

su Milestone sono stati lanciati a livello globale, sarà quello di capitalizzare questo investimento estendendo il loro valore al di là della mera loss prevention», conclude Bingham. «Abbiamo intenzione di lavorare a stretto contatto con il nostro team di retail management per esplorare le potenzialità del nuovo sistema video IP, le tecniche come il riconoscimento facciale, la mappatura del calore e l'analisi del tempo medio di permanenza che ci permettono di capire e servire meglio i nostri clienti».



The Open Platform Company

**Ideale:**  
azzerare il rischio di furti  
e rapine, escludere i falsi  
e ridurre l'immobilizzo del  
fondo cassa.

**Perfetto:**  
elimina conteggi manuali,  
gli ammanchi e i compiti  
ripetitivi.

**Gradito:**  
facile da usare,  
dà sempre il resto esatto,  
riduce le code alle casse.

**...e il Servizio?**  
Flessibile, rapido,  
affidabile.

In una parola:



il Sistema di  
trattamento denaro

## Soluzioni che creano valore

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



[www.gunnebo.it](http://www.gunnebo.it)

**GUNNEBO**  
For a safer world®

# Il Barometro dei furti nel retail offerto da Checkpoint

*a colloquio con Alberto Corradini, Sales Director di Checkpoint Systems a cura della Redazione*

**Quale trend viene evidenziato dall'edizione 2013 del Barometro dei Furti nel Retail, realizzato da Euromonitor su richiesta di Checkpoint Systems?**

Secondo il Barometro dei Furti nel Retail 2013 le differenze inventariali, a livello globale, sono in aumento, con una percentuale dell'1,4%. Sebbene i fenomeni di taccheggio rappresentino, in media, la causa principale delle differenze inventariali, seguiti dai furti dei dipendenti, le percentuali registrate variano in relazione alla categoria merceologica del retailer, alle sue dimensioni e al modo in cui viene gestita la prevenzione delle perdite. Lo studio evidenzia inoltre una crescita della criminalità organizzata, caratterizzata da bande che rubano principalmente articoli costosi, come farmaci e prodotti elettronici. A incidere su questo trend anche la crisi economica, indicata dai retailer come altra causa importante. Dobbiamo tuttavia sottolineare che sono state rilevate alcune eccezioni a questo incremento, che hanno dimostrato l'importanza di investire nella prevenzione delle perdite. Molti retailer tedeschi e inglesi hanno infatti confermato che il miglioramento delle tecnologie ha contribuito ad arginare le differenze inventariali.

**A livello globale i furti commessi dai dipendenti (30%) e dai fornitori (9%) quasi equivalgono a quelli commessi dai clienti (41%). In che modo la tecnologia può aiutare a contrastare il fenomeno delle "appropriazioni indebite"?**

In realtà non esiste un'unica tecnologia in grado di contrastare il fenomeno, ma una pluralità di sistemi, che insieme garantiscono una protezione efficace. Per questo all'uso di antenne antitaccheggio, solu-



oni per il libero tocco ed etichette RF/RFID si abbina l'utilizzo di telecamere a circuito chiuso e la presenza di addetti alla sorveglianza. Lo stesso Barometro ha confermato che la maggior parte dei retailer italiani sta implementando diversi sistemi per la prevenzione delle perdite, quali per esempio etichette o antenne EAS, soluzioni espositive, sistemi di acquisto con ticket per articoli come profumi, oltre alla sorveglianza con sistemi a circuito chiuso e personale dedicato. In particolare le soluzioni EAS sono state più volte indicate come il sistema di prevenzione delle perdite in grado di offrire il migliore ritorno sull'investimento,

in quanto i taccheggiatori trovano molte difficoltà nel rimuovere questo tipo di etichette.

**Come si colloca l'Italia nella classifica mondiale delle differenze inventariali? Quali sono le categorie di prodotti più colpite?**

Nel nostro paese i retailer ritengono che la percentuale di differenze inventariali sia cresciuta in particolare a causa della crisi economica e dei bilanci familiari ristretti, attestandosi all'1,3%. Fra le cause principali il taccheggio (49%) e i furti da parte dei dipendenti (27%). Seguono gli errori amministrativi e le frodi da parte dei fornitori. Gli articoli più rubati in Italia sono prodotti primari, di piccole dimensioni, facili da rubare e da nascondere e dal prezzo relativamente elevato. Naturalmente la tipologia di articoli più taccheggiate dipende dalla categoria merceologica. Per esempio nel food si rubano soprattutto vini, superalcolici, formaggi, carni e prodotti gastronomici di qualità, mentre nel fashion gli articoli più a rischio sono jeans, calzature, accessori moda e vestiti firmati. Per i retailer del settore brico home&garden nel mirino troviamo serrature per porte, cavi, batterie, viti e rondelle. iPhone, Smartphone e tablet sono invece nella top ten dell'elettronica, seguiti da fotocamere

digitali, GPS e DVD. Sono state segnalate infine variazioni stagionali importanti: il periodo natalizio, per esempio, è uno dei momenti più soggetti al fenomeno furti.

**I retailer chiedono livelli di integrazione sempre più elevati dei diversi sistemi di sicurezza (anti intrusione, anti taccheggio, videosorveglianza, etc.) e di business intelligence (video analisi comportamentale, controllo flussi, etc.). Quali sono gli scenari del prossimo futuro secondo Checkpoint?**

Il futuro secondo Checkpoint Systems sono le "merchandise availability solution", ovvero tecnologie in grado di contrastare il fenomeno dei furti e migliorare, al tempo stesso, l'esperienza di acquisto dei clienti, incrementando la redditività dei punti vendita. In tal senso la nostra azienda ha studiato nuove tecnologie basate su sistemi RFID, che assicurano una perfetta gestione dell'inventario e consentono al retailer di avere sempre il prodotto giusto al posto giusto e al momento giusto. Questo comporta un enorme vantaggio per il cliente, che sarà più soddisfatto e di conseguenza più fidelizzato verso il brand, e un beneficio per il retailer che potrà consolidare il business e la propria posizione sul mercato.



# Retail, come proteggere dispositivi, dati e reti con PCI - DSS 3.0

*un libro bianco di Ergonomic Solutions  
prefazione di Chris Field, Fieldworks Connections*

## **Perché la sicurezza dei pagamenti in-store non si limita a lucchetti e chiavi**

Nonostante l'avvento sia di una regolamentazione sia delle migliori pratiche in Europa per migliorare la sicurezza dei pagamenti, c'è ancora molta incertezza, da territorio a territorio, sulle modalità con cui i commercianti debbano raccogliere questa sfida.

Per alcuni, l'incertezza è stata sfruttata da fornitori che usano la paura per costringere i commercianti ad adottare misure che sono a volte eccessive, con il risultato di investimenti inutili, una scarsa ergonomia nel punto vendita e difficoltà per i consumatori che utilizzano i dispositivi di pagamento.

Talvolta, le misure adottate vanno nella direzione sbagliata, per esempio, se da un lato può apparire che soddisfino i requisiti delle linee guida del PCI Council, possono non funzionare in tutte le circostanze in un ambiente reale.

Resta il semplice fatto che, se da un lato la maggior parte degli aspetti degli standard PCI sono stati presi in considerazione dai produttori di terminali, l'ultima linea di difesa nei confronti dei potenziali criminali rimane sulle spalle del retailer. E questi criminali stanno diventando più intelligenti e più determinati da un giorno all'altro: ogni giorno, sono oltre 5.000 i terminali disponibili per le aste online, e i terminali legittimi nei negozi sono costantemente in pericolo.

Di conseguenza, i retailer sono inondati da società



*Chris Field, Fieldworks Connections*

operanti nel settore della sicurezza dei dispositivi di pagamento, in parte a causa dei requisiti loro imposti dal settore delle carte di pagamento, ma anche perché il problema della sicurezza dei dati continua a far notizia e ad aumentare le preoccupazioni dei consumatori.

Si tratta di preoccupazioni reali, evidenziate dall'impatto che pratiche negligenti di protezione dei dati possono avere sui retailer di qualsiasi dimensione;





tuttavia la pressione esercitata sui retailer affinché reagiscano a tali sfide arriva proprio in un momento in cui sono costretti a prestare attenzione come mai prima d'ora a ogni singolo investimento. Dovendo già operare in un ambiente difficile, i retailer sono costretti a concentrarsi maggiormente sull'esperienza del cliente, e con nuovi investimenti in dispositivi mobili che si connettono alla rete wireless e che tuttavia devono anche soddisfare i requisiti PCI DSS 3.0 per la protezione dei dati.

Abbiamo deciso di lavorare con il leader del mercato, Ergonomic Solutions, su richiesta dei nostri retailer associati per portare un po' di buon senso nel problema, pubblicando una guida sulle migliori pratiche sulla sicurezza dei dati di pagamento che abbraccia non soltanto la sicurezza fisica dei terminali e degli altri dispositivi di pagamento, ma anche le implicazioni della PCI compliance sulla sicurezza, gestione, registrazione e manutenzione dei dispositivi, come pure sull'ambiente di pagamento.

La nostra missione è quella di analizzare il problema in modo imparziale e aiutare i commercianti a capire le loro possibilità di scelta in modo che possano prendere decisioni in base alle loro esigenze specifiche.

Utilizzando questa guida, i commercianti potranno con maggiore facilità rispettare pienamente le raccomandazioni PCI DSS 3.0 su:

- sicurezza fisica dei terminali di pagamento;
- ambiente dei pagamenti;
- prevenzione della strisciata;
- valutazioni del rischio.

Questo approccio è sostenuto dalle primarie organizzazioni in materia di pagamenti, da VeriFone a Visa e segue le linee guida e i requisiti pubblicati dal PCI Council.

*Chris Field*

Fieldworks Connections

### **Le minacce**

Qualcuno nel settore dei pagamenti ha voluto incutere paura per spingere i commercianti lungo l'irto percorso di una sicurezza a volte eccessiva, a volte

errata e, altre volte, inutile dei dispositivi fissi e mobili in-store e altri componenti aggiuntivi per il punto vendita.

Significativi investimenti vengono operati nei terminali di pagamento, per cui l'ultima cosa di cui numerosi retailer vogliono sentir parlare è che debbano spendere ancora più soldi sulla sicurezza dei dispositivi. L'approccio onesto consiste nell'aiutarli a comprendere i rischi e creare un proprio profilo di rischio sulla cui base operare qualsiasi successivo investimento. Ciò contrasta nettamente con gli spacciatori di paura unicamente interessati a vendere apparecchiature.

Occorre quindi raggiungere un compromesso tra inerzia e reazione eccessiva.

La PCI DSS 3.0, 9.9 afferma che un esercente deve proteggere da manomissioni e sostituzioni i dispositivi POS (point-of-sale) che acquisiscono dati delle carte di pagamento attraverso l'interazione fisica diretta con la carta. Diventerà un obbligo per i dettaglianti a partire dal 30 giugno 2015.

Per i dispositivi mobili la guida asserisce che laddove un esercente possiede o è in altro modo responsabile di un dispositivo mobile utilizzato nell'ambito di una soluzione di pagamento, spetta all'esercente adottare misure per consolidare e mantenere la sicurezza del dispositivo. Le misure descritte in questa sezione devono essere applicate anche a eventuali componenti hardware aggiuntivi che fanno parte della soluzione mobile di accettazione dei pagamenti (per esempio lettori di schede).

### **Impedire accessi non autorizzati al dispositivo fisico**

Il dettagliante è tenuto ad assicurare l'integrità e la sicurezza del dispositivo mobile e la sua conservazione in luogo sicuro quando non è in uso (per esempio chiudendolo a chiave in un armadietto, ancorandolo a un banco o tenendolo sotto sorveglianza 24 ore al giorno).

Le minacce sono reali e l'obbligo di ridurle ai sensi del Payment Council Industry Data Security Standard (PCI: DSS) è fondamentale se i retailer vogliono evitare multe e una perdita di fiducia dei clienti se i

dati vengono rubati.

Qualsiasi violazione della sicurezza dei dati delle carte di pagamento ha conseguenze di vasta portata sulle organizzazioni coinvolte, tra cui:

- obblighi normativi di segnalazione;
- perdita di reputazione;
- perdita di clienti;
- potenziali passività finanziarie;
- contenzioso.

Tuttavia, numerosi produttori di dispositivi di protezione fisica semplicemente ignorano la PCI e si concentrano soltanto sul dispositivo.

Ne derivano:

- investimenti errati;
- mancanza di redditività a lungo termine;
- mancata PCI compliance;
- il dispositivo selezionato diviene obsoleto molto prima di arrivare al ritorno dell'investimento;
- il dispositivo selezionato agisce da deterrente per i truffatori, ma allontana anche i clienti.

La paura può tendere a superare gli istinti naturali dei retailer ad assicurarsi che tutti gli investimenti in tecnologia e apparecchiature siano supportati da un solido ritorno dell'investimento e da un modello di costo totale di gestione. Questo è sbagliato, poiché per acquistare i retailer non soltanto vogliono comprendere la concreta redditività finanziaria, ma anche benefici più intangibili ma comunque cruciali in termini di esperienza del cliente.

Occorre considerare pro e contro tra sicurezza, ac-

cessibilità e design. La soluzione deve tenere conto della situazione futura e non limitarsi a risolvere un problema e poi ad ammortizzare.

### **Non si tratta soltanto del dispositivo**

Poiché gli standard PCI riguardano la protezione dei dati, è importante proteggere non soltanto il dispositivo ma tutto il cablaggio che lo collega alla rete, la rete a cui si appoggia e l'intero l'ambiente a cui si appoggiano la rete e i dispositivi. Trattando le apparecchiature indipendentemente dalla rete si corre il rischio di molteplici soluzioni fra loro incompatibili, di settori che possono passare inosservati, di una possibile duplicazione degli sforzi ed è possibile che un modello di ritorno dell'investimento non trovi facilmente conferma.

Concentrarsi sul soltanto dispositivo può comportare costi significativi:

- se il dispositivo non è fissato, può cadere durante il passaggio fra il personale e i clienti;
- il cablaggio si usura con il rischio che il dispositivo passi alla modalità antisabotaggio divenendo di fatto inutilizzabile;
- mettere in sicurezza il soltanto dispositivo non necessariamente dissuade da frodi su altre parti della rete, per esempio sui cavi.

Dobbiamo quindi considerare due aspetti principali:

- mettere in sicurezza il dispositivo, sia fisso che mobile;
- mettere in sicurezza l'ambiente.



ergonomic solutions

# vigilanza & dintorni



la piattaforma multimediale per :  
vigilanza  
servizi fiduciari  
trasporto valori  
trattamento del denaro

## 74 ANIVP, quando le associazioni sono al servizio delle imprese

*a colloquio con Andrea Menegazzi, presidente A.N.I.V.P.*

*a cura di Raffaello Juvara*

## 76 Nemici per la pelle ma uniti contro il DM 269

*di Gossip Particolare Giurato*



# ANIVP, quando le associazioni sono al servizio delle imprese

*a colloquio con Andrea Menegazzi, presidente A.N.I.V.P.  
a cura di Raffaello Juvara*

ANIVP ha firmato all'inizio dello scorso febbraio, insieme alle altre associazioni della vigilanza Assvigilanza e Univ facenti capo a Federsicurezza, il CCNL per la vigilanza privata e i servizi fiduciari con i sindacati Filcams/CGIL e Fisascat/CISL.

Con questo importante passaggio è stata superata la divisione della categoria, che si era determinata a seguito della sottoscrizione da parte di Federsicurezza alla fine del 2012 di un CCNL per i servizi fiduciari con il solo sindacato Uiltucs/UIL, che aveva provocato disagi alle imprese della vigilanza e ai lavoratori coinvolti.

## **Quali sono gli effetti della firma del CCNL sul piano contrattuale per i lavoratori e per le aziende facenti capo a ANIVP, Assvigilanza e Univ?**

Sul piano contrattuale i lavoratori avranno un trattamento economico e normativo analogo a quello degli altri lavoratori del settore ai quali è stato applicato il CCNL firmato nel febbraio del 2013; inoltre sarà riconosciuto loro un importo sotto forma di una tantum a copertura del 2013. Per le aziende vi è una normalizzazione rispetto agli altri operatori del mercato.

## **Secondo Lei quale validità ha ora il CCNL per i soli servizi fiduciari sottoscritto da Federsicurezza con Uiltucs, e quali aziende lo applicano?**

Abbiamo sottoscritto anche noi il CCNL per i servizi fiduciari con Uiltucs. Rammento infatti che abbiamo ampliato l'oggetto statutario dell'associazione già dal 2009. Ritengo che, senza dubbio, continuerà a essere valido. Le aziende associate, anzi, ora possono disporre di un altro strumento pensato per i servizi fiduciari e in pratica possono decidere autonomamente quale CCNL applicare. Certo il proliferare dei CCNL non è positivo, ma in qualità di presidente mi trovo davanti a una pluralità di riferimenti e opportunità per il bene degli



associati che non posso non considerare.

**In quale modo la firma diretta da parte delle associazioni datoriali ANIVP, Assvigilanza e Univ di un CCNL modifica il quadro di riferimento precedente, con Federsicurezza che aveva firmato il CCNL della vigilanza scaduto nel 2008, in rappresentanza delle associazioni?**

In realtà il precedente contratto non era stato sottoscritto da Federsicurezza nel vero senso della parola, in quanto il riferimento alla federazione era riportato soltanto nella copertina e nel verbale di accordo; scorrendo il CCNL risulta evidente che lo stesso era stato stipulato dalle singole associazioni di categoria aderenti a Federsicurezza. Non a caso lo statuto di Federsicurezza prevede espressamente la potestà contrattuale in capo alle associazioni. Federsicurezza nella dinamica relazionale che porta ai contratti è un importante momento di confronto e sintesi delle diverse componenti.

**Il presidente di Federsicurezza, avv. Luigi Gabriele, aveva pubblicamente dichiarato lo scorso mese di settembre che il progetto Federsicurezza “era da ripensare”. Ritieni che questo ultimo passaggio relativo al CCNL vada nella direzione di un “ripensamento” della federazione come evocato da Gabriele?**

Federsicurezza è nata nel 2005: sta per compiere 10 anni. In questo lasso di tempo, e direi soprattutto negli ultimi anni, molte cose sono accadute. Federsicurezza ha ampliato la sua sfera d'azione ricomprendendo non soltanto il settore della vigilanza privata, che tra l'altro ha visto l'entrata anche di ANIVP, ma anche quelli dei servizi fiduciari, della geolocalizzazione dei mezzi in movimento e quindi

di gran parte del settore della security.

Non posso quindi fare altro che confermare la necessità di organizzare e strutturare Federsicurezza in modo più adeguato ai tempi e alle necessità. Federsicurezza è impegnata su diversi fronti, non ultimo quello di monitorare in via continuativa l'andamento del mercato della sicurezza in Italia. Non dimentichiamo poi che Federsicurezza è l'unica organizzazione

nazionale presente in Co-ESS, la confederazione europea dei servizi di sicurezza che sempre più è in stretto contatto con la Commissione Europea per tutti gli aspetti legati alla security privata europea al fine di gestire i necessari correttivi.

**Quali sono i progetti di ANIVP per rappresentare gli interessi delle imprese associate, sul piano istituzionale e del**

**supporto nella fase di cambiamento epocale che sta vivendo il settore?**

Fin dalla sua nascita ANIVP ha cercato di fornire agli associati un servizio informativo e di consulenza che ancora oggi a mio parere non ha rivali.

Molti associati hanno riconosciuto la capacità dell'associazione di dare risposte precise e chiare. La circolazione delle informazioni soprattutto verso gli associati in ANIVP è continua.

ANIVP siede in tutti i tavoli ove si definiscono le sorti del settore e attua ogni sforzo per contribuire in modo fattivo a supportare l'attività imprenditoriale degli associati. In questi anni ANIVP si è resa protagonista di molte iniziative, intervenendo direttamente o tramite Federsicurezza presso tutte le sedi ritenute opportune, non tralasciando neppure iniziative in sede di Commissione Europea. ANIVP fin dalla sua nascita - o meglio rinascita - ha cercato di seguire e cavalcare il cambiamento e sicuramente proseguirà così per i prossimi anni.



**ASSOCIAZIONE NAZIONALE  
ISTITUTI DI VIGILANZA PRIVATA**

# Nemici per la pelle ma uniti contro il DM 269

di Gossip Particolare Giurato

**L**a tavola rotonda di Vigilanza & Dintorni sull'applicazione del DM 269 prevista per il 16 maggio a Medity Expò è stata pensata con il dichiarato e puntuale intento di mettere in chiaro i motivi della ripulsa che sta montando nel mondo della vigilanza nei confronti del decreto, e cercare di capire come trovare una via di uscita da una situazione assai critica.

Sostanzialmente divisi in due "scuole di pensiero" che si contrappongono su ogni cosa, gli operatori convergono soltanto su un punto, seppure con motivazioni del tutto opposte: **il DM 269 è una iattura inapplicabile al settore.**

Da una parte, la scuola dei **Favorevoli ma Pentiti (FmP)** è costituita dalle realtà più strutturate, non necessariamente le più grandi, che vorrebbero una concorrenza basata su fattori qualitativi misurabili, e non soltanto sul fattore prezzo. Avevano accolto con favore l'introduzione dei requisiti minimi previsti dalla norma volontaria UNI 10891 come standard della norma cogente, ma si attendevano: a) controlli rigorosi *erga omnes* sulla corretta applicazione da parte delle questure; b) certezza delle sanzioni da parte delle prefetture e dei TAR in caso di irregolarità riscontrate dalle questure.

Allo stato attuale, gli **FmP** si considerano beffati dallo Stato, perché sostengono di aver investito tempo, risorse e denaro per adeguarsi ai requisiti previsti dal DM, ma ora starebbero subendo la concorrenza sleale di operatori che, invece, non si sarebbero adeguati, nei confronti dei quali non verrebbero effettuati i controlli previsti e, soprattutto, non verrebbero applicate le sanzioni dovute.

Ritengono, pertanto, che a questo punto tanto varrebbe avere tutti le mani libere, e vinca il più forte!

Dall'altra parte c'è la scuola dei **Contrari a Prescindere (CaP)**, nella quale si riconoscono principalmente i piccoli imprenditori autonomi che, fin dal primo giorno, vivono il DM come un attentato alla libertà d'impresa. Sostenendo che i costi di adeguamento siano alla portata solamente dei grandi gruppi, i **CaP** accusano questi ultimi di aver oscuramente manovrato per abbattere il numero degli operatori in Italia tramite la "livella" del DM, e potersi quindi spartire la ricca torta del mercato nazionale senza la concorrenza dei "piccoli", espulsi non dall'utenza ma dagli organi di controllo. I **CaP** vorrebbero quindi una revisione globale dell'attuale testo del DM, puntando a un ribasso dei requisiti minimi per permettere alla piccole imprese di sopravvivere e di mantenere i posti di lavoro offrendo servizi "low cost" alla piccola utenza locale.

È consequenziale che avvertano la mancanza di controlli e/o sanzioni come una sorta di via indultiva per tirare avanti. Una contrapposizione che appare insanabile, risalendo all'atavico scontro tra "grandi" e "piccoli". Per il decisore politico e gli organi di controllo non sarà facile trovare una sintesi condivisa, anche per la contestuale emersione di un altro problema, più insidioso ancora: una strisciante frattura tra gli uffici centrali e quelli territoriali dell'Amministrazione.

Molti sostengono infatti che la mancanza di controlli e l'incertezza delle sanzioni, viste come una dannazione da uno schieramento e una benedizione dall'altro, non deriverebbero sempre dalla pochezza o dalla inadeguatezza delle risorse disponibili sul campo. Talvolta sarebbero invece conseguenti a una valutazione delle

singole situazioni da parte dei funzionari che operano “in corpore vivo” sul territorio, del tutto diversa rispetto a quella dei colleghi che operano al centro, che devono avere invece una visione distaccata dai casi particolari, per poter guidare il sistema globale.

In alcuni casi, che si potrebbero definire “buoni”, la vicinanza a situazioni che dovrebbero venire trattate con rigore e imparzialità – comminando magari sanzioni di sospensione o di revoca delle licenze – porta invece i funzionari investiti del problema a valutare con maggior attenzione gli aspetti sociali, come l’occupazione

o la continuità degli appalti; in altri casi meno “buoni”, quella vicinanza potrebbe diventare pericolosa, in particolare per i funzionari stessi (vedi riquadro).

Appare abbastanza ovvio che, se la mancanza di controlli e di sanzioni non fosse dovuta a impossibilità operative e nemmeno a valutazioni “umanitarie”, ma alla malafede di controllandi e controllori, sarebbe la credibilità dell’intero sistema a vacillare paurosamente, non soltanto quella dei ribaldi colti con le mani nel sacco. Cosa ne pensano i protagonisti? Lo racconteremo nella prossima puntata, dopo l’incontro del 16 maggio.



**securindex.com**

HOME NEWS NEWS DALLE AZIENDE LIBRARY SECURINDEX TV ARTICOLI ESSECOME

TOP NEWS ATTUALITÀ GOODS SECURITY SERVICES TECHNOLOGIES PEOPLE MON

SECURITY SERVICES



## Arrestato il prefetto di Benevento per favori agli istituti di vigilanza dei Buglione

La Guardia di Finanza ha arrestato oggi il prefetto di Benevento, Ennio Blasco, a seguito di un’inchiesta condotta dalla Procura di Avellino su presunti episodi di corruzione relativi a certificazioni antimafia di imprese di vigilanza privata dei fratelli Carmine e Carlo Buglione tra il 2009 e il 2011.

Tra le persone coinvolte dalle indagini, c’è anche Antonio Buglione che fu rapito nel 2010 da una banda di sardi e poi liberato dopo pochi giorni. Le indagini della Guardia di Finanza sono partite proprio per verificare il pagamento o meno di un riscatto in quella oscura vicenda. Antonio Buglione è al momento solo indagato nell’ambito dell’inchiesta.

E’ stato invece posto agli arresti domiciliari Erasmo Callendo, cognato di Carlo Buglione. Callendo sarebbe stato - secondo gli inquirenti - l’anello di collegamento con il prefetto Blasco che, per favorire le imprese di vigilanza privata dei fratelli Buglione avrebbe accettato gioielli, viaggi, un’auto con autista per i suoi spostamenti e perfino il pagamento di spese di lavanderia.

Il nome dei fratelli Buglione è ricorso frequentemente nelle cronache giudiziarie degli ultimi anni relative agli istituti di vigilanza, collegato alle vicende dell’International Security Service di Nola. Vicende che nel 2010 culminarono con un default dell’istituto di vigilanza che provocò la revoca del mandato ricevuto in precedenza da IntesaSanPaolo per intermediare i servizi di vigilanza per una buona parte del territorio nazionale. Un episodio che determinò la dura presa di posizione delle associazioni di categoria, in particolare di ASSIV, nei confronti delle banche, accusate di assegnare gli appalti per i servizi di vigilanza al massimo ribasso, senza preoccuparsi della qualificazione degli assegnatari di tali appalti e degli effetti devastanti che procuravano sul mercato della vigilanza privata.

# Meditry Expò, lo snodo naturale per il centro-sud

*a colloquio con Antonio Razzano, Presidente Medity  
a cura di Cristina Isabella Carminati*

**Con quali obiettivi si presenta questa seconda edizione di Medity Expò, che si propone come l'evento fieristico di riferimento per il mercato della sicurezza del centro-sud?**

L'obiettivo di Medity è ovviamente quello di migliorare sempre più, per costruire ed estendere un format che diventi un punto di riferimento per il centro-sud Italia. Intendiamo creare un volano che coinvolga aziende, istituzioni e visitatori. I frutti della scorsa edizione stanno maturando: quest'anno si sono registrate più aziende e abbiamo ricevuto più patrocini. E tutto ciò è stato possibile grazie a un'attività di coinvolgimento delle istituzioni e delle associazioni di categorie.

**Una caratteristica peculiare della manifestazione è la promozione del dialogo tra le istituzioni di riferimento e gli operatori, in particolare gli installatori dei sistemi di sicurezza e gli istituti di vigilanza. Quali sono i presupposti di questa impostazione, così importante per la sicurezza del territorio?**

Quest'anno abbiamo deciso di dedicare un momento importante al confronto con le istituzioni affrontando le problematiche legate alla sicurezza urbana.

La missione di Medity è anche quella di favorire il consolidamento del rapporto tra il "mondo sicurezza" e quello "elettrico" tramite le diverse tecnologie di riferimento, creando appuntamenti di tipo tecnico-commerciale basati sull'integrazione, in cui proporre soluzioni tecnologiche partendo dal mondo della formazione per arrivare al mercato di riferimento. Le attività di informazione e formazione per i settori di riferimento rappresentano l'idea innovativa del "fare



fiera" collaborando con le associazioni, le istituzioni e le organizzazioni.

**Quali iniziative specifiche per la professionalizzazione degli installatori verranno proposte in occasione della manifestazione di quest'anno?**

Principalmente le iniziative di professionalizzazione degli installatori seguiranno due filoni.



### PATROCINI PUBBLICI E ISTITUZIONALI

Ministero Sviluppo Economico, Regione Campania, Anci Nazionale e Campania, UNCEM, Corpo Naz. e Caserta Vigili del Fuoco, Agenzia per l'Italia Digitale, Legautonomie, Cons. Naz. dei Periti Industriali, Cons. Naz. degli Architetti Pianificatori Paesaggisti e Conservatori, Amm. Prov. Caserta, Messina, Matera, Chieti, Brindisi, Latina, Lecce, L'Aquila, Isernia, ENEA, FIRE, RENAEL, CASACERTA, APRE, ASSISTAL, ANIPA, Coord. FREE, AICTT, CONFASSOCIAZIONI, Ord. Geologi Campania, Camera Commercio Caserta, Ass. Nazionale della Polizia di Stato, InArSind, A.N.A.M.A., Confindustria Caserta, Comune Napoli, Caserta, Salerno, Palermo, Pastorano, Maddaloni, Camera di Commercio Italia Africa Centrale, Univ. di Bari "Aldo Moro", Univ. degli Studi Suor Orsola Benincasa di Napoli, Distretto Scolastico n.13 Caserta, Inail Caserta, Ordine Dot. Comm. Esperti Contabili di Napoli, Tutti gli Ordine e Collegi professionale di Caserta (Ingegneri, Architetti, Geometri, Periti, etc.) e in ordine sparso di Benevento, Bari, Avellino e Napoli, ASI Caserta.

### ALTRI PATROCINI

Anie Sicurezza, Assosicurezza, Assovalori, Aipros, Assicurezza, Confesercenti Nazionale e Caserta, A.N.I.V.P., AISS, Assintel, Federsicurezza Italia, ASSIV, I.P.F.S., CNA di Caserta e Lecce, SULPL, Scuola Internazionale Etica & Sicurezza de L'Aquila, KNX Italia, Anorc, Arbirt, Anorc Professioni, Aiesil, AnFov, Studio 147, LonMark Italy, Union, Fast, Comm. impianti elettrici ed elettronici Periti di Caserta, CNA Media, Associazione Ese, Ist. Naz. BioArchitettura, Medaarch, ANCORS, Aipsa, Ascom Caserta, Federalberghi Caserta, Mediterranean fablab. Ed ancora Lega Problemi Handicappati, Federhand-Onlus e Fish Campania, Sud Project Camp, IST: Buonarroti di Caserta, Polo Tecnico Filiera Costruzioni di Caserta, ANFUS, FUSPA, Fond. Villaggio dei Ragazzi di Maddaloni. Eventi partner Security Forum di Barcellona, Habitage 2014 e A1Expò.

### PARTNER TECNICI

CEI, C.I.P.I., Arame, Ucct, GDG Campania – Google, Akropolis, Security Group, Fashion Wellness, Ist. di Vigilanza Security Service.

### MEDIA PARTNER

Essecome, Securindex.com, Vigilanza & dintorni, Casamiasicura.it, Cuadernos de Seguridad, SecSolution, Security&safety, Security, a&s Italy, Editoriale il Delfino, Ip Security Magazine, Ip Center, Agenda Tecnica, City Life Magazine, Legislazione Tecnica, Caffè News, EthosMediaGroup, ReteArchitetti.it, ReteIngegneri.it, CercaGeometri.it, LM Leadership&Management, ICT Security, Safety&Security, l'Attacco, Quotidiano Caserta In, Caserta Web, Ondawebtv, Caserta24ore, Oggi Insieme Magazine, Eco di Caserta, L'Ermes.

Il primo si basa su tre importanti seminari che rilasceranno crediti formativi: quello di giovedì 15 maggio è organizzato dagli ordini e collegi professionali di Caserta, quello di venerdì 16 maggio da CEI e CIPI, mentre quello di sabato 16 maggio dal Corpo dei Vigili del Fuoco in collaborazione con l'UCCT.

Per quanto riguarda la seconda sfera di attività, all'interno della fiera quattro sale saranno messe a disposizione delle aziende, che potranno organizzare corsi tecnici per clienti e installatori. In questo modo si dà la possibilità agli installatori di approfittare della fiera

non soltanto per vedere e conoscere novità di prodotto ma anche per partecipare a tre giorni di formazione continua.

Crediamo, quindi, con questo meccanismo di continuare a sviluppare l'obiettivo di Medity: formazione e informazione.

### Quali iniziative riguarderanno la vigilanza privata?

Questa edizione gode del patrocinio di molte importanti associazioni di categoria della Vigilanza. Medity intende dare un'opportunità a tutti gli operatori del



settore, alle FFOO, alle società di vigilanza privata, di trasporto valori e ai rappresentanti delle guardie giurate di potersi confrontare per valutare gli effetti della riforma e della normativa di riferimento della vigilanza soprattutto su contesti socio-economici particolari, come la regione Campania: un tema messo al centro dell'attenzione con un seminario che coinvolge gli operatori e le aziende in merito all'applicazione del DM269. È un tema importantissimo, perché il ruolo degli istituti di vigilanza che viene delineato dal nuovo DM 269 li vedrebbe consolidare anche come systems integrator tra tecnologie e servizi, quindi con una forte potenzialità di traino per i fornitori di tecnologie.

**Come valuta il mercato della sicurezza nel centro-sud? Quali sono le principali opportunità e quali le criticità?**

Penso che il centro-sud Italia rappresenti una grossa opportunità per il mercato della sicurezza, tanto è an-

cora da fare, soprattutto nella diffusione della cultura del fare sicurezza. Medity vuole essere un'opportunità per le aziende per presenziare da vicino il mercato di riferimento e per gli operatori per migliorare sempre più conoscenze e professionalità.

Mi rendo conto della criticità del periodo e del momento storico che stiamo attraversando, ma credo che se uniamo gli sforzi tutti assieme possiamo creare l'opportunità giusta, e il centro-sud è un'opportunità!

**È confermata anche quest'anno la sessione autunnale di Medity Expò in Sicilia? Come verrà impostata?**

Certo, è confermata, sarà presentata a maggio! L'obiettivo dell'Associazione Medity è partire da Medity Expò 2014 per arrivare a Medity Expò 2015, di creare quindi un evento itinerante che anche quest'anno toccherà Caserta e Palermo.

# MEDITY

Con il Patrocinio di



Caserta

## EXPÒ 2014 dell'INTEGRAZIONE oltre la SICUREZZA

Security - Electricity - Safety - Automation - Energy - Electronics

### 15 -16 -17 MAGGIO 2014

dalle ore **9:30** alle ore **19:00**

Polo Fieristico **A1 EXPÒ** Pastorano (CE) Uscita A1 Capua



Registrati Subito su  
[www.meditry.it](http://www.meditry.it)

**MEXPO**  
POLO FIERISTICO  
Pastorano (CE) Uscita A1 Capua

**RA**  
di Razzano Antonio

SICUREZZA  
DOMOTICA  
AUTOMAZIONE

Tel. +39 0823 405405 - e.mail: info@medity.it

Seguici su

# Security Essen, la regina delle fiere della sicurezza

a cura della Redazione



Dal 23 al 26 settembre 2014 la Fiera mondiale per la security e la protezione antincendio presenterà le ultime tendenze internazionali. Security Essen festeggerà il suo 40° anniversario e sarà ancora una volta la fiera leader mondiale della sicurezza. Le sfide globali e le ultime tendenze nel settore della security saranno protagoniste nel mese di settembre. I temi principali saranno la sicurezza IT, le soluzioni smartphone intelligenti, la sicurezza dei viaggi e i veicoli speciali. Con una superficie espositiva più grande e un gran numero di espositori già iscritti, Security Essen continua il suo percorso di crescita. Dal 23 al 26 Settembre sono attesi oltre 1.000 espositori provenienti da circa 40 nazioni. Per la prima volta rappresenteranno più di 40 segmenti di mercato: dalla tecnologia della sicurezza meccanica alla protezione antincendio, la sicurezza per le aree esterne e le telecamere a circuito chiuso, fino alla prevenzione del terrorismo, grazie anche a dimostrazioni dal vivo, workshop e forum di esperti. Security Essen sarà il palcoscenico internazionale per

i nuovi prodotti: sarà infatti presentato il “Premio per l’innovazione nella security”. I migliori nuovi prodotti e servizi saranno premiati con l’”Oscar della security”. Claus-Peter Regiani, direttore della fiera, si aspetta un anniversario indimenticabile: «Ci occuperemo di temi di scottante attualità come la sicurezza informatica». In questa edizione, infatti, si affronteranno le sfide della sicurezza IT con un forum specialistico. «Eventi quali l’Area di ricerca sulla sicurezza e la Giornata per la formazione e l’approfondimento apriranno prospettive interessanti per l’intero compartimento della security. Ai settori in forte crescita sarà dedicato molto più spazio», ha sottolineato Regiani. Security Essen, il mercato più importante per la security e la protezione antincendio, ha ospitato nel corso dell’ultima edizione 39.000 visitatori professionali da 115 paesi. Oltre l’80 per cento erano acquirenti e decision maker, provenienti in prevalenza da industria, artigianato, commercio, sorveglianza ed enti governativi. Per il 40° anniversario ci si attende grande interesse anche da parte delle banche e delle compagnie assicurative.

23-26 SETTEMBRE 2014

# Fiera internazionale della sicurezza e della protezione antincendio



## DA 40 ANNI IL NUMERO UNO

Eccellenti affari vi aspettano al mercato internazionale della sicurezza. 115 nazioni sul posto. Tutti i settori, i trend più attuali, le innovazioni più importanti. L'82% dei 36.000 visitatori sono decision maker pronti ad investire. Non fatevi trovare impreparati!



[www.security-essen.de](http://www.security-essen.de)



# Sicurezza 2014 in crescita

**SICUREZZA**  
Fiera Milano, Rho 12-14 NOVEMBRE 2014

a cura della Redazione

**S**ICUREZZA 2014 cresce. A otto mesi dalla prossima edizione, che si terrà dal 12 al 14 novembre 2014 a Fiera Milano, è già stato occupato il 60% della superficie prevista e le aziende nazionali e internazionali che hanno confermato la partecipazione a oggi superano di oltre il 25% il numero di quelle che, nello stesso periodo pre-mostra, avevano aderito nel 2012.

Grazie ad aziende da sempre fedeli al progetto della manifestazione, imprese che tornano a SICUREZZA dopo alcune edizioni e brand che si presentano per la prima volta, la varietà dell'offerta merceologica si preannuncia particolarmente interessante e in grado di rappresentare l'innovazione prodotta dai maggiori comparti del settore. Così, oltre alla videosorveglianza, saranno protagoniste sempre più presenti a SICUREZZA anche le soluzioni antintrusione, il controllo accessi, la prevenzione incendi, l'ICT security, i dispositivi per la sicurezza fisica e per quella passiva. L'offerta della manifestazione sarà dunque in linea con le esigenze di un mercato tenace, la cui cultura è fortemente radicata nel nostro paese, che guarda oggi alle prospettive di sempre maggiore integrazione tecnologica, alle opportunità di aggiornamento professionale e a nuovi mercati internazionali a cui puntare.

Con una crescita dello 0,92% nel 2013 rispetto al 2012 (dati ANIE Sicurezza) il settore dimostra una stabilità positiva per porre le basi di una ripresa: «Pur in un contesto macroeconomico molto critico, il comparto ha mostrato una capacità di tenuta superiore alla media del manifatturiero, in particolare nel segmento della videosorveglianza, che ha mantenuto segno positivo. La crescente percezione di insicurezza legata alla diffusione di reati contro il patrimonio ha favorito la richiesta da parte dei privati di apparecchiature

e dispositivi tecnologicamente sempre più evoluti. Le prospettive di sviluppo della nostra industria sono legate all'innovazione tecnologica, in Italia e all'estero, e a una sempre maggiore integrazione con gli strumenti ICT, nell'ottica di una evoluzione smart di tutte le tecnologie», dichiara Rosario Romano, presidente ANIE Sicurezza.

«SICUREZZA 2014 sarà da un lato il riflesso dell'attuale situazione del mercato nel settore», afferma Giuseppe Garri, Exhibition Manager di SICUREZZA, «ma punta anche a riaffermare la sua leadership come occasione unica e strumento in più per offrire nuove vie di sviluppo a tutte le aziende e agli operatori. Abbiamo investito molto sull'incoming dall'estero e stiamo lavorando affinché i giorni di manifestazione possano rappresentare una autentica occasione di internazionalizzazione per le aziende espositrici, grazie all'attenta profilazione dei buyer che porterà a incontri mirati. Inoltre, grazie a tutti i maggiori editori del settore, stiamo approntando un panel di eventi e iniziative destinate a dare vivaci spunti di crescita del know how di tutti i profili professionali del settore».



# SICUREZZA

Biennale Internazionale di Security & Fire Prevention

Fiera Milano (Rho) 12.14 NOVEMBRE 2014

Follow us on



[www.sicurezza.it](http://www.sicurezza.it)

THE INTERNATIONAL NETWORK



Official Partner

# Golfo e Medio Oriente a Dubai per Oil & Gas Security Summit

a cura della Redazione

L'International Research Networks Ltd. ha riunito il 4 e 5 marzo scorso presso il Sofitel Jumeirah Beach Hotel di Dubai un gruppo eccezionale di esperti provenienti da tutto il Medio Oriente, che hanno presentato ai partecipanti una visione olistica della sicurezza nel settore oil&gas. Tra i prestigiosi relatori si sono visti gli esperti di sicurezza di Chevron Shipping, Maersk Oil, GDF Suez, GE Oil and Gas, Transocean, Lukoil, Danagas, Qatar Petroleum, ConocoPhillips, Kuwait Oil Company, Abu Dhabi National Energy Company, Baker Hughes e OSAC. L'eccezionale competenza degli speaker ha fornito ai partecipanti approfondimenti dettagliati legati all'esperienza diretta nella pianificazione e messa in opera di sistemi di sicurezza nel panorama ricco di minacce che caratterizza il Medio Oriente.

Un tema ricorrente nel corso delle due giornate sono state le sfide concernenti la valutazione e la riduzione del rischio, parallelamente alle difficoltà incontrate dai security manager nel convincere i decision maker della necessità di investire adeguatamente nel settore, anche se non si sono verificati incidenti recenti. Di solito, infatti, le politiche aziendali sono fatte guardando al passato, ma i delegati hanno convenuto che in materia di sicurezza si tratta di un approccio perdente e potenzialmente pericoloso. È stata inoltre discussa la debolezza degli attuali



livelli di pianificazione nella continuità operativa all'interno delle aziende petrolifere in Medio Oriente. I delegati hanno beneficiato di analisi hands-on sull'evacuazione dall'Iraq, di una panoramica della pianificazione della sicurezza per un importante IOC in Algeria prima, durante e dopo la tragedia d'Amenas, e di una presentazione che ha esplorato la sicurezza implicita nel corso del conflitto siriano, per citare soltanto alcune delle sessioni più interessanti. Il primo giorno del vertice è stato organizzato anche un workshop interattivo sulla preparazione di un piano di risposta a eventuali minacce terroristiche.

**L'IRN ospiterà due ulteriori forum regionali mirate su Oil & Gas Security nei prossimi mesi.**





# SICHERHEITSEXPO

2.-3. JULY 2014 MÜNCHEN



The Trade Fair for

-  Access Control
-  Video Surveillance
-  IT Security
-  Fire Protection

2. – 3. JULY 2014  
MOC MÜNCHEN



NETCOMM GmbH, Tel. +49 89 88949370  
info@sicherheitsexpo.de



WWW.SICHERHEITSEXPO.DE

# intersec

January 18 – 20, 2015

Dubai, UAE

**Don't miss out!**  
The 5% Early Bird Discount is  
available until April 15, 2014!

## Book your stand!

More than 1,200 exhibitors and 24,766 visitors from 126 countries, qualified Intersec as the world's largest and most international exhibition for Safety & Security.

[www.intersecexpo.com](http://www.intersecexpo.com)



messe frankfurt

# L'inconsapevolezza di oggi, la crisi di domani

a cura della Redazione

**I**l 20 aprile 2010, durante le fasi finali della realizzazione di un pozzo petrolifero nelle acque profonde del Golfo del Messico, si è verificata un'esplosione che ha provocato un incendio e innescato un'immensa fuoriuscita di idrocarburi dal fondo del mare, che ha portato a gravissime conseguenze ambientali nel Golfo del Messico, particolarmente per le coste della Louisiana. La fuoriuscita di petrolio dalla piattaforma Deepwater Horizon ha provocato effetti impensabili sull'intero settore: la morte di 11 persone, la perdita di milioni di barili di petrolio e un grandissimo impatto ambientale. Le conseguenze dei disastri industriali possono avere un impatto sull'intero settore e non causano soltanto imponenti perdite finanziarie, ma influiscono anche sulla reputazione del brand e, ultimo ma non per questo meno importante, portano alla perdita di vite umane. Alla luce dell'evoluzione delle attuali minacce, essere preparati a incidenti e inconvenienti è indispensabile. Dal 10 al 12 giugno 2014 si terrà a Dubai, negli Emirati Arabi Uniti, "The Emergency Management and Crisis Response Summit", durante il quale l'episodio del Deepwater Horizon sarà uno dei più importanti casi di studio. «Imparare dal passato è uno dei modi migliori per essere preparati al futuro; i case study possono aiutare i professionisti del settore a comprendere e a pianificare le azioni contro tali calamità», afferma Danish Shaikh, Executive Vice President di MICE Quotient, organizzatrice dell'evento.

«La piattaforma petrolifera Deepwater Horizon era nota per la perforazione del più profondo pozzo petrolifero

della storia. In seguito divenne ancora più famosa per un titolo assai meno ambito, la più grande fuoriuscita di petrolio nella storia degli Stati Uniti. Durante il case study i partecipanti potranno fare un esame interattivo a 360 gradi dell'evento, avranno modo di esaminare quanto è stato attivato per la pianificazione, l'attenuazione e il recupero dell'enorme fuoriuscita. Potranno tornare alla propria attività avendo imparato i passi concreti e fattibili per aumentare la sicurezza e accrescere la resilienza delle infrastrutture, dell'ambiente, del personale e del brand. La sessione sarà incentrata sul ruolo insostituibile della partnership pubblico-privato e della comunicazione in caso di crisi, per incidenti importanti come la fuoriuscita dalla piattaforma Deepwater Horizon ma anche per i piccoli eventi di tutti i giorni», afferma Robert Katz, Managing Director e fondatore dell'Holistic Security Institute & Disaster & Terrorism Adviser presso la Federal Emergency Management Agency, U.S. Department of Homeland Security.

The Emergency Management and Crisis Response Summit è orgoglioso di presentare una piattaforma per i leader del settore, gli esperti, gli enti governativi e altri soggetti interessati a collaborare, imparare, condividere e sviluppare una gestione delle emergenze e delle risposte alle situazioni critiche più forte e agile. Il summit, organizzato per i professionisti del settore provenienti dall'aviazione, delle infrastrutture, dall'oil&gas e per i risk managers, fornirà opinioni e idee specifiche per il settore sulla gestione delle emergenze e le risposte alle criticità.





# Abbonati!

6 numeri a soli 60 €

Abbonandoti a



**entrerai nel mondo della sicurezza fisica professionale**

---

Un mondo di informazione, cultura e opportunità di business,  
dove troverai

**articoli, interviste e redazionali di approfondimento  
su attualità, tecnologie, fiere**

e le esclusive sezioni dedicate ai principali mercati verticali  
**Banche, Retail, Infrastrutture critiche, Residenziale,  
Vigilanza, Trasporto e Trattamento valori**

---



**securindex**  
TV



**securindex.com**



**PREVENZIONE RAPINE**



**4POWER SRL**  
(+39) 081 8193441  
www.4power.it

## Nuovi Switch PoE Gigabit managed layer 2 e 3

4Power presenta i nuovi switch PoE managed WGSW-48040HP rame/fibra ottica di Planet Technology: flessibilità, funzioni all'avanguardia, risparmio energetico e ottimo rapporto qualità prezzo. IPV4 e IPV6 Layer 2 con routing statico Layer 3, 48 porte LAN gigabit e 4 porte SPF, configurabili con moduli Mini-GBIC, per la migliore configurazione (p.es. fibra ottica monomodale per collegamenti sino a 150 km). Alimentatore PoE ad alta potenza IEE 802.at, per periferiche sino a 30W, 600 W di potenza totale. Integra caratteristiche avanzate per la gestione remota dispositivi e risparmio energetico. Programmazione accensione e spegnimento periferiche: es. spegnere telefoni e i Wi-fi di servizio nelle ore notturne e attivare videocamere FLIR perimetrali; gestione potenza fornita alle porte; PD Alive (riavvio di singoli dispositivi in caso di problemi); reboot di dispositivi programmabile (riduce le possibilità di crash per buffer overflow). Interfaccia WEB e SNMP per la gestione remota con SSH, SSL e SNMPv3, Allarmi SMTP/SNMP via mail. Switch ideale per applicazioni Voip e sorveglianza.



**AVS ELECTRONICS SPA**  
(+39) 049 9698411  
www.avselectronics.com

## Outspider DT smart edition di AVS ELECTRONICS

Outspider DT smart edition di AVS Electronics è il nuovo sensore da esterno digitale innovativo, in grado di generare il funzionamento di due microonde distinte, dotato di un'efficace funzione antimascheramento e di una particolare tecnologia di funzionamento che aumenta l'adattabilità all'ambiente esterno e potenzia la capacità di discriminare i falsi allarmi.

Facile da installare, Outspider DT smart edition permette una massimizzazione immediata della distanza di rivelazione, in tutte le posizioni. Infatti, durante l'installazione, è possibile eseguire, con il solo utilizzo dei più comuni attrezzi di lavoro e senza alcun collegamento al Pc, una procedura di calibrazione semplificata pratica e sempre perfetta. Inoltre, grazie all'attivazione di una segnalazione ottico acustica, è facile ottimizzare la posizione della scheda elettronica in funzione del contesto da proteggere, così da consentire un risultato affidabile, con una riduzione del tempo di lavoro.



**EKEY BIOMETRIC SYSTEMS SRL**  
(+39) 0471 922712  
www.ekey.net

## Biometria e bluetooth in un unico lettore

Novità a livello mondiale il pacchetto combinato della ekey: lettore biometrico e bluetooth come apriporta e administration in un unico congegno, naturalmente con App gratuita. Con il nuovo lettore biometrico IN 2.0 bluetooth il n° 1 in Europa nelle soluzioni d'accesso a impronta digitale presenta un set 2 in 1 che unisce i vantaggi di un lettore classico con la funzionalità bluetooth.

La nuova App (per Android e iPhone) offre due possibilità:

Apertura con il cellulare: Premendo un tasto nella App si aprono porte e cancelli o si disattiva l'impianto di allarme. Ovviamente lo scambio di dati Bluetooth ha luogo in modo cifrato.

Gestione: l'utente amministra dispositivo e persone autorizzate in modo molto semplice direttamente dallo Smartphone. Il codice di accesso del cellulare e/o dell'App impedisce l'accesso alle persone non autorizzate.

Non è mai stato così semplice inserire, amministrare o cancellare gli utenti: registrazione delle impronte digitali, autorizzazioni all'accesso, aggiornamenti del sistema, etc.



**GUNNEBO ITALIA S.P.A.**  
(+39) 02 267101  
www.gunnebo.it

## Una nuova App per gli SpeedStile Gunnebo

Pratica, elegante e innovativa, Speedstile App consente ai possessori di iPad di visionare in anteprima l'effetto dell'inserimento dei varchi Gunnebo all'interno di un progetto. Basta scattare con il tablet una foto dell'ambiente in cui si desiderano inserire le barriere e disegnare tramite touchscreen la linea di base lungo la quale intendiamo collocare i varchi, indicandone la lunghezza. Selezionando poi il modello prescelto dal catalogo, l'App provvede a collocare l'immagine perfettamente riproporzionata nella posizione richiesta. È possibile inserire più varchi, spostarli e sostituirli, salvando l'immagine solo quando saremo soddisfatti del risultato. L'App, gratuita e reperibile nell'Apple Store digitando "Gunnebo", consente di scegliere la soluzione più adatta fra le quattro linee di SpeedStile, declinate in più tipologie e disponibili con un'inedita varietà di finiture.



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

## HESA presenta i nuovi rivelatori HE-100X e HE-110X

La gamma di rivelatori HE-100 e HE-110, studiata per la protezione di porte e finestre con una doppia tenda dall'alto e caratterizzata da alta precisione di rilevazione e immunità ai falsi allarmi, si rinnova sia dal punto di vista tecnologico che estetico. Nelle nuove versioni HE-100X e HE-110X la parte elettronica è stata aggiornata per diminuire l'assorbimento, mentre l'introduzione della guarnizione ha portato il grado di protezione a IP55. Le nuove versioni a basso assorbimento consentono inoltre di effettuare la sostituzione della batteria in modo estremamente semplice e veloce. Oltre alla versione a basso assorbimento HE-110X, sono disponibili varie versioni pre-assemblate con i trasmettitori compatibili con una vastissima gamma di centrali. Caratteristiche: conteggio impulsi selezionabile 1 o 2, funzionamento LED d'allarme selezionabile On/Off, funzionamento selezionabile in AND o OR, protezione antiapertura, lente di Fresnel, compensazione automatica della temperatura, disponibilità nei colori bianco e marrone.



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

## I sensori Ital15 di Saet

La linea di rilevatori Saet comprende un'ampia gamma di tecnologie e di versioni, adatta a coprire praticamente tutte le esigenze di protezione per interni con qualsiasi unità centrale impiegata. Propone un sensore a microonde, un supercollaudato sensore a infrarossi passivo e una doppia tecnologia che racchiude le qualità di entrambi i sensori sopra citati. Dal punto di vista visivo, la Saet è riuscita a sviluppare un progetto che è in grado di mantenere lo stesso aspetto estetico per tutte e tre le tipologie di sensore, sia per il collegamento con centrali che gestiscono ingressi del tipo ON/OFF, sia centrali che gestiscono linee seriali Saet. Caratteristiche: tecnologia di rilevazione DRO a microstrip per le MW e DT; immunità alle lampade fluorescenti per tutta la gamma; comando di blocco programmabile; sensibilità, portata e conteggio impulsi programmabili; antiaccecamento; portata 4-16 m + 90°; frequenza di lavoro MW 9,9 Ghz; lente di Fresnel 28 zone 3 piani; antistrisciamento a 3 settori.



**SAMSUNG TECHWIN EUROPE LTD**  
(+39) 02 89656410  
www.samsungsecurity.it

## Nuovo NVR Samsung SRN-4000

SRN-4000 offre una banda di registrazione pari a 400Mbps permettendo di registrare fino a 64 telecamere 2MP a risoluzione FullHD (1920x1080) a 25fps ognuna. Oltre alle telecamere IP Samsung supportate vengono anche gestite le telecamere di altri produttori tramite ONVIF Profile S.

Supporta inoltre la configurazione RAID 5 e RAID 6 con un massimo di 12 Hdd (Hot Swap) installabili e doppio alimentatore, consentendo la registrazione ininterrotta anche in caso di guasto.

L'interfaccia grafica permette la configurazione delle telecamere senza l'ausilio di PC esterni in modo semplice e veloce tramite "Wizard", e consente inoltre la visualizzazione delle telecamere "live", delle registrazioni, e la ricerca per tipo di allarme e analisi video avanzata.

Quest'ultima funzionalità di Analisi Video Avanzata offre le possibilità di analizzare statisticamente tramite "Heat Mapping" le aree con più attività di movimento.



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

## Satel presenta INT-TSI touch 7"

Grazie alla sua tecnologia spinta e ad un'attraente interfaccia grafica, INT-TSI è in grado di soddisfare gli utenti e gli installatori più esigenti. Le innumerevoli possibilità di configurazione offerte dai sistemi INTEGRA richiedono una gestione all'altezza delle potenzialità della centrale. INT-TSI introduce quindi una nuova qualità di utilizzo dei sistemi di allarme. La INT-TSI racchiude una tecnologia avanzata, un efficiente processore garantisce un funzionamento fluido dell'estesa interfaccia grafica, i componenti di alta qualità utilizzati consentono le azioni con una scorrevolezza unica, sfiorando semplicemente lo schermo in vetro. Il potente software TSI-BUILDER offre la possibilità di configurare un sistema che associa sicurezza e home automation con standard di massima professionalità. Le soluzioni futuristiche applicate nell'INT-TSI offrono all'installatore progettazioni illimitate dell'interfaccia utente.



**SECURITATEM LTD**  
(+39) 0362 185440  
www.setik.biz

## La nuova serie AI di Setik.biz

Setik.biz presenta in anteprima la nuova serie AI che introduce funzionalità "Hybrid" sui DVR Setik, permettendo così di integrare sullo stesso impianto sia telecamere di generazione analogica (WD1/960H) che IP (2MPX/1080p) contemporaneamente. Sono previsti 5 modelli tutti Full Frame (25fps) su tutti i canali sia IP che Analogici, che supportano nativamente lo standard ONVIF, in modo da garantire un'ampia compatibilità di prodotto in ambito IP.

È garantito il supporto fino a 2 dischi da 4TB, portando la capacità totale ad 8TB per sistema; è stata inoltre prevista la nuova funzionalità CLOUD, che permette di raggiungere le telecamere anche in condizioni di connettività, in cui non è possibile una raggiungibilità diretta dell'apparato. La nuova Generazione AI è stata infine resa compatibile con i browser più diffusi e con tutte le piattaforme mobili sul mercato. I nuovi modelli sono: ST6204H-AI, ST6208F-AI, ST6216F-AI, ST6208H-AI, ST6216H-AI. Saranno disponibili sul mercato dalla metà di aprile su [www.setik.biz](http://www.setik.biz)



**SYAC-TB**  
(+39) 059 289891  
www.syac-tb.com

## Apps DigiEye per IOS/Android e Win/Mac

Le app DigiEye, iDigiEye e iDigiEye HD permettono di visualizzare l'elenco di tutti i siti disponibili, selezionare un sito dall'elenco per connettersi e visualizzare la lista di tutte le telecamere del sito selezionato. Per ogni camera sono disponibili le seguenti informazioni: tipo, stato attuale e nome della telecamera, stato di registrazione del DVR/NVR. Altre feature:

- LIVE VIEW: split x1/x4/x16, full screen, zoom digitale, stato e attivazione delle uscite digitali, visualizzazione degli stati degli allarmi, cambiamento di qualità e risoluzione immagine, snapshot, controllo PTZ;
- REMOTE PLAYBACK: visualizzazione di data/ora inizio/fine registrazione e barra di riproduzione della telecamera selezionata, funzionalità di riproduzione remota e possibilità di specificare la data della sequenza di interesse;
- CONFIGURAZIONE: consentono di aggiungere/rimuovere/modificare i parametri dei siti nell'elenco dei siti, impostare/modificare i parametri dell'account utente/amministratore dell'app e impostare/modificare i parametri generali.



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

## Piattaforma CST, una nuova era

Coded Sensor Technology (CST) è la prima piattaforma al mondo per la realizzazione di sensori magnetici su misura con tecnologia Magnasphere®.

Sulla base di un cuore tecnologico comune, TSEC può personalizzare le funzionalità dei sensori in modo da soddisfare le più stringenti esigenze di alta sicurezza, a partire dalla possibilità di realizzare tamper anti-rimozione su parte sensore e parte magnete, alla integrabilità di contatto magnetico e sensore inerziale in un unico dispositivo: le possibilità sono semplicemente infinite. Il contatto riconosce il proprio magnete: la Coded Sensor Technology, esclusivo brevetto TSEC, permette di realizzare coppie di sensori e magneti codificate. Tentativi di utilizzare un magnete diverso da quello codificato causano l'apertura di un circuito di tamper 24h indipendente dal contatto primario.

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



**WD**  
(+39) 340 7845464  
www.wd.com

## Da WD un hard disk su misura per il mercato della videosorveglianza

WD Purple™ è la nuova linea di hard disk da 3,5 pollici specificamente progettati per applicazioni di sorveglianza. Pensati ad hoc per le unità di videosorveglianza, gli hard disk WD Purple danno il meglio di sé negli ambienti di sicurezza domestici e delle piccole realtà aziendali, nuovi ed esistenti, con un massimo di otto hard drive e di 32 videocamere ad alta risoluzione (HD). Attualmente in distribuzione, gli hard disk WD Purple sono disponibili con capacità da 1TB fino a 4TB.

Ottimizzata per le applicazioni di sorveglianza e con una riproduzione video in alta risoluzione migliorata per operare in ambienti di videosorveglianza con carico di lavoro 24x7, la linea di hard disk WD Purple è pensata per rispondere alle necessità di ambienti di registrazione digitale PVR, DVR e NVR sempre operativi. Gli hard disk WD Purple vantano inoltre un consumo energetico ridotto e numerose funzionalità avanzate riservate tipicamente allo storage di livello enterprise.



**essecome**  
security&safety

**securindex.com**

**securindex**  
TV

**CASAMIASICURA.it**  
Dove trovi la sicurezza che cerchi

Informazione  
cultura  
business  
della sicurezza  
dal 1981

Per informazioni:  
[marketing@securindex.com](mailto:marketing@securindex.com)

**essecome**  
security&safety

n. 02 marzo-aprile 2014

ISSN: 2282-5770

Anno XXXIV - II  
Periodico fondato da Paolo Tura

**DIRETTORE RESPONSABILE**

Cristina Isabella Carminati

**COORDINAMENTO EDITORIALE**

Raffaello Juvara  
[editor@securindex.com](mailto:editor@securindex.com)

**REDAZIONE**

Cristina Isabella Carminati - Raffaello Juvara

**HANNO COLLABORATO A QUESTO NUMERO**

Maurizio Barbo, Alessandro Del Rosso, Bruno Fazzini, Barbara Ferraris di Celle,  
Luca Salgarelli

**SEGRETERIA DI REDAZIONE**

[redazione@securindex.com](mailto:redazione@securindex.com)

**GRAFICA/IMPAGINAZIONE**

servizio interno dell'editore

**PUBBLICITÀ E ABBONAMENTI**

[marketing@securindex.com](mailto:marketing@securindex.com)

**EDITORE**

Secman srl  
Verona - Via Bozzini 3  
Milano - Via Stefanardo da Vimercate 28  
Tel. +39 02 36757931

**ISCRIZIONE AL ROC**

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

**REGISTRAZIONE**

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

**STAMPA**

Seven Seas srl  
Via Tonso di Gualtiero 12/14  
47896 Faetano - Repubblica di San Marino  
Tel. 0549 996194 - Fax 0549 900104  
[sevenseasrsm@gmail.com](mailto:sevenseasrsm@gmail.com)

4POWER	<a href="http://www.4power.it">www.4power.it</a>	42-44, 47, 91
ALLEGION	<a href="http://www.allegion.com">www.allegion.com</a>	38-40
ANIVP	<a href="http://www.anivp.it">www.anivp.it</a>	74-75
ASSA ABLOY	<a href="http://www.assaabloy.it">www.assaabloy.it</a>	65
ATIK	<a href="http://www.atik.it">www.atik.it</a>	30-33
AVS	<a href="http://www.avselectronics.com">www.avselectronics.com</a>	17, 21, 91
CHECK POINT SYSTEMS	<a href="http://www.checkpointsystems.com">www.checkpointsystems.com</a>	68-69
CITEL	<a href="http://www.citel.it">www.citel.it</a>	34-37
DEA SECURITY	<a href="http://www.deasecurity.com/it">www.deasecurity.com/it</a>	19-20
ELAN	<a href="http://www.elan.an.it">www.elan.an.it</a>	Il copertina
EKEY BIOMETRIC SYSTEMS	<a href="http://www.ekey.net">www.ekey.net</a>	91
EMCRS	<a href="http://www.micequotient.com">www.micequotient.com</a>	13, 89
ERGONOMIC SOLUTIONS	<a href="http://www.ergonomic-solutions.net">www.ergonomic-solutions.net</a>	70-72
EURALARM	<a href="http://www.euralarm.org">www.euralarm.org</a>	10-12,14
GUNNEBO	<a href="http://www.gunnebo.it">www.gunnebo.it</a>	67, 92
HESA	<a href="http://www.hesa.it">www.hesa.it</a>	24-25, 92
HI-CARE	<a href="http://www.hi-care.eu">www.hi-care.eu</a>	15-16,18
HONEYWELL	<a href="http://www.security.honeywell.com/it">www.security.honeywell.com/it</a>	I romana
INTERSEC 2014	<a href="http://www.intersecexpo.com">www.intersecexpo.com</a>	88
MEDITY EXPO 2014	<a href="http://www.medity.it">www.medity.it</a>	78-81
MILESTONE SYSTEMS	<a href="http://www.milestonesys.com">www.milestonesys.com</a>	50-52, 64-66
MONDIALPOL	<a href="http://www.mondialpol.it">www.mondialpol.it</a>	60-62
OIL & GAS SECURITY 2014	<a href="http://www.oilgassecurity.com">www.oilgassecurity.com</a>	86
ONVIF	<a href="http://www.onvif.org">www.onvif.org</a>	8-9
SAET	<a href="http://www.saetitalia.it">www.saetitalia.it</a>	92, IV copertina
SAMSUNG	<a href="http://www.samsungsecurity.com">www.samsungsecurity.com</a>	22-23, 41, 93
SATEL	<a href="http://www.satel-italia.it">www.satel-italia.it</a>	I copertina, 55-57, 93
SECURITATEM	<a href="http://www.setik.biz">www.setik.biz</a>	93
SECURITY ESSEN	<a href="http://www.security-essen.de">www.security-essen.de</a>	82-83
SICHERHEITS EXPO	<a href="http://www.sicherheitsexpo.de">www.sicherheitsexpo.de</a>	87
SICUREZZA 2014	<a href="http://www.sicurezza.it">www.sicurezza.it</a>	84-85
SIEMENS	<a href="http://www.siemens.it/securityproducts">www.siemens.it/securityproducts</a>	53-54
TECHBOARD	<a href="http://www.syac-tb.com">www.syac-tb.com</a>	94
T-SEC	<a href="http://www.tsec.it">www.tsec.it</a>	26-29, 58-59, 94, III copertina
VIDEOTREND	<a href="http://www.videotrend.net">www.videotrend.net</a>	2-3, 48-49
WD	<a href="http://www.wdc.com/it">www.wdc.com/it</a>	45-47, 94

# CLH-111

## GRADO 3

- + SICUREZZA
  - + DESIGN
  - + ROBUSTEZZA
  - + QUALITÀ
  - COSTO
  - INGOMBRO
- 
- = CLH-111



Contatti magnetici antimascheramento  
CLH-111 certificati Grado 3:  
il calcolo della sicurezza.



# SICUREZZA TOTALE A 360°



**SISTEMA MIRUS MULTIFUNZIONE**  
CENTRALIZZAZIONE ED INTEGRAZIONE IMPIANTI  
CONTROLLO ACCESSI - CONTROLLO TECNOLOGICO - MODULARITA'

## L'ELENCO DEI CONCESSIONARI SAET IN ITALIA

- |                                  |                   |                                  |                 |
|----------------------------------|-------------------|----------------------------------|-----------------|
| • BERGAMO: S.C. SECURITY CENTER  | TEL. 035.244728   | • MILANO: CRS                    | TEL. 02.9762052 |
| • BOLOGNA: SAET BOLOGNA          | TEL. 051.520701   | • MODENA: MODENA ANTIFURTO       | TEL. 059.222999 |
| • BOLZANO: THEOREMA              | TEL. 0471.811343  | • NAPOLI: SECURITY NAPOLI        | TEL.081.5920014 |
| • BRESCIA: LAIS                  | TEL. 030.3540419  | • PADOVA: SITEL SISTEMI          | TEL.049.8074945 |
| • CAGLIARI: ITALTEC              | TEL. 070.912395   | • PALERMO: SAET SICILIA          | TEL.091.6884191 |
| • CREMONA: DISAITALIA SISTEMI    | TEL. 0372.838720  | • PERUGIA: S.D.S.                | TEL.075.8989292 |
| • CROTONE: DIELETTRA             | TEL. 0962.902370  | • PESCARA: LOGIKEY               | TEL.085.4225213 |
| • CUNEO: COBER                   | TEL. 0172.693867  | • POTENZA: GENOVESE ROCCHINA     | TEL.0971.35659  |
| • FROSINONE: P.B.SYSTEM          | TEL. 0775.270323  | • REGGIO EMILIA : CENTRO ALLARMI | TEL.0522.322304 |
| • GENOVA: ELETTRODINAMICA        | TEL. 010.84660011 | • RIETI: SECUTRON                | TEL.0746.689053 |
| • GENOVA: SICURCONTROL           | TEL. 010.8380110  | • RIMINI: 3 G ELETTRONICA        | TEL.0541.778605 |
| • LECCE: A.T.S. ELETTRONICA      | TEL. 0832.332884  | • ROMA: SAET                     | TEL.06.24402002 |
| • LIVORNO: FLASHNET              | TEL. 0586.426899  | • ROMA: ANTARES                  | TEL.06.39375658 |
| • MANTOVA: ALGOR ELETTRONICA     | TEL. 0376.48246   | • SALERNO: SALERNO KONTROL       | TEL.089.772070  |
| • MESSINA: MEGA SISTEM           | TEL. 090.7381062  | • TORINO: AXIOMA                 | TEL.011.3096941 |
| • MESSINA: INGEGNERIA AMBIENTALE | TEL. 090.9392041  | • TORINO: G.P.M.                 | TEL.011.3358127 |
| • MILANO: SAET MILANO            | TEL. 02.2440294   | • TREVISO: SECURITY CENTER       | TEL.0422.305511 |
| • MILANO: TECNOESSE              | TEL. 02.3491321   | • VICENZA: ELPRO I.C.A.          | TEL.044.501294  |

**SAET ITALIA S.p.A.** SISTEMI DI SICUREZZA E CONTROLLO

Sede legale: Via F. Paciotti, 30 · 00176 Roma - Sede operativa: Viale Filarete, 122/128 · 00176 Roma  
Tel. 06.24.40.20.08 - Fax 06.24.40.69.99 - www.saetitalia.it - saetitalia@saetspa.it