a&S ITALY
Tecnologie e soluzioni per la sicurezza professionale
www.asitaly.com
febbraio 2017
anno VIII 43

Edifici multipurpose: progettare la sicurezza

Rivelazione incendi IP: aumentare il valore **e l'efficienza**

Big Data nella videosorveglianza

Proteggere il perimetro: **sfide e tecnologie**

HIKVISION

TOTAL SOLUTION PROVIDER

CCTV | Intrusion | Intercom | Access Control

HIKVISION

www.hikvision.com

ANTINTRUSIONE - CONTROLLO ACCESSI - VIDEOSORVEGLIANZA - RIVELAZIONE INCENDIO E GAS - AUTOMAZIONE PORTE E CANCELLI - CITOFONIA - VIDEO-CITOFONIA - TELEFONIA E INTERFONICI - NETWORKING - DIFFUSIONE SONORA - CLIMATIZZAZIONE

SICURTEC®

SOLUZIONI PER LA SICUREZZA

SICURTEC BRESCIA SRL

Sede: Via Bernini, 14 - 25010 San Zeno Naviglio (BS)

Tel. 030 35.32.006 - Fax 030 34.69.798 - info@sicurtecbrescia.it

Filiale: Via Venier, 7 (ang. via Pialoi, 20) - 30020 Marcon (VE)

Tel. 041 59.70.344 - Fax 041 59.71.744 - marcon@sicurtecbrescia.it

www.sicurtecbrescia.it

FINALMENTE MAGGIORENNI!

1999-2017

ANNIVERSARIO

18°

SICURTEC BRESCIA.

SICURI DI DARE IL MEGLIO.

JF TECH

Science & Technology, Make Life Better

IPC

12MP
4K
H.265
WDR
Starlight
Smart
Analisys

NVR

H.264/H.265
4K
POE

AHC

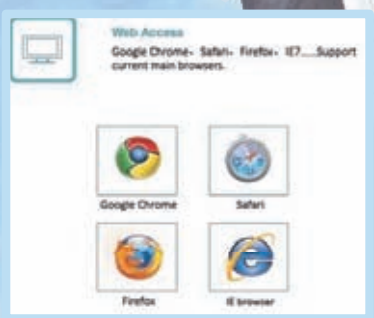
AHD-TVI-
CVI-CVBS
Switable
UTC control
OSD

ADVR

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

ACCESSORIES

Videowall
Monitor
Switch
Balun



Semplicemente...Alternativi

melchioni
PROFESSIONAL SECURITY SYSTEM

pss@melchioni.it

a&S ITALY
PERIODICO CON TIRATURA CERTIFICATA

FEBBRAIO 2017 – ANNO VIII – n.43

LE INDAGINI

LE INDAGINI

TECH CORNER

VERTICAL MARKET SOLUTIONS GALLERY

PARLIAMO DI BUSINESS

RIFLESSIONI

MERCATI VERTICALI

CHIEDI AL LEGALE

CHIEDI ALL'ESPERTO

TECH CORNER

VOCI DAL MERCATO

ACADEMY

MERCATI ESTERI

LE INDAGINI

FOCUS PRODUCT

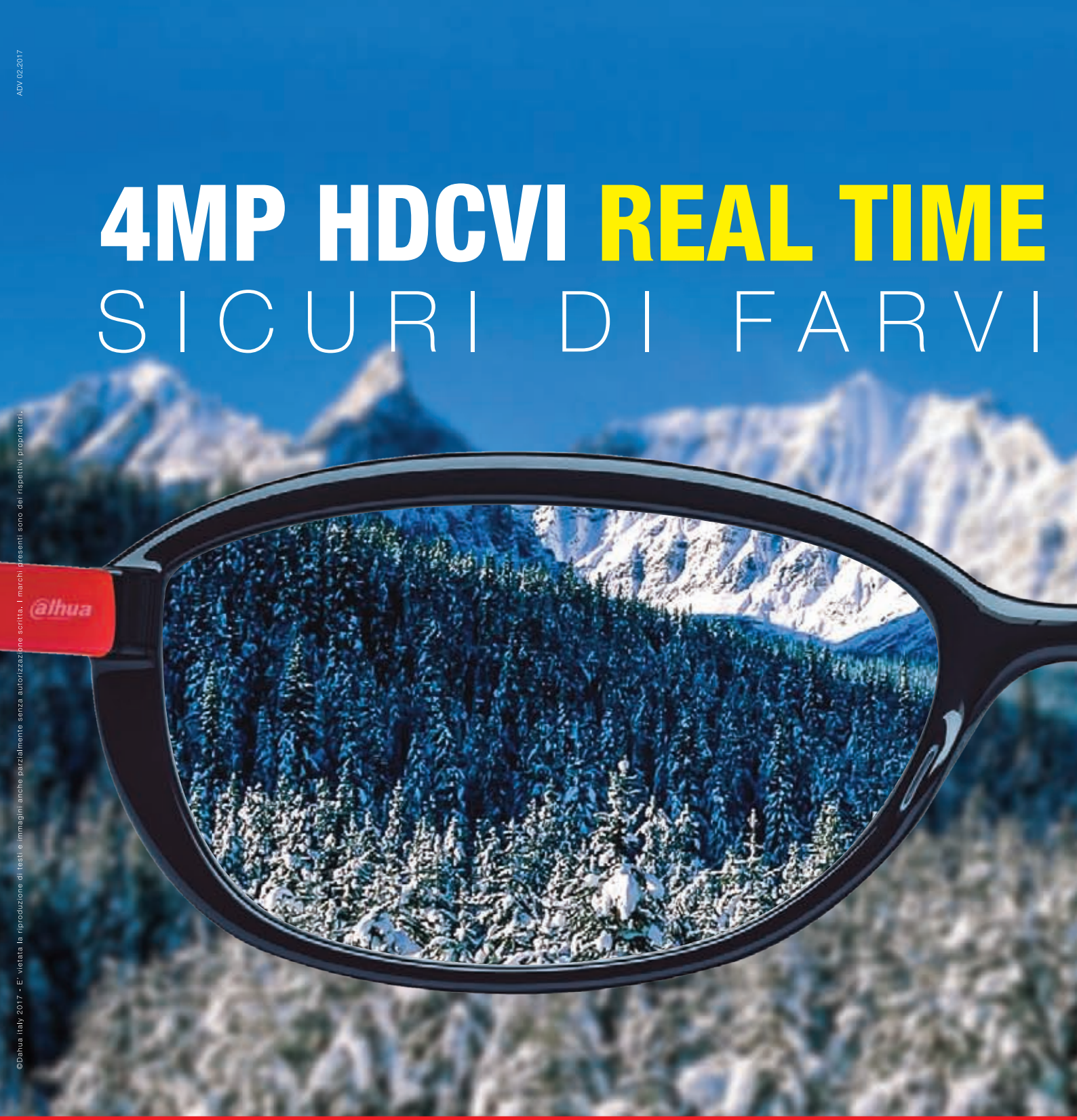
Certificarsi per differenziarsi

In un mercato sempre più inflazionato, dove il fai da te imperversa anche nel mondo "professionale" e diverse figure di altri comparti sono attratte dall'interessante redditività del settore sicurezza (ben più golosa di quella raggiungibile in aree *limitrofe* come l'ICT o il comparto elettrico), per gli operatori della security differenziarsi diventa un must. Ma come? La novità è che oggi il comparto ha la possibilità di accedere ad un sistema di certificazione dei professionisti serio ed affidabile.

Si tratta ovviamente di certificazione volontaria: uno strumento pensato per posizionare, valorizzare e differenziare le professionalità su un mercato complesso, ad alta densità di competizione ed estremamente frammentato. In un simile scenario, la certificazione rappresenta lo strumento di differenziazione più affidabile perché riconosciuto da una parte terza competente e indipendente, che si incarica sotto la propria responsabilità di garantire all'utente finale qualità e sicurezza della prestazione ricevuta. In una parola: del valore acquisito affidandosi a quello specifico soggetto. L'essenza stessa del processo di certificazione è infatti la dichiarazione di una terza parte, a sua volta sottoposta a diverse asseverazioni che ne testimoniano l'attendibilità, che una certa figura risulta essere dotata delle competenze necessarie per svolgere al meglio la sua professione e generare valore. Lo schema di certificazione è stato elaborato dal TUV ed Ethos Academy ci ha scommesso sin da subito. E voi?

4MP HDCVI REAL TIME

SICURI DI FARVI



Numeri 1 al mondo nei
sistemi megapixel analogici

alhua TECHNOLOGY

SU CAVO COASSIALE
VEDERE MEGLIO

VIDEOTREND
ITALIA | ESPAÑA
Chiedilo a noi!
Distributore esclusivo Dahua

VIDEOTREND Srl
Tel. +39 0362 182681
info@videotrend.net
www.videotrend.net

DAHUA ITALY s.r.l.
Via Torri Bianche, 9 - Torre Quercia Int. 14
20871 Vimercate (MB)
www.dahuasecurity.com

www.dahuasecurity.com

Tutta la sicurezza in una UNICA soluzione

BiTech

V.Tech

Sistema di allarme touch con video-verifica

- 4 zone filari espandibili a 20 IN-OUT con moduli bus RS485
- 28 zone (+4 REP) wireless con tecnologia bidirezionale BiTech
- Modello con o senza tastiera touch-screen integrata 7"
- Gestione di tastiere ausiliarie touch-screen 5,7" e capacitive
- Lettore di prossimità integrato RFID (solo su modello con touch)
- Video-verifica (fotogrammi) attivabile su allarme o richiesta con tecnologia V-Tech
- Infrarossi e doppia-tecnologia con telecamera (640x480 pixel) + AM
- Connettività multipla del sistema (digitale, GSM/GPRS, Lan)
- Anti-jamming su GSM e frequenza radio (868MHz)
- Invio messaggi in sintesi vocale tramite motore TTS (Text-To-Speech)
- App per Smartphone MY-SICEP (iOS, Android)
- Software di programmazione con quadro sinottico integrato (locale o da remoto)
- Completa gestione da Centrale Operativa SICEP - MvsNET
- Ampia gamma di accessori utilizzabili

ANDROID APP ON Google play

Available on the App Store

SICEP®

SICEP S.r.l.
50052 Certaldo (Firenze) - Via Calabria, 14 - Italy
Tel. 0571 664166 r.a. - Fax 0571 652285
Internet: http://www.sicep.it - e-mail: sicep@sicep.it

Distributore ufficiale per l'Italia

advanced innovations

Your perfect partner

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

DiMAR ELECTRONIC Srl

CERCHIAMO AGENTI

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

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

DiMAR ELECTRONIC Srl

www.dimarelectronic.eu

ASN®

www.asntransformer.com

JIANFU

www.jian-fu.com

HF®

www.forward-relays.com

DIMAR ELECTRONICS srl VIA NAZIONALE DEI GIOVI,13 - 20813 BOVISIO MASCIAGO (MB) - Italy
TEL.: +39-(0)-362 - 598268 - FAX: +39-(0)-362- 1441858 - Mobile: +39 335228943
E-mail: info@dimar-srl.com - Website: www.dimarelectronic.eu

Enforcer

All-in-one Smart Cloud Security Solution

ENFORCER tecnologia bidirezionale senza fili

Sistema Radio Bidirezionale Enforcer 32-WE APP
ENF-APP-KITG-IT

TECNOLOGIA WIRELESS BIDIREZIONALE IN UN'INTUITIVA INTERFACCIA CLOUD-BASED

Entra subito nella tecnologia wireless bidirezionale con il Kit Enforcer! Il Kit include: rivelatore IR Quad radio bidirezionale, contatto magnetico radio bidirezionale, telecomando radio bidirezionale, tag di prossimità e modem GPRS.
Ed attraverso HomeControlSIM, l'innovativa SIM Card Pyronix che ti offre la migliore soluzione di comunicazione e la maggior semplicità d'installazione via PyronixCloud, è possibile esaltare la semplicità e l'intuitività del sistema.

Key Features

- Bus radio con protocollo di cifratura a 128 bit
- Portata radio 1.6 km in campo aperto
- Compatibile con PyronixCloud e HomeControl+APP
- Fino a 32 dipositivi, 32 telecomandi radio e 2 sirene wireless
- Controllo istantaneo bidirezionale dei dispositivi (ITDC)
- Rilevamento jamming avanzato con tecnologia Hopping

marketing@pyronix.com | www.pyronix.com | Pyronix | @Pyronix

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

CYBERSECURITY: VARATO IL DECRETO E UN PROGRAMMA NAZIONALE

ROMA – Un programma nazionale per la cybersecurity in più fasi e un nuovo decreto in sostituzione del decreto Monti, che risale al gennaio 2013 e che fino ad oggi ha regolato l'architettura nazionale per la sicurezza cibernetica. Sono queste le decisioni prese il 17 febbraio scorso durante una riunione del Cisr (Comitato Interministeriale per la Sicurezza della Repubblica), presieduto dal presidente del Consiglio Paolo Gentiloni.

http://www.secsolution.com/notizia.asp?id=7415

TVCC: PROSPETTIVE DI CRESCITA PER LO SMALL BUSINESS

BIRMINGHAM (UK) - Ben l'82% delle PMI dotate di videosorveglianza intende aggiornare o sostituire il vecchio impianto. Lo rivela una ricerca di Axis Communication su 500 piccole imprese del Regno Unito. Dal sondaggio emerge che oltre un terzo degli intervistati (il 39%) sta valutando di effettuare l'intervento entro i prossimi 2 anni e la ragione più frequente è la ricerca di sistemi più efficaci di prevenzione di furti e perdite: quasi il 38% degli intervistati ha dichiarato infatti di avere subito effrazioni e furti nei propri locali.

http://www.secsolution.com/notizia.asp?id=7329

REPORT ANNUALE SULLA SICUREZZA

MILANO – Il 12° Worldwide Infrastructure Security Report (WISR) di Arbor Networks sulla sicurezza delle infrastrutture mondiali raccoglie le osservazioni degli esperti di reti presso le maggiori organizzazioni aziendali e i principali provider di telecomunicazioni, cloud e hosting. Diverse le tematiche: dall'identificazione delle minacce alla risposta agli incidenti, passando per la definizione di servizi, personale e budget dedicati, fino alle problematiche affrontate ogni giorno dai professionisti della sicurezza informatica e alle strategie adottate per mitigarle.

http://www.secsolution.com/notizia.asp?id=7310

4,67 MILIARDI DI DOLLARI: IL 2016 DI HIKVISION

VITTORIO VENETO (TV) – 4,67 miliardi di dollari di fatturato con una crescita anno su anno del 26.69%, un utile operativo di 998 milioni di dollari (+ 24.84%) e un profitto totale di 1,2 miliardi di dollari (+ 23.56%). Questi i risultati del preliminare di bilancio Hikvision, numero 1 al mondo per soluzioni e sistemi di sicurezza, per l'anno 2016. Il segreto di questo successo? Investimenti costanti in R&D, una gamma completa in senso orizzontale e verticale, continuo ampliamento del business sul piano globale, nuovi segmenti operativi.

http://www.secsolution.com/notizia.asp?id=7433

LAVORO DOMESTICO E VIDEOSORVEGLIANZA

ROMA – L'Ispettorato Nazionale del Lavoro, con nota prot. n. 1004 dell'8 febbraio 2017, ha affrontato il tema dell'installazione di videosorveglianza in un'abitazione privata ove operi un lavoratore domestico. Per installare un impianto in questi casi non occorre chiedere alcuna autorizzazione alla sede competente dell'Ispettorato territoriale, ma si applica comunque la disciplina sul trattamento dei dati personali, quindi occorre ottenere il consenso preventivo del lavoratore e fornirgli l'informativa.

http://www.secsolution.com/notizia.asp?id=7381

RUGGERO LENSI NUOVO DIRETTORE GENERALE DI UNI

MILANO - Il Consiglio Direttivo di UNI (Ente Italiano di Normazione) ha nominato Ruggero Lensi nuovo Direttore Generale. Una scelta, come l'ha definita il Presidente Torretta, "per la continuità nel miglioramento". Lensi, ingegnere civile, è entrato in UNI nel 1995 come Funzionario Tecnico, diventando Coordinatore dell'Attività di Normazione nel 2000 e Direttore Tecnico nel 2003. Dal 2010 ricopre il ruolo di Direttore Relazioni esterne, sviluppo e innovazione. E' il rappresentante italiano nel Consiglio di Amministrazione del CEN.

http://www.secsolution.com/notizia.asp?id=7371

SICUREZZA ANTINCENDIO: ACCORDO ANIMA E VVFF

ROMA – Federazione Anima e Corpo Nazionale dei Vigili del Fuoco hanno firmato un accordo di collaborazione finalizzato alla condivisione di esperienze e competenze in materia di sicurezza antincendio. Tra gli obiettivi, la promozione della cultura della sicurezza e lo sviluppo di attività e progetti volti alla prevenzione degli incidenti collegati al rischio incendi, oltre alla diffusione di buone pratiche - tecniche, organizzative e formative - coerenti alle evoluzioni normative e alle nuove modalità di organizzazione del lavoro.

http://www.secsolution.com/notizia.asp?id=7340

CONTROLLO ACCESSI: ATTESO UN EXPLOIT

BIRMINGHAM (UK) – Ottime prospettive di crescita per il mercato del controllo accessi su scala mondiale. È quanto emerge dalla recente ricerca pubblicata da report-snreports.com, che prevede un incremento annuale fino al 13% entro il 2020, a partire dal tasso attuale pari al 7.49%. Se nel 2015 il mercato globale del controllo accessi valeva 5.92 miliardi di dollari, le aspettative per il 2022 sono di raggiungere i 9.8 miliardi. Tra le ragioni della crescita, l'incremento delle minacce alla sicurezza, la maggiore urbanizzazione e i progressi della tecnologia.

http://www.secsolution.com/notizia.asp?id=7334

ASSIV: NUOVA GIUNTA DI PRESIDENZA

ROMA - I Consiglio direttivo di Assiv ha nominato i consiglieri delegati, proposti dalla neo Presidentessa Maria Cristina Urbano, che comporranno la nuova Giunta di Presidenza. Ai sei attuali membri (Marco Bavazzano - Axitea; Massimiliano Giacoletti - Allsystem; Giulio Gravina - Italpol; Carlo Matarazzo - Cosmopol; Fabio Mura - Mondialpol Services Group; Raffaele Zanè - Securitas Metronotte) è stato attribuito l'incarico di vice Presidente: a marzo il Consiglio Direttivo nominerà un ulteriore membro in rappresentanza delle PMI.

http://www.secsolution.com/notizia.asp?id=7315

ANIE SICUREZZA-IMQ: CORSO PER MANUTENTORE FIRE

MILANO - Anie Sicurezza propone un corso per manutentori di componenti di impianti di rivelazione automatica e manuale antincendio e di evacuazione audio, propedeutico alla certificazione IMQ della figura professionale del Tecnico Manutentore. In assenza di una norma o di un albo, lo schema di certificazione IMQ-ANIE T.I.R.A.E., rivolto ai Tecnici Manutentori Fire ed Evac, si pone quale percorso qualitativo in grado di attestare tali competenze e fornire una garanzia oggettiva all'utente finale. Il corso di formazione si svolgerà a Milano dal 27 al 30 marzo 2017.

http://www.secsolution.com/notizia.asp?id=7398

NATALE MOZZANICA CONFERMATO ALLA PRESIDENZA UMAN

MILANO - L'associazione nazionale delle aziende sicurezza e antincendio, Uman, ha confermato fino al 2018 Natale Mozzanica come presidente, eletto per il suo primo mandato nel 2014. Il suo programma è di promuovere il riconoscimento delle aziende a livello legislativo-normativo e di completare i percorsi per la formazione dei i tecnici manutentori, considerando che al momento sono state coperte solo alcune discipline (manutenzione estintori, manutenzione componenti idranti, manutenzione porte tagliafuoco, manutenzione sistemi di evacuazione naturale fumo e calore e manutenzione stazioni di pompaggio).

http://www.secsolution.com/notizia.asp?id=7215

COSA RISERVA IL CLOUD PER QUESTO 2017?

MILANO – Da una recente ricerca Check Point Software Technologies emerge che per il 93% delle aziende la sicurezza dei cloud risulta essere un tema preoccupante. Basandosi sui risultati dello studio, Check Point formula due previsioni per questo 2017: 1) probabile attacco contro un importante fornitore cloud, dal momento che le aziende archiviano un numero sempre maggiore di dati sul cloud pubblico e vi trasferiscono i flussi di produzione; 2) un ransomware che si insidierà in un data center.

http://www.secsolution.com/notizia.asp?id=7198

Integrazione WIRELESS

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

Semplicità di installazione ed elevati standard di sicurezza

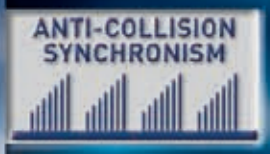
40 anniversario
Tecnoalarm 1977 - 2017

1977 - 2017
40 anni di ricerca e innovazione

SYNC@BWL

Doppia banda bidirezionale supervisionata

16 canali per banda con sintonia automatica



Sincronismo modulare anticollisione

Protocollo con doppia chiave di crittografia

Autoregolazione dinamica potenza RF

Gestione intelligente degli assorbimenti

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

Tecnoalarm
HI-TECHNOLOGY & DESIGN
WORLDWIDE FROM ITALY

Tecnoalarm
Via Ciriè, 38 - 10099
San Mauro T.se Torino (Italy)
tel. +390112235410 - fax +390112735590
info@tecnoalarm.com
www.tecnoalarm.com

Full Video IP per proteggere un leader nella lavorazione carne

solutions gallery

LA PROBLEMATICA

Carnitalia Spa, azienda italiana di Ospedaletto Lodigiano nata negli anni '50, leader nella lavorazione della carne, si sviluppa su un'area di 20.000mq. Lo stabile aveva subito nel febbraio 2015 un incendio fortuito e quindi l'intero stabile ha dovuto subire una completa ricostruzione. Durante la progettazione si è valutata l'introduzione di una tecnologia per la protezione dell'intera struttura direttamente sul perimetro esterno. L'area è disposta lungo il tratto dell'A1 e della TAV, quindi soggetta a diverse interferenze ambientali, ed è esposta ad una forte nebbia invernale: la scelta delle tecnologie doveva quindi essere particolarmente oculata.

LA SOLUZIONE

Il totale rifacimento delle strutture, caratterizzato da design moderno, funzionale ed accattivante, è durato solamente 14 mesi grazie alla collaborazione proattiva tra la proprietà, la direzione tecnica dell'azienda, la società che ha curato il progetto e tutti gli operatori interessati. La soluzione per la protezione di un sito di tali dimensioni è stata valutata, ponderata e comparata con varie tecnologie: la scelta è ricaduta sullo standard che ormai da 40 anni garantisce la sicurezza delle maggiori Infrastrutture Critiche nel mondo: la barriera a microonde ad analisi digitale fuzzy logic Ermo 482X pro di CIAS, distribuita nell'area da Sicurtec Brescia. La barriera a microonde da sempre garantisce la sua funzionalità in qualunque condizione ambientale, sia con temperature estreme, sia in ambienti esterni con scarsa visibilità (fumo o nebbia). La soluzione è stata quella di posizionare le varie tecnologie lungo il perimetro esterno secondo una disposizione tale da minimizzare l'impatto estetico, ma nel contempo in grado di asservire la piena funzionalità di tutte le tecnologie.

La nuova generazione di barriere intelligenti CIAS, progettata per situazioni ad alto rischio, offre caratteristiche qualificanti, ovvero indispensabili in questa installazione, e più precisamente:

- digitalizzazione del segnale che può essere visualizzato ed analizzato (forma d'onda del segnale) per una migliore taratura e per la *cancellazione* di eventuali disturbi ambientali, anche causati da piccoli animali;
- firmware di funzionamento *a logica sfumata o probabilistica* (fuzzy), che conferisce alle barriere CIAS una precisione di allarme mai raggiunta prima e con il più alto grado di discriminazione di eventi impropri;
- barriere collegate e alimentate da

un unico cavo Over IP che possono essere controllate da un solo punto di monitoraggio con la facoltà di telegestire da remoto l'intero sistema grazie alla scheda IP Doorway.

A completamento della protezione del sito vi sono anche sensori antintrusione interni volumetrici a doppia tecnologia anti masking, sistema di controllo accessi di prossimità, impianto di rilevazione fumi ed impianto di telecamere megapixel IP fisse e dome, il tutto centralizzato nella control room.

I BENEFICI

L'impianto di Carnitalia Spa rappresenta lo stato dell'arte della tecnologia moderna che integra tutti i dispositivi su IP minimizzando l'utilizzo delle infrastrutture senza rinunciare alle performance e alla sicurezza delle informazioni. Il responsabile servizi generali e tecnologici d'azienda, Ing. Gianfranco Pastorelli, dichiara che nella nuova struttura era necessario un impianto all'altezza dell'innovazione e che garantisse la massima sicurezza della struttura e dei suoi impianti come quello proposto ed installato. Il progetto dell'immobile è frutto dello Studio Castiglioni & Nardi Architetti Associati di Varese, la progettazione degli impianti è della società Varese Controlli (Ing. Stefano Castellani, Ing. Carlo Ascoli, Ing. Dario Bellocchio, Geom. Alessandro Pasquadibisceglie), gli impianti di sicurezza sono stati forniti da CIAS Elettronica ed installati dalla PA Sistemi di Brescia (PM. Cristian Zenoni), che ha attivamente partecipato alla fase progettuale proponendo nel dettaglio la migliore tecnologia di protezione.

CIAS ELETTRONICA www.cias.it

Carnitalia Spa, leader nella lavorazione carne, protegge il perimetro esterno con la barriera a microonde ad analisi digitale fuzzy logic di CIAS

Il firmware di funzionamento a logica sfumata o probabilistica (fuzzy) conferisce alle barriere CIAS il più alto grado di discriminazione di eventi impropri

L'impianto di Carnitalia Spa integra tutti i dispositivi su IP, minimizza l'uso delle infrastrutture, garantisce performance e sicurezza delle informazioni

Gli SCL Tigers guadagnano punti in fatto di sicurezza

solutions gallery

LA PROBLEMATICA

Gli "SCL Tigers" sono ai vertici delle classifiche svizzere di hockey su ghiaccio dal 1964. La squadra ha sede nello stadio di ILFISHALLE a Langnau i.E. Gli "SCL Tigers" giocano nella
Lega nazionale A: per le squadre di questa categoria, la Federazione svizzera dell'hockey su ghiaccio prevede norme rigorose di sicurezza. Dopo una lunga serie di incidenti, la Federazione ha imposto delle norme specifiche a salvaguardia dell'incolumità delle persone e della sicurezza delle strutture all'interno e nel perimetro dello stadio. La scelta tecnologica è ricaduta su Panasonic.

LA SOLUZIONE

Per monitorare l'interno dello stadio sono state utilizzate telecamere 4K di Panasonic, che coprono un'area 4 o 9 volte superiore a quella delle telecamere a 1080p o 720p. Ciò non soltanto assicura una qualità dell'immagine più elevata e affidabile, ma riduce anche i requisiti di velocità di trasmissione di rete. Grazie allo zoom ottico 6x è possibile identificare chiaramente oggetti e persone. A ILFISHALLE, sopra alle tribune, sono state installate telecamere dome 4K WV-SFV781L. Da tale posizione, questi dispositivi monitorano l'area opposta e i lati delle tribune. Sono talmente evoluti che ne bastano 2 per monitorare l'intera lunghezza di una tribuna. Anche le tribune laterali e le curve dei tifosi vengono monitorate ciascuna con una telecamera 4K, che registra e documenta con precisione ogni dettaglio. Il grandangolo è importante: queste telecamere 4K garantiscono una nitidezza cristallina in tutte le aree dell'immagine, senza differenza fra il centro e gli angoli. E tutto questo è possibile anche a una distanza di oltre 50 m fra la telecamera e gli spettatori! Un altro vantaggio della tecnologia 4K è la riduzione del numero di telecamere e della quantità di risorse necessarie per visualizzare e valutare le immagini. Naturalmente, limitando l'hardware richiesto si contengono i costi operativi generali, pur migliorando la qualità. La telecamera antivandalo WVSFV781L si distingue anche per l'alto livello di affidabilità.
Per le aree più piccole si è scelto il modello WV-SFV631, un prodotto antivandalo ideale per monitorare angoli e spazi ristretti. Grazie a funzionalità quali Auto Back Focus (ABF) e Remote Zoom, l'installazione diventa più semplice, poiché è possibile impostare il dispositivo mediante un PC desktop o portatile. Se una telecamera perde il fuoco, è facile correggere il problema senza dover utilizzare una scala. Inoltre la funzione "Deep of Field" (DoF) sviluppata per la fotografia garantisce la costante nitidezza delle immagini, sia negli ingrandimenti che a lunga distanza. Per maggiore flessibilità

nel monitoraggio all'interno e all'esterno dello stadio è stata selezionata la telecamera dome IP Full HD WV-SW598A, dotata di funzione PTZ. Questa telecamera integra uno zoom ottico 30x ed è protetta da un case IP66 antivandalo. Con la sua gamma dinamica da 128x, è perfetta per produrre immagini giorno e notte. Grazie alla sua ricca dotazione, la SW598A è una telecamera intelligente, le cui funzionalità analitiche consentono prestazioni ottimali persino in presenza di pioggia, neve o nebbia. La calotta speciale, con tecnologia antipioggia, supporta e migliora ulteriormente la qualità eccezionale delle immagini. Per le necessità di registrazione lo stadio utilizza il modello WJ-NV300. Questo registratore con disco rigido e supporto di rete si connette fino a 32 canali video. È un dispositivo che si distingue per l'elevata affidabilità e l'interfaccia utente grafica intuitiva e lineare. Su tutti i canali sono possibili registrazioni live e in tempo reale (30 fps). Le telecamere sono di facile uso e consentono la sorveglianza live in diverse modalità di visualizzazione. Tramite lo splitter integrato, un monitor aggiuntivo può mostrare la panoramica di un'intera partita di hockey su ghiaccio. Di conseguenza, è molto semplice eseguire ricerche o esportare foto o sequenze video, sia sul registratore che su un PC in rete.

I BENEFICI

Le soluzioni di sicurezza IP Panasonic offrono le tecnologie più recenti e una vasta gamma di funzioni innovative per una molteplicità di applicazioni di sorveglianza e consentono di investire capitale nel modo migliore, traendone il massimo vantaggio.

PANASONIC http://business.panasonic.it/

Lo stadio di ILFISHALLE - sede degli SCL Tigers, squadra storica di hockey su ghiaccio in Svizzera – è protetto da un sistema di videosorveglianza Panasonic all'avanguardia.

Numerose telecamere Panasonic distribuite all'interno e all'esterno dell'edificio gestiscono tutti gli aspetti della sicurezza di una partita di hockey su ghiaccio.

Tecnologia 4K: immagini sempre nitide e dettagliate, area più estesa, meno costi operativi.

Quando il controllo accessi è gestito (anche) da lontano

solutions gallery

LA PROBLEMATICA

È meglio gestire in casa la sicurezza della propria azienda o è più sicuro ed economico affidarsi alle mani esperte di una società esterna specializzata? Ogni scelta, si sa, ha i suoi pro e i suoi contro. Comunque la si pensi, è in costante crescita il numero di soggetti che affidano all'esterno la gestione della propria sicurezza, in Italia come all'estero. In risposta a questo fenomeno stiamo assistendo ad una mutazione degli operatori del settore, i quali si stanno trasformando da tradizionali istituti di vigilanza in imprese capaci di offrire una molteplicità di servizi attraverso l'impiego di tecnologie avanzate e nel pieno rispetto della privacy. Una delle aziende di maggior spicco in questo campo è Lis SpA di Olgiate Olona (VA). Dal 1982 la società fornisce soluzioni e tecnologie rivolte a proteggere beni (materiali e immateriali) e persone. Grazie all'esperienza maturata in questi 34 anni di attività e al costante processo di ricerca e sviluppo, Lis offre un servizio completo e su misura in materia di sicurezza fisica e logica ponendosi nei confronti del cliente come unico fornitore tecnologico di riferimento. Non solo. In sede di stipula della polizza assicurativa, le condizioni riservate al cliente da parte di primarie compagnie, sono spesso così vantaggiose da poter coprire l'intero costo del servizio. Alla telegestione dei classici impianti di sicurezza (antintrusione, antincendio, telesorveglianza ecc.), Lis ha affiancato da tempo anche il controllo elettronico degli accessi, sia perimetrali che interni. L'esigenza della società, tuttavia, non era quella di disporre solo di un controllo accessi tradizionale (ormai integrato nella maggior parte degli impianti antintrusione), ma di offrire una soluzione molto più completa e avanzata, in grado anche di integrarsi pienamente nella propria Centrale Operativa.

LA SOLUZIONE

La Centrale Operativa è il fiore all'occhiello dell'azienda varesina. Attiva tutti i giorni dell'anno, 24 ore su 24, gestisce attualmente circa 5000 servizi. É da questa avveniristica control room – opportunamente protetta e dotata delle infrastrutture ICT più evolute – che viene tenuta sotto costante controllo la sicurezza dei clienti. Un team di operatori, selezionati e formati, assolve ogni giorno un compito impegnativo e delicato, quello di dare al cliente una risposta rapida e puntuale, completa e risolutiva, come si richiede in ogni situazione di emergenza. Per l'identificazione automatica degli utenti (persone e veicoli), per il controllo elettronico degli accessi e per la rilevazione delle presenze al lavoro, da anni Lis ha scelto come partner tecnologico la Elex srl di Torino. Elex,

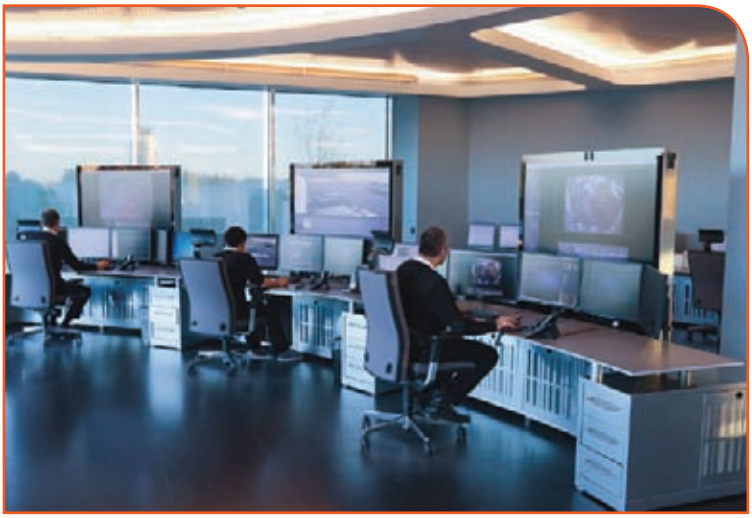
nata 28 anni fa, un know how che risale ai primi anni '70, è un'azienda italiana indipendente da gruppi industriali, specializzata esclusivamente nel settore accessi e presenze. Con oltre 20 mila installazioni in tutta Italia vanta referenze in ogni settore merceologico. La soluzione progettata e prodotta dalla società torinese – offerta da Lis alla propria clientela business, in versione autonoma o integrata nella Centrale Operativa - è Censor® S1XX, sistema elettronico, hardware e software, di ultima generazione. Il sistema, in particolare, si avvale di Controller per accessi, multivarco e polivalenti, progettati e prodotti da Elex, in grado di operare sia in modalità networked che stand alone, capaci di supportare tutte le tecniche d'identificazione (PIN, card, transponder, smartphone, impronta biometrica ecc.) e di offrire ben 35 funzioni supplementari oltre al classico comando di apertura.

I BENEFICI

Il controllo degli accessi è uno dei tasselli del mosaico sicurezza che Lis, attraverso la Centrale Operativa, gestisce a distanza, con la massima tempestività ed efficacia. Integrare gli accessi insieme agli altri sottosistemi (furto, incendio, video ecc.) non è compito facile se si vogliono sfruttare le notevoli potenzialità offerte da questa tipologia d'impianto. L'integrazione realizzata nel caso specifico è riuscita a conciliare le esigenze di un controllo raffinato e di una minuziosa tracciabilità degli eventi, sempre più richieste dalla clientela, con la necessità di sintesi di una grande Centrale Operativa. Il sistema Elex, infatti, da un lato consente un monitoraggio puntuale e completo di tutto ciò che accade e dall'altro offre una serie di telecomandi sui singoli varchi (blocco, sblocco, fuori servizio ecc.), particolarmente utili ai fini dell'integrazione.

ELEX www.elex.it

Lis è un'affermata società di servizi per la protezione dei beni e delle persone con sede a Olgiate Olona (VA).



Uno scorcio della Centrale Operativa Lis. É da qui che viene telegestita tutto l'anno, 24 ore su 24, la sicurezza della clientela, inclusi gli accessi.

Per controllare e telegestire gli accessi dei propri i clienti, Lis ha scelto come partner tecnologico la Elex srl di Torino.

Sicurezza a bordo: vantaggi di una soluzione mobile avanzata

solutions gallery

LA PROBLEMATICA

Negli ultimi anni, la notevole crescita della popolazione nelle aree urbane ha portato ad un incremento della domanda di servizi pubblici, come autobus, tram e taxi. Tuttavia, soprattutto in un periodo di crisi economica come quello che stiamo da tempo vivendo, fenomeni criminosi come le rapine o atti di teppismo e vandalismo sono cresciuti in maniera altrettanto proporzionale, rendendo le città e l'utilizzo dei mezzi pubblici un servizio poco sicuro per i passeggeri e per gli stessi conducenti. Secondo diversi sondaggi, questi fenomeni rappresentano una seria fonte di preoccupazione per gli abitanti degli agglomerati urbani: di conseguenza per le Amministrazioni trovare una soluzione efficiente ed affidabile per gestire e controllare le situazioni critiche è diventata un'assoluta priorità.

LA SOLUZIONE

Dahua ha messo in campo una soluzione mobile avanzata per permettere ai conducenti, ai passeggeri ed alle aziende di taxi e di autobus di salvaguardare la propria sicurezza attraverso un servizio più, che garantisce anche un notevole risparmio di tempo ed energia. La soluzione mobile di Dahua offre un servizio completo che comprende tutta la componentistica HD-SW: dalle telecamere al sistema di registrazione, fino alla piattaforma di gestione e controllo della soluzione video (Mobile System Management Platform). Per soddisfare le diverse esigenze del cliente, Dahua ha sviluppato ed immesso sul mercato tre differenti serie di sistemi: IP, HDCVI ed analogico. Anche le telecamere prevedono formati diversi ed adatti a tutte le necessità: compatto, minidome, etc. Il sistema di registrazione (DVR/NVR), oltre alla memorizzazione locale, è in grado di scambiare dati con la piattaforma attraverso le reti wireless 3G , 4G e WIFI: è inoltre in grado di inviare al sistema di gestione centrale la posizione GPS del veicolo e le eventuali informazioni di allarme. La soluzione Dahua si completa con tutti i necessari accessori per supportare diverse applicazioni: il microfono a mano per la comunicazione bidirezionale, il pulsante di emergenza, il sensore di livello del carburante per controllare i consumi, il lettore di carta magnetica per il conducente, lo schermo da 7 pollici. Il cuore del sistema Dahua Mobile Solution è rappresentato dal Server DSS-M, che è in grado di collegare contemporaneamente fino a 2000 canali e viene principalmente utilizzato per controllare e gestire i DVR presenti sui mezzi mobili. La soluzione mobile di Dahua è stata progettata tenendo presente tre aspetti essenziali:

Backup Automatico via WiFi - Il segnale wireless in un automezzo passa automaticamente dalla rete 4G a WiFi quando il veicolo rientra nuovamente al deposito, di conseguenza tutte le im-

magini registrate vengono scaricate nel sistema centrale per essere a disposizione degli operatori del Centro di Controllo.

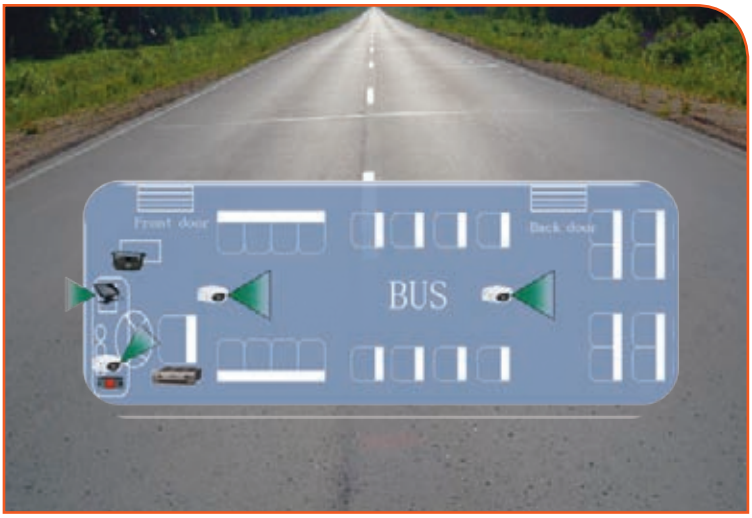
People Counting (IPC) - La funzione di People Counting viene utilizzata per contare il numero di persone che hanno usato un veicolo in un determinato periodo di tempo. Le statistiche vengono inviate dal registratore alla piattaforma DSS, attraverso la rete wireless, per essere elaborate e generare report ed analisi dei flussi.

Mappe grafiche con aree regolamentate - Dal centro di controllo è possibile creare sulle e-map delle aree nelle quali applicare determinate regole, come velocità massima di un mezzo, oppure generare un allarme quando un veicolo transita in un'area non autorizzata. Questo sistema viene spesso applicato su mezzi come Portavalori o Cisterne Carburante, dove la pericolosità del carico sconsiglia il passaggio in determinate zone della città.

I BENEFICI

La soluzione mobile di Dahua, grazie alla sua avanzata tecnologia (People Counting, Geo Fance etc), permette di realizzare una piattaforma completa per la gestione di un impianto video on board: dal centro di controllo, quindi, tramite l'utilizzo di mappe grafiche, è possibile gestire un'intera flotta di mezzi conoscendone l'esatta posizione, il percorso effettuato e gli allarmi ed è possibile avere tutte le registrazioni delle telecamere sempre disponibili (live-playback) salvaguardando la sicurezza di conducenti e passeggeri. Con i successi ottenuti sul campo in molti paesi, come il Messico, la Turchia e la Thailandia, questa soluzione ha dimostrato la propria efficacia nel garantire un valido supporto al trasporto pubblico urbano e nel migliorare l'esperienza degli utenti. Nel 2013 è stato realizzato il Progetto Città Bus in Russia, dove sono stati utilizzati oltre 8000 DVR mobile di Dahua.

DAHUA ITALY www.dahuasecurity.com



La soluzione mobile di Dahua si incardina su backup automatico via WiFi; people counting (IPC); mappe grafiche con aree regolamentate

Nel 2013 è stato realizzato il Progetto Città Bus in Russia, dove sono stati utilizzati oltre 8000 DVR mobile di Dahua

Una piattaforma completa per gestire un impianto video on board: tramite mappe grafiche, dal centro di controllo si può gestire un'intera flotta e disporre di tutte le registrazioni

Soluzioni Audio per Parcheggi e Aree di Sosta

INTERFONIA E DIFFUSIONE SONORA OVER IP

ermes
freedom to communicate

Barre d' Ingresso
Assistenza Clienti

Telecomando Ascensori
Spirale Induttiva

Gestione a Distanza
Chiamate d'Emergenza

Diffusione Sonora
Annunci Commerciali

P2P Peer To Peer

PoE Power over Ethernet

VoIP Voice over IP

No Server

www.ermes-cctv.com ermes@ermes-cctv.com Tel. +39 0438 308470 Via Treviso, 36 - 31020 San Vendemiano (TV) - Italy

Nuovo design, qualità di sempre.

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

combivox.it

Simplya

NUOVO DESIGN, QUALITÀ DI SEMPRE.

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

Scopri di più su www.combivox.it

MADE IN ITALY

COMBIVOX
ENJOY LIFE, SAFELY.

MAGGIPINTO

La Redazione

Crescita con redditività: identikit di un comparto maturo

SECONDA PARTE

Siamo giunti al quinto appuntamento con Italian Security Leaders, Top 25, l'attesa indagine finanziaria sviluppata annualmente dalla rivista a&s Italy assieme all'analista KF Economics (Gruppo K Finance). E' quindi tempo di fare bilanci anche sul piano quinquennale, confrontando l'andamento del comparto sicurezza nell'intero lasso di tempo compreso tra il 2011 e il 2015, con uno sguardo già proiettato però sul 2016 appena chiuso. Ebbene, pur analizzando un quinquennio non certo brillante per l'economia italiana nel suo complesso, dall'indagine emerge la fotografia di un comparto ormai maturo, che cresce continuativamente senza compromettere la propria redditività. Se la prima parte dell'indagine (a&s Italy n. 42/Dicembre 2016) si concentrava sugli aspetti "macro" dell'andamento di settore, questa seconda parte si addentra nei numeri del comparto.

CRESCITA E REDDITIVITÀ

Come nella scorsa edizione il settore dei produttori di sistemi di anti intrusione si conferma il leader nella marginalità con un eccellente 17,8%, sebbene sostanzialmente stabile (+3,9% di crescita media); anche i campioni della crescita si confermano i produttori di sistemi TVCC (+17,2%) che pagano invece in termini di redditività ("solo" il 5,2%).

Questa osservazione conferma il fatto che sia difficile, sia per una azienda sia per un settore, avere delle prestazioni eccezionali di marginalità e, al contempo, di crescita. Infatti per spingere in modo straordinario

FIGURA 1

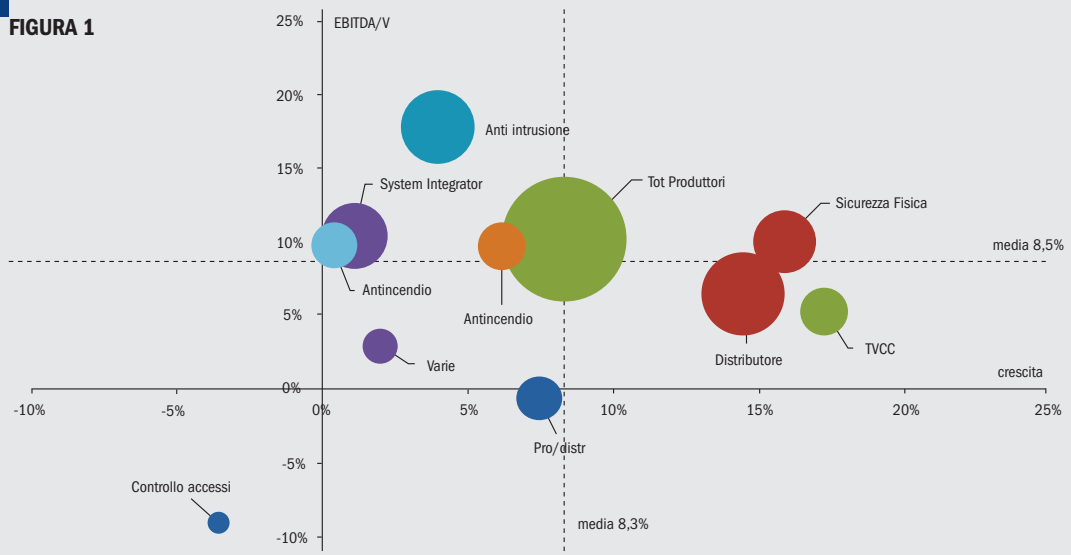


Figura 1. La dimensione delle bolle è pari al fatturato del comparto, in relazione al campione da noi analizzato. Questo grafico esprime la distribuzione per EBITDA/V e crescita ricavi 2014-15 (solo aziende PMI/Corporate). a&s Italy© - Tutti i diritti riservati

BOX 1

EBITDA/RICAVI %		
POSIZIONAMENTO COMPETITIVO	*Impresa manifatturiera*	*impresa di distribuzione*
SAD - Sex, Alcohol, Drugs	>50%	
monopolio/oligopolio	40%	*>10% non è un distributore*
vantaggio competitivo unico e sostenibile	25%	*8%*
vantaggio competitivo riconoscibile	20%	*7%*
modesto vantaggio competitivo	15%	*6%*
"me too" efficiente	12%	*5%*
"me too"	10%	*4%*
mediocrità	8%	*3,5%*
sopravvivenza	6%	*3%*
default	<6%	*<3%*

Box 1. Tabella indicativa di confronto tra valori di EBITDA/V e posizionamento competitivo. a&s Italy© - Tutti i diritti riservati

TABELLA 1

Settori	Ricavi	Media EBITDA/V	Media Crescita Ricavi
Anti intrusione	181.926	17,8%	3,9%
antincendio	81.536	9,5%	6,3%
Controllo accessi	21.512	-9,0%	-3,6%
Sicurezza fisica	156.895	10,1%	15,9%
TVCC	71.475	5,2%	17,2%
Varie	55.141	2,9%	2,0%
Tot Produttori	**568.485**	**10,1%**	**8,3%**
Distributore	248.181	6,3%	14,5%
Pro/distr	70.632	-0,6%	7,5%
System Integrator	172.218	10,4%	1,1%
Totale complessivo	**1.059.517**	**8,5%**	**8,3%**

Tabella 1. Distribuzione per EBITDA/V e crescita ricavi 2014-15 (solo aziende PMI/Corporate). a&s Italy© - Tutti i diritti riservati

FIGURA 2

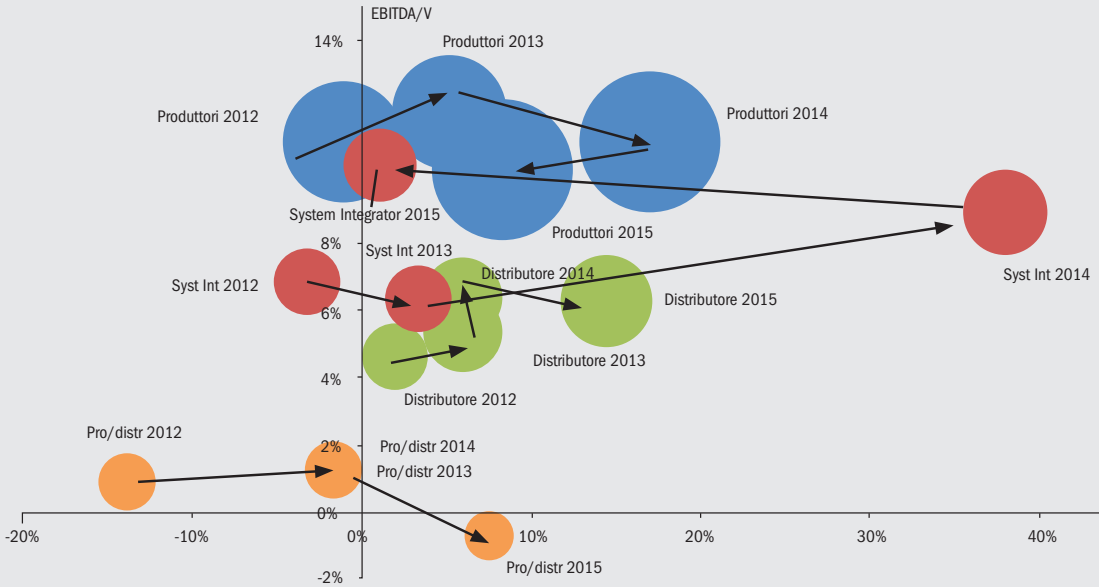


Figura 2. Andamento storico di redditività e crescita. a&s Italy© - Tutti i diritti riservati

FIGURA 3

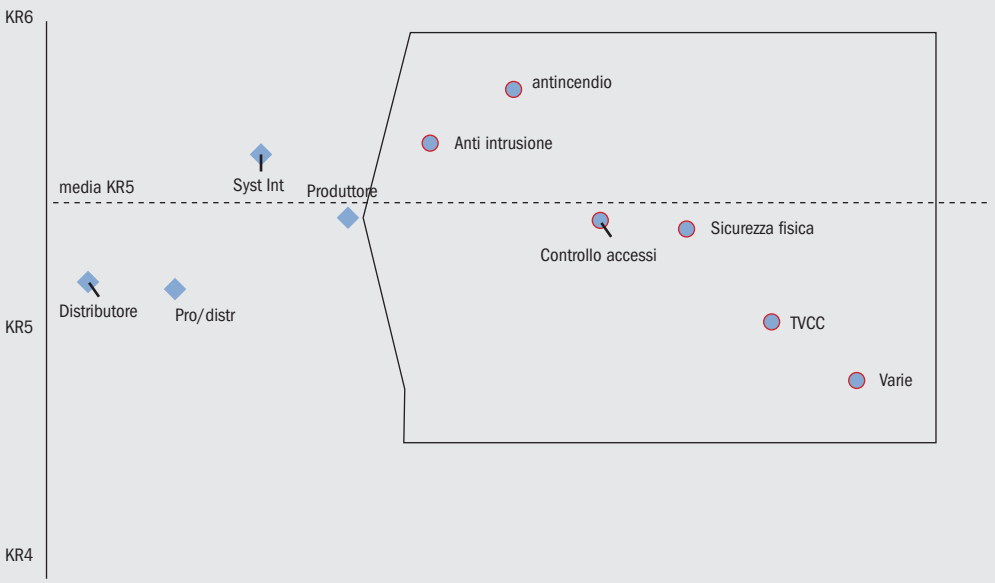


Figura 3. Andamento storico di redditività e crescita. a&s Italy© - Tutti i diritti riservati

sulla crescita si tende a sacrificare l'efficienza a favore dell'efficacia: perseguendo anche commesse con marginalità non eccellente o acquisendo altri operatori con marginalità inferiore per allargare il proprio mercato.
Rispetto all'anno passato la situazione del campione dei system integrator si è stabilizzata; il balzo del 2014 rispetto al 2013, che era principalmente dovuto all'ingresso nel nostro campione di un grosso player non presente nelle precedenti edizioni, si è ricomposto.
Si può osservare che system integrator e produttori mantengono costante la redditività (EBITDA/V) ma hanno rallentato la crescita.
I distributori, invece, presentano una crescita ancora in doppia cifra (crescita media delle PMI e Corporate = 14,5% rispetto al 2015) con una redditività stabile (EBITDA/V media delle PMI e Corporate = 6,3%) continuando così il processo di rafforzamento di crescita con presidio di buona marginalità.

RATING

Finora abbiamo analizzato i ricavi e la redditività (EBITDA/V). In questo paragrafo ci focalizziamo sull'altra dimensione su cui si misurano le prestazioni di una azienda e di un settore: il rating. Il rating rappresenta un indicatore di quanto un soggetto (o un settore) sia resistente alle sollecitazioni negative derivanti da avverse condizioni in cui si può trovare. Di conseguenza, sebbene non tutte le aziende con basso rating arrivino necessariamente all'insolvenza, sono quelle più esposte all'insolvenza in caso di rallentamento del ciclo economico, crisi di settore e crisi interne.
Il rating del settore della sicurezza si conferma ancora una volta eccellente, attestandosi mediamente intorno al KR5, un valore di un paio di scalini superiore alla media della manifattura italiana (KR3).
Nella scala di KF Economics che va da KR1, massimo rischio, a KR7, il KR5 corrisponde mediamente ad un rischio di fallimento pari allo 0,2%: ovvero mediamente due aziende su 1.000 in questa fascia falliscono entro i 12 mesi seguenti alla valutazione.
Il gruppo più solido quest'anno risulta quello dell'antincendio mentre nella scorsa rilevazione era quello dell'anti intrusione. Va comunque sottolineato che tutti i gruppi si collocano in zone di buona solidità.

TABELLA 2

Classe rating	Descrizione	Implicazioni per i Clienti	PD ‰
KR7	Azienda solvibile e finanziariamente solida in grado di resistere anche a gravi peggioramenti delle condizioni economiche / di mercato	Fornitore molto solido, massima capacità di approvvigionarsi di risorse finanziarie per operare e conseguente basso rischio di problemi di continuità di fornitura.	0,1
KR6			
	Azienda in grado di onorare regolarmente i debiti con buona capacità di copertura; potrebbe però deteriorarsi in caso di grave peggioramento delle condizioni economiche / mercato		0,6
KR5	Azienda in grado di onorare i debiti ma esposta al peggioramento delle condizioni economiche e di mercato.	Fornitore solido, alta capacità di approvvigionarsi di risorse finanziarie per operare. Limitati rischi sulla continuità operativa.	2,1
KR4	Azienda con solidità finanziaria modesta ma attualmente in grado di onorare i debiti	Fornitore con normale capacità di approvvigionarsi di risorse finanziarie. Rischi sull'operatività in caso di serie congiunture.	5,8
KR3	Azienda finanziariamente debole ed esposta al rischio di insolvenza	Fornitore con limitata capacità di approvvigionarsi di risorse. Rischioso nel caso in cui, per operare, abbia forti esigenze finanziarie.	13,7
KR2	Azienda a significativo rischio di insolvenza	Fornitore le cui difficoltà finanziarie (e quindi nel pagare i propri fornitori) rendono difficile garantire l'operatività: tempestività e qualità delle consegne.	30,5
KR1	Azienda a elevato rischio di insolvenza		74,7

Tabella 2. Le classi di rating di KF Economics. a&s Italy© - Tutti i diritti riservati

BOX 2

Tipologia	Media PFN/V 2015	Media PFN/V 2014	Media PFN/V 2013	Media PFN/V 2012	Media PFN/V 2011
Distributore	11%	8%	10%	9%	8%
Produttore / Distributore	4%	8%	3%	3%	20%
Produttore	7%	6%	8%	10%	9%
System Integrator	3%	-3%	7%	9%	6%
Totale	7%	5%	8%		

Box 2. Indebitamento finanziario medio del settore sicurezza. L'indebitamento è in aumento rispetto al 2014 ma comunque ampiamente all'interno di un range di sostenibilità. a&s Italy© - Tutti i diritti riservati

TABELLA 3

Settori	Media IVF%	Classe Rating Media
Tot produttori	56%	KR5
System integrator	40%	KR5
Distributore	30%	KR5
Anti intrusione	102%	KR6-
Sicurezza fisica	45%	KR5
Pro/distr	-2%	KR5
Antincendio	52%	KR5
TVCC	39%	KR5-
Varie	5%	KR5
Controllo accessi	-45%	KR4-
Totale complessivo	42%	KR5

Tabella 3. Distribuzione per Rating e Indice di valore finanziario (IVF%) (solo aziende PMI/Corporate). a&s Italy© - Tutti i diritti riservati

RATING E CAPACITÀ DI CREARE VALORE

Nelle sezioni precedenti abbiamo analizzato il settore su alcune dimensioni, in particolare la marginalità e il rischio finanziario.

La marginalità (EBITDA/V) è un interessante indicatore del valore generato da una azienda ma, per completarne la rappresentazione, si deve sottrarre il valore del debito finanziario.

La formula che in modo semplice esprime il valore finanziario generato da una azienda è pari a Valore Finanziario = EBITDA * M – PFN dove M è un moltiplicatore specifico di ogni azienda che racchiude al suo interno aspetti "strategici" quali: dimensione, tasso di crescita, marchi, brevetti, know-how. Per una prima analisi si possono però utilizzare moltiplicatori tipici della famiglia cui il soggetto appartiene (es. M=6 per una manifattura e M=8 per un distributore). Questi moltiplicatori tipici derivano dall'osservazione di centinaia di transazioni finanziarie di aziende paragonabili. Infatti questo Valore Finanziario è il punto di partenza economico di quasi tutte le negoziazioni per l'acquisizione di una azienda.

La PFN è invece l'indebitamento netto verso istituti finanziari che, come si vede nel **box 2**, sebbene in aumento rispetto al 2014, risulta comunque ampiamente all'interno di un range di sostenibilità.

Dividendo questo Valore Finanziario per il fatturato otteniamo un indice che permette di confrontare per valore generato aziende diverse, che noi chiamiamo IVF (Indice di valore finanziario).

Analizzando valore (sintetizzato da IVF) e Rating troviamo che il gruppo leader è quello dei produttori di sistemi di anti intrusione mentre il gruppo meno eccellente è quello del controllo accessi.

Dall'osservazione dell'evoluzione del posizionamento valore/rating (**figura 5**) si nota come il gruppo dei produttori/distributori abbia peggiorato progressivamente il posizionamento al contrario dei distributori che si trovano in miglioramento. Produttori e system integrator sono, invece, stabili.

FIGURA 4

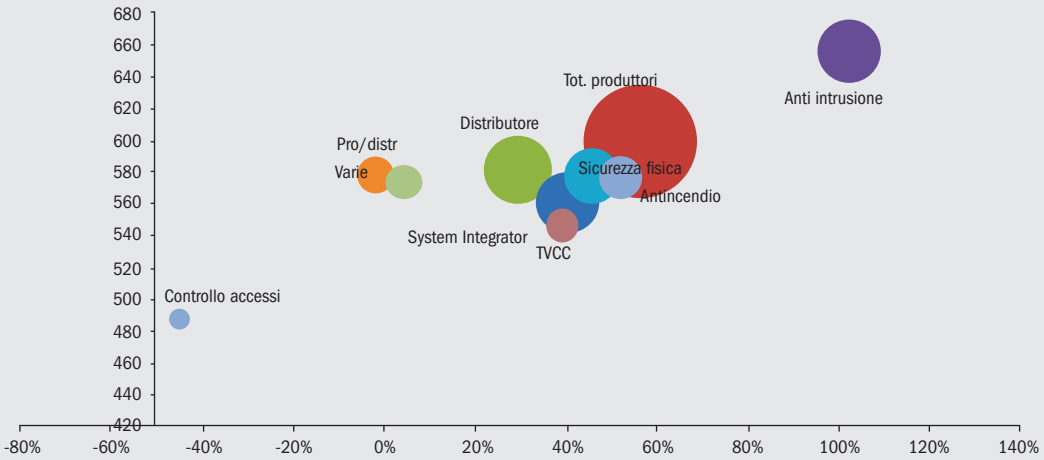


Figura 4. Distribuzione per Rating e Indice di valore finanziario (IFV%). il gruppo leader è quello dei produttori di sistemi di anti intrusione mente il gruppo meno eccellente è quello del controllo accessi. a&s Italy© - Tutti i diritti riservati

FIGURA 5

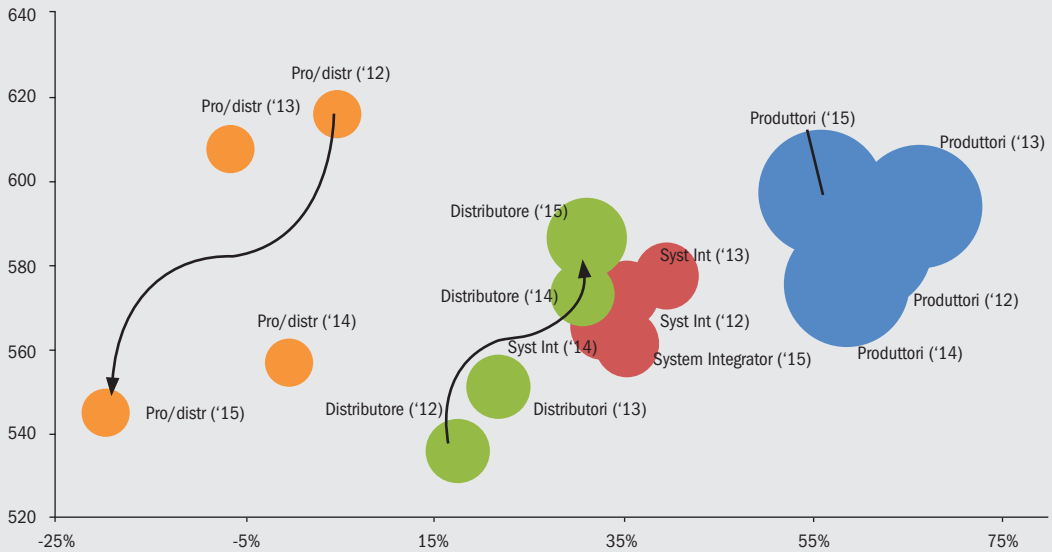


Figura 5. Distribuzione per Rating e Indice di valore finanziario (IFV%). Confronto storico (solo aziende PMI/Corporate). a&s Italy© - Tutti i diritti riservati

TABELLA 4

Classifica Produttori 2016 (bilanci 2015)	Classifica Produttori 2015 (bilanci 2014)	Ragione Sociale	Regione	Fatturato 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti	Settore
1	1	NOTIFIER ITALIA SRL	Lombardia	46.437	7%	7.637	16%	6.116	6.136	89	Antincendio
2	2	CIMA S.P.A.	Emilia-Romagna	36.175	15%	5.583	15%	5.304	5.332	99	Sicurezza fisica
3	3	TECNOALARM SRL	Piemonte	32.665	8%	8.701	27%	7.813	7.821	120	Anti intrusione
4	4	SAIMA SICUREZZA SPA	Toscana	31.834	16%	1.421	4%	1.039	1.053	128	Sicurezza fisica
5	5	BENTEL SECURITY SRL	Abruzzo	30.456	13%	5.832	19%	5.381	5.242	141	Anti intrusione
6	11	HIKVISION ITALY S.R.L.	Lombardia	26.169	90%	1.355	5%	589	552	27	TVCC
7	8	INIM ELECTRONICS SRL	Marche	22.825	16%	8.331	36%	7.613	7.622	76	Anti intrusione
8	6	SELESTA INGEGNERIA SPA	Liguria	20.879	-6%	4.533	22%	1.612	575	184	Sicurezza fisica
9	9	VIDEOTEC SPA	Veneto	20.545	8%	1.923	9%	1.440	1.851	104	TVCC
10	7	ATRAL ITALIA SRL	Emilia-Romagna	19.975	0%	638	3%	286	282	57	Anti intrusione
11	10	EL.MO. SPA	Veneto	18.408	7%	1.242	7%	959	788	67	Varie
12	13	BOSCH SECURITY SYSTEMS S.P.A.	Lombardia	13.647	13%	557	4%	537	572	17	Varie
13	12	COOPER CSA SRL	Lombardia	12.731	1%	731	6%	509	-4.616	24	Anti intrusione
14	17	CESPRO SRL	Toscana	12.643	14%	507	4%	389	451	65	Sicurezza fisica
15	15	ZUCCHETTI AXESS SPA	Lombardia	12.584	8%	1.571	12%	1.380	692	54	Controllo accessi
16	25	COMETA - S.P.A.	Toscana	11.702	38%	667	6%	487	469	39	Sicurezza fisica
17	21	TECHNOMAX SRL	Lombardia	11.424	19%	650	6%	614	495	35	Sicurezza fisica
18	23	ARGUS SECURITY SRL	Lombardia	11.142	23%	943	8%	473	264	69	Antincendio
19	27	MARCH NETWORKS SPA	Lombardia	11.121	33%	478	4%	401	898	50	TVCC
20	18	CIODUE S.P.A.	Lombardia	10.370	-6%	699	7%	550	539	44	Antincendio
21	20	AVS ELECTRONICS SPA	Veneto	10.272	0%	2.338	23%	2.140	2.156	48	Anti intrusione
22	22	CONFORTI S.P.A.	Veneto	9.351	3%	575	6%	230	-41	46	Sicurezza fisica
23	19	TECHCO SECURITY ITALIA S.R.L.	Lombardia	8.928	-15%	-2.714	-30%	-3.395	-3.984	68	Controllo accessi
24	40	BORDOGNA SPA	Lombardia	8.813	49%	1.292	15%	602	35	69	Sicurezza fisica
25	26	COMBIVOX SRL	Puglia	8.768	4%	2.704	31%	2.389	2.395	39	Anti intrusione
		Media TOP25 (produttori)		18.395	14%	2.328	11%	1.818	1.503	70	
		Media PMI e Corporate (produttori)		13.998	9%	1.685	10%	1.264	1.054	58	
		Media Totale (produttori)		5.237	9%	600	9%	434	365	23	

Tabella 4. Classifica TOP 25 dei **produttori** per fatturato 2015. a&s Italy© - Tutti i diritti riservati

I PRODUTTORI

La classifica per ricavi dei produttori vede al primo posto ancora una volta Notifier Italia SRL (46M€), nel settore antincendio, che continua il suo percorso di crescita (+7%). Al secondo posto si conferma CIMA SPA (36M€) e al terzo Tecnoalarm SRL (33M€). Anche le posizioni successive sono sostanzialmente stabili, ad eccezione di

TABELLA 5

Classifica Produttori 2016 (bilanci 2015)	Classifica Produttori 2015 (bilanci 2014)	Ragione Sociale	Regione	Fattura-to 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti
Antincendio										
1	1	NOTIFIER ITALIA SRL	Lombardia	46.437	7%	7.637	16%	6.116	6.136	89
18	23	ARGUS SECURITY SRL	Lombardia	11.142	23%	943	8%	473	264	69
20	18	CIODUE S.P.A.	Lombardia	10.370	-6%	699	7%	550	539	44
Sicurezza fisica										
2	2	CIMA S.P.A.	Emilia-Romagna	36.175	15%	5.583	15%	5.304	5.332	99
4	4	SAIMA SICUREZZA SPA	Toscana	31.834	16%	1.421	4%	1.039	1.053	128
8	6	SELESTA INGEGNERIA SPA	Liguria	20.879	-6%	4.533	22%	1.612	575	184
14	17	CESPRO SRL	Toscana	12.643	14%	507	4%	389	451	65
16	25	COMETA - S.P.A.	Toscana	11.702	38%	667	6%	487	469	39
17	21	TECHNOMAX SRL	Lombardia	11.424	19%	650	6%	614	495	35
22	22	CONFORTI S.P.A.	Veneto	9.351	3%	575	6%	230	-41	46
24	40	BORDOGNA SPA	Lombardia	8.813	49%	1.292	15%	602	35	69
Anti intrusione										
3	3	TECNOALARM SRL	Piemonte	32.665	8%	8.701	27%	7.813	7.821	120
5	5	BENTEL SECURITY SRL	Abruzzo	30.456	13%	5.832	19%	5.381	5.242	141
7	8	INIM ELECTRONICS SRL	Marche	22.825	16%	8.331	36%	7.613	7.622	76
10	7	ATRAL ITALIA SRL	Emilia-Romagna	19.975	0%	638	3%	286	282	57
13	12	COOPER CSA SRL	Lombardia	12.731	1%	731	6%	509	-4.616	24
21	20	AVS ELECTRONICS SPA	Veneto	10.272	0%	2.338	23%	2.140	2.156	48
25	26	COMBIVOX SRL	Puglia	8.768	4%	2.704	31%	2.389	2.395	39
TVCC										
6	11	HIKVISION ITALY S.R.L.	Lombardia	26.169	90%	1.355	5%	589	552	27
9	9	VIDEOTEC SPA	Veneto	20.545	8%	1.923	9%	1.440	1.851	104
19	27	MARCH NETWORKS SPA	Lombardia	11.121	33%	478	4%	401	898	50
Varie										
11	10	EL.MO. SPA	Veneto	18.408	7%	1.242	7%	959	788	67
12	13	BOSCH SECURITY SYSTEMS S.P.A.	Lombardia	13.647	13%	557	4%	537	572	17
Controllo accessi										
15	15	ZUCCHETTI AXESS SPA	Lombardia	12.584	8%	1.571	12%	1.380	692	54
23	19	TECHCO SECURITY ITALIA S.R.L.	Lombardia	8.928	-15%	-2.714	-30%	-3.395	-3.984	68
		Media TOP25 (produttori)		18.395	14%	2.328	11%	1.818	1.503	70
		Media PMI e Corporate (produttori)		13.998	9%	1.685	10%	1.264	1.054	58
		Media Totale (produttori)		5.237	9%	600	9%	434	365	23

Tabella 5. TOP 25 **produttori** suddivisi per tecnologia. a&s Italy© - Tutti i diritti riservati

TABELLA 6

Classifica Produttori Cavi 2016 (bilanci 2015)	Classifica Produttori Cavi 2015 (bilanci 2014)	Ragione Sociale	Regione	Fatturato 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti
1	1	RAMCRO SPA	Lombardia	24.484,431	7%	1.702,941	7%	1.170,493	640,007	56
2	2	CEAM CAVI SPECIALI S.P.A.	Veneto	21.908,948	12%	3.386,981	15%	2.475,505	2.413,515	94
3	3	CAVICEL S.P.A.	Lombardia	17.477,178	-4%	1.584,657	9%	627,225	551,256	68
4	4	PROSPECTA CAVI SPECIALI SRL	Emilia-Romagna	9.393,189	4%	487,453	5%	249,623	82,498	31
5	5	BATA CAVI SRL	Campania	7.731,14	9%	799,082	10%	420,302	257,564	31
6	7	MICRO TEK S.R.L.	Lombardia	5.840,159	15%	368,874	6%	330,437	301,696	9
7	8	LUCEAT SRL	Lombardia	321,475	-33%	-183,271	-57%	-201,057	-197,996	9
n.d.	6	ELAN SRL	Marche	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.	n.d.

Tabella 6. Principali **produttori di cavi** che si occupano anche di sicurezza. a&s Italy© - Tutti i diritti riservati

Hikvision Italy SRL, settore della TVCC, che sale dalla posizione 11 alla 6 con una crescita del 90%.
Dalla ripartizione della TOP25 dei produttori per settore si nota come ancora una volta non vi sia un settore dominante: il primo della classifica si occupa di antincendio, il secondo di sicurezza fisica ed il terzo di anti intrusione.

I PRODUTTORI DI CAVI

Dal momento che servono normalmente differenti comparti (dalla telefonia al settore elettrico e al broadcasting) e non trovano nella sicurezza il mercato principale di riferimento, nel nostro studio le aziende che producono cavi sono sempre state tenute separate dai produttori.

Anche quest'anno Ramcro si conferma al primo posto per fatturato dei produttori di cavi.

DISTRIBUTORI

Nella classifica dei TOP25 distributori troviamo quasi solamente soggetti che erano presenti nella classifica scorsa: questo testimonia una forte stabilità dei leader del comparto distributori.
Al vertice della classifica si conferma la HESA SPA (40M€) che continua la crescita, +12%. La redditività media (EBITDA/V) dei TOP25 (6%) è di poco superiore a quella media dei distributori (5,1%) e comunque, secondo l'esperienza KF Economics, in una zona di buone prestazioni per un distributore.

TABELLA 7

Classifica Distributori 2016 (bilanci 2015)	Classifica Distributori 2015 (bilanci 2014)	Ragione Sociale	Regione	Fatturato 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti
1	1	HESA SPA	Lombardia	39.531	12%	1.752	4%	930	987	66
2	4	AIKOM TECHNOLOGY S.R.L.	Emilia-Romagna	25.581	64%	1.000	4%	907	1.133	15
3	3	DISTRIBUZIONE APPARECCHIATURE SICUREZZA DIAS SRL	Lombardia	19.947	20%	1.402	7%	1.042	1.060	6
4	2	ELECTRONIC'S TIME S.R.L.	Puglia	17.374	-1%	1.288	7%	1.035	492	44
5	5	SICURTEC SRL	Lombardia	14.984	3%	22	0%	-144	247	51
6	n.d.	SICE TELECOMUNICAZIONI	Toscana	14.617	42%	339	2%	277	358	n.d.
7	6	QUBIX S.P.A.	Veneto	12.294	8%	2.441	20%	2.346	2.132	13
8	7	S. & A. SRL	Lombardia	12.169	10%	698	6%	618	596	30
9	8	TRANS AUDIO VIDEO	Campania	11.877	33%	568	5%	533	515	19
10	10	DOPPLER SRL	Piemonte	9.747	15%	478	5%	347	349	31
11	11	SICURTEC BRESCIA SRL	Lombardia	8.792	6%	495	6%	352	90	22
12	9	LASERLINE SAFETY AND SECURITY SYSTEMS SRL	Lombardia	8.219	-7%	632	8%	357	286	23
13	20	MICROCONTROL ELECTRONIC S.R.L.	Lombardia	7.818	61%	463	6%	391	346	15
14	n.d.	GIUDICI & POLIDORI	Marche	7.539	26%	617	8%	591	582	15
15	17	TELEVISTA S.R.L.	Veneto	7.136	24%	134	2%	113	72	18
16	13	DODIC ELETTRONICA S.R.L.	Lazio	7.006	7%	239	3%	162	164	16
17	12	ITS ITALELETTRONICA S.R.L.	Abruzzo	6.640	1%	287	4%	198	134	25
18	n.d.	D.S.T. DISTRIBUZIONE SISTEMI TECNOLOGICI S.R.L., IN BREVE D.S.T. S.R.L.	Lazio	6.598	27%	340	5%	299	262	21
19	19	TROLESE S.R.L.	Veneto	6.328	30%	152	2%	110	81	18
20	14	SERTEC SRL	Veneto	6.274	-3%	1.184	19%	1.060	1.089	11
21	15	ASCANI ELETTROCOMM S.R.L.	Marche	6.061	2%	275	5%	254	47	21
22	16	TOP ITALIA S.R.L.	Sicilia	5.796	-1%	374	6%	271	167	7
23	18	CHECKPOINT SOCIETA A RESPONSABILITA LIMITATA	Lazio	4.958	-1%	146	3%	128	54	16
24	22	ABES S.R.L.	Piemonte	4.881	6%	103	2%	83	38	14
25	23	FPM S.R.L.	Veneto	4.675	5%	169	4%	86	40	9
		Media TOP25 (Distributori)		11.074	16%	624	6%	494	453	22
		Media PMI e Corporate (distributori)		11.924	17%	690	6,1%	548	509	23
		Media Totale (distributori)		4.848	14%	275	5,1%	217	192	11

Tabella 7. TOP 25 **distributori** per fatturato. Il primo classificato HESA SPA si conferma come anche la quasi totalità dei TOP25. Solo tre nuovi ingressi. a&s Italy© - Tutti i diritti riservati

TABELLA 8

Classifica Pro/Distr 2016 (bilanci 2015)	Classifica Pro/Distr 2015 (bilanci 2014)	Ragione Sociale	Regione	Fatturato 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti	Settore
1	3	GUNNEBO ITALIA SPA	Lombardia	18.843	9%	247	1%	157	141	79	Sicurezza fisica
2	2	HONEYWELL SECURITY ITALIA SPA	Lombardia	17.092	-11%	-2.391	-14%	-2.908	-2.976	39	Varie
3	5	VIDEOTREND S.R.L.	Lombardia	14.109	29%	820	6%	735	607	40	TVCC
4	4	SICURIT ALARMITALIA SPA	Lombardia	12.808	3%	44	0%	-5	155	45	Varie
5	6	BETTINI SRL	Lombardia	7.779	7%	256	3%	138	110	42	TVCC
6	7	SAET I.S. - S.R.L.	Piemonte	5.154	9%	671	13%	486	628	15	Anti intrusione
7	8	GSG INTERNATIONAL SRL	Lombardia	3.076	-5%	218	7%	164	22	11	TVCC
8	11	SAET SERVICE S.R.L.	Piemonte	2.691	35%	299	11%	270	263	12	Anti intrusione
9	10	TECNOPOST SPA	Lombardia	2.551	7%	295	12%	192	232	22	Sicurezza fisica
10	9	MESA SRL	Toscana	2.550	-7%	55	2%	-284	-411	11	Varie
11	12	SIQR SRL	Lombardia	816	-9%	26	3%	19	13	1	TVCC
		Media TOP25 (prod / dist)		7.952	6%	49	4%	-94	-111	29	
		Media PMI e Corporate (prod / distr)		12.631	8%	-59	2%	-233	-222	43	

Tabella 8. TOP **produttori/distributori**. Anche nel 2015 questi operatori "assomigliano" per marginalità più ai distributori che ai produttori.

PRODUTTORI/DISTRIBUTORI

I produttori/distributori sono soggetti che producono alcune componenti e integrano la loro offerta svolgendo il ruolo di distributori di altri produttori.

Il primo classificato è la GUNNEBO Italia SPA (18M€) che ha mostrato una crescita del 9% e passa dal terzo al primo posto.

Al secondo posto si conferma la Honeywell security Italia (17M€), seguita dalla Videotrend SRL (14M€).

TABELLA 9

Classifica System Integrator 2016 (bilanci 2015)	Classifica System Integrators 2015	Ragione Sociale	Regione	Fatturato 2015	Crescita Fatturato '15 su '14	EBITDA	EBITDA/V	EBIT	EBT	Numero dipendenti
1	1	PROJECT AUTOMATION SPA	Lombardia	43.044	11%	2.653	6%	1.770	1.904	206
2	2	DAB SISTEMI INTEGRATI SRL	Lazio	15.975	-4%	854	5%	656	390	70
3	3	SISTEMI INTEGRATI SRL	Emilia-Romagna	14.798	1%	2.699	18%	1.731	1.724	14
4	9	CONSORZIO NAZIONALE SICUREZZA SCARL	Campania	10.263	18%	792	8%	665	608	9
5	10	S.C.A.M.E. SISTEMI S.R.L.	Lombardia	9.114	14%	1.848	20%	1.578	1.504	22
6	4	DATA GENERAL SECURITY S.R.L.	Lazio	8.820	-31%	-172	-2%	-236	-202	9
7	8	TELETRONICA SPA	Friuli-Venezia Giulia	8.549	-2%	40	0%	-232	-229	44
8	n.d.	ADVANTEC S.R.L	Piemonte	8.318	8%	35	0%	15	40	15
9	12	VAGO SPA	Lombardia	7.386	0%	1.070	14%	637	648	40
10	13	C.I.S.A.- COSTRUZIONI IMPIANTI SPECIALI ANTIFURTO SRL	Lombardia	7.231	2%	341	5%	299	334	29
11	17	SAIET TELECOMUNICAZIONI SPA	Emilia-Romagna	7.141	12%	175	2%	122	51	10
12	14	SECURITY TRUST.IT SRL	Lombardia	7.086	7%	865	12%	663	264	32
13	15	TELEIMPIANTI SPA	Emilia-Romagna	6.713	2%	460	7%	392	401	39
14	19	TELEFONIA E SICUREZZA SPA	Lombardia	6.138	10%	275	4%	201	186	44
15	18	CONSORZIO GOSS ITALIA	Veneto	5.983	-4%	13	0%	12	17	1
16	11	CONSIAG S.P.A.	Toscana	5.659	-27%	3.601	64%	27	276	1
17	22	F.G.S. BRESCIA SRL	Lombardia	5.042	5%	219	4%	132	73	36
18	23	UMBRA CONTROL S.R.L.	Umbria	4.880	2%	107	2%	59	21	35
19	21	SPEE SRL	Abruzzo	4.763	-4%	642	13%	154	101	37
20	32	COGEN SPA	Lombardia	4.397	28%	258	6%	193	81	38
21	29	DAGO ELETTRONICA SRL	Marche	4.394	18%	200	5%	82	59	41
22	26	CENTRUM SRL	Emilia-Romagna	4.309	1%	141	3%	122	113	21
23	24	TONALI - S.P.A.	Lombardia	4.209	-10%	120	3%	-5	50	15
24	16	TSI SYSTEM SPA	Lombardia	4.080	-37%	-626	-15%	-754	-852	32
25	33	METROVOX SRL	Lazio	3.853	14%	164	4%	-23	46	14
		Media TOP25 (system integrator)		8.486	1%	671	8%	330	304	34
		Media PMI e Corporate (system integrator)		10.427	1%	928	10%	496	470	37
		Media Totale (system integrator)		3.378	3%	243,13	4,7%	122,91	108,40	17,68

Tabella 9. TOP 25 **System Integrator**. Primi posti della classifica dei system integrator invariati rispetto alla scorsa edizione; i TOP crescono meno del campione complessivo.

SYSTEM INTEGRATOR

Le prime tre classificate sono invariate da due edizioni della classifica e sono la Project Automation SPA (43M€) in crescita dell'11%, DAB Sistemi Integrati (15M€) e Sistemi Integrati SRL (15M€).

Complessivamente i system integrator sono stabili (+3% di crescita dal 2014). Della TOP25, i soggetti con i fatturati maggiori (PMI e Corporate) hanno una migliore redditività (10% contro 8% della TOP25) denotando che in questo particolare segmento l'effetto scala è importante per presidiare la marginalità.

TABELLA 10

	NordOvest		NordEst		Centro		Sud		Totale Italia	
Tipologia	Num.	Ricavi	Num.	Ricavi	Num.	Ricavi	Num.	Ricavi	Num.	Ricavi
Produttore	75	376.666	39	181.353	21	133.969	9	62.084	144	754.073
Distributore	30	159.743	22	95.024	13	59.282	12	59.255	77	373.305
System Integrator	37	141.525	25	77.174	21	61.755	8	26.927	91	307.380
Pro/distr	10	84.921			1	2.550			11	87.470
Totale complessivo	**152**	**762.855**	**86**	**353.552**	**56**	**257.556**	**29**	**148.266**	**323**	**1.522.228**

Tabella 10. Distribuzione delle tipologie di operatore per geografia. a&s Italy© - Tutti i diritti riservati

TABELLA 11

Geografia	Media EBITDA/V	Media Crescita Ricavi
Centro	3%	9%
NordEst	10%	9%
NordOvest	12%	7%
Sud	11%	11%
Importo totale	9%	8%

Tabella 11. Distribuzione per geografica dell'EBITDA/V e della crescita dei ricavi. Corporate e PMI.
a&s Italy© - Tutti i diritti riservati

GLOSSARIO

EBT (*Earnings before taxes*): è il reddito che l'azienda è in grado di generare prima delle imposte e al netto degli oneri finanziari.
EBIT (*Earnings before interest and taxes*): è il reddito operativo aziendale, ovvero il reddito che l'azienda è in grado di generare prima delle imposte e degli oneri finanziari.
EBITDA (*Earnings before interest, taxes, depreciation and amortization*): rappresenta l'utile al lordo di interessi passivi, imposte e ammortamenti su beni materiali e immateriali; è un fondamentale indicatore di redditività.
EBITDA/V: noto anche come **margine EBITDA**, è il rapporto fra EBITDA e vendite, ed esprime la redditività lorda delle vendite; questo parametro aiuta a capire meglio l'incidenza dei costi nel tempo. Più questo valore è elevato, più l'azienda è efficiente e performante.

DISTRIBUZIONE GEOGRAFICA

Sul fronte strettamente geografico, il campione rimane fortemente concentrato - sia come numerosità, sia come fatturato - sul nord ovest, che assomma circa il 50% delle imprese analizzate.
Il sud, sebbene poco rappresentato rispetto al nord e al centro, mantiene un buon tasso di crescita (11%) e la migliore marginalità media (11% di EBITDA/V).

DISCLAIMER

Cinque anni di analisi di un settore che continua a tenere, a dispetto della situazione economica globale. Ma come? E soprattutto perché? L'abbiamo chiesto a Giuseppe R. Grasso, Presidente di KF Economics (società di ricerca e consulenza controllata da K Finance, focalizzata sulla produzione di modelli di rating e di modelli econometrici per analisi finanziarie)

Siamo ormai arrivati alla quinta edizione del nostro rapporto sul settore Sicurezza redatto in collaborazione con la vostra realtà: è quindi tempo di fare bilanci...

Sul piano generale, nel 2012 ci si aspettava di uscire dalla crisi iniziata nel 2008 mentre, di anno in anno, ci siamo accorti che non si trattava di una crisi, ma di un cambiamento strutturale. In questi cinque anni sono fallite circa 70.000 aziende e molte di quelle che sopravvivono lo fanno con marginalità e volumi drasticamente ridotti rispetto ai primi anni 2000. Tutto vero. Poi ogni anno guardiamo i dati del comparto sicurezza e troviamo un mondo completamente diverso. Un settore in cui il margine (EBITDA/V) medio (10,1% per i produttori e 6,3% per i distributori) raggiunge valori che in altri comparti sono propri solo delle aziende eccellenti.

All'interno di questo "microcosmo d'eccellenza", vi sono segmenti più dinamici?

All'interno di questo mondo eccellente, vi sono settori che stanno continuando un processo di rapida crescita, quali la TVCC, che ha mostrato una crescita dei ricavi 2015 rispetto al 2014 in doppia cifra, mantenendo comunque una accettabile marginalità (5,2% di EBITDA/V).
Un aspetto molto peculiare risiede nel fatto che, sebbene stiamo parlando di aziende di media dimensione (nessuna nel campione supera i 50M€ di fatturato), al vertice delle diverse classifiche troviamo quasi sempre gli stessi attori, il che significa che il vantaggio competitivo acquisito negli anni passati consente di mantenere una posizione rilevante nelle classifiche.

Dinamismo, dunque, ma sostanziale stabilità e consolidamento delle posizioni più forti. Ha per caso a che fare con la solidità finanziaria del comparto?

La solidità del settore, che noi misuriamo con il nostro KF Rating, si trova intorno al livello KR5 (in una scala che va dai meno solidi KR1, agli eccellenti KR7): si tratta di un rating decisamente sopra la media italiana, che si posiziona intorno al KR3. Questo dimostra che il comparto Sicurezza non solo continua a crescere mantenendo una buona marginalità, ma lo fa anche presidiando la solidità. E questo non è per niente scontato. Infatti spesso grosse crescite e alti margini vengono ottenuti a scapito della solidità finanziaria, dando origine a bolle che poi portano alle crisi di settore.

Le nostre aziende sono quindi in grado di generare valore?

Se guardiamo il campione dal punto di vista di un investitore, notiamo come il valore delle aziende rappresentato da nostro IFV% (indice di valore finanziario pari al EBITDA X Multiplo – Debito finanziario diviso il fatturato), che in percentuale sul fatturato rappresenta il valore da cui normalmente inizia qualunque negoziazione per acquisizione di aziende, ci parla di aziende che hanno saputo accrescere il proprio valore e portarlo a livelli di assoluta eccellenza.
Si pensi ai produttori che mediamente hanno un IFV% superiore al 50%, quando mediamente valori elevati sono quelli superiori al 30%.

www.kfinance.org

CrismaSecurity

ASIS EUROPE 2017

FROM RISK TO RESILIENCE MILAN, ITALY 29–31 MARCH 2017

MiCo Nord - Livello +1 - Stand C14

...vieni a trovarci!

Crisma Security è un System Integrator focalizzato sulla sicurezza fisica e logica.

Nel settore della sicurezza fisica è specializzata nella progettazione e realizzazione di sistemi di videosorveglianza, protezione perimetrale, sistemi di controllo accessi e sistemi di localizzazione in tempo reale.

Inoltre è specilizzata nella physical and cyber securty analytics.

NAVTECH RADAR · THERMAL RADAR · LOGIPIX · sightlogix

Certificazione UNI EN ISO 9001:2008

Per garantire ai nostri clienti i più elevati standard di qualità, Crisma Security risponde ai requisiti di qualità richiesti dalla norma UNI EN ISO 9001:2008. La certificazione ha portato alla elaborazione di procedure e istruzioni operative che regolano i processi e, parallelamente, alla informatizzazione della modulistica e documentazione a supporto del sistema di gestione per la qualità.

Crisma Security s.r.l.
Via Rhodesia, 2 - 00144 Roma
Tel: +39 06 94365650
Fax: +39 06 45426345
www.crismasecurity.it
sales@crismasecurity.it

HUAWEI ENTERPRISE ICT SOLUTION **A BETTER WAY**

TELECAMERA BULLET IP

con **Analisi Video Intelligente** e **LED** IR **invisibili**

Telecamera Bullet IP **2MP** (1920x1080) a colori Day & Night
Sensore CMOS Sony EXMOR R da 1/2.8"
Obiettivo varifocale motorizzato 2.8-12mm autofocus
Filtro IR meccanico | **H.265/HEVC** e **H.264** Multistream
Alimentazione **DC12V/DC24V/AC24V/PoE**
2ch allarme In/Out | 1ch audio In/Out
Uscita video CVBS | RS485 | **Ultra WDR 120dB**
Funzione Defog | **Auto Back Focus** (ABF) | IR 30m | **IR invisibili** | IP66 | **IK10**
Slot microsd max 64GB | **Funzioni analisi video intelligente**
Speciale verniciatura antigoccia (Huawei coating glass)
Temperatura -40°C / +60°C

HUAWEI
CCTV Solution

DEATRONIC

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

Ne parliamo con Franco Dischi e Raffaele de Astis

Assosicurezza: due Presidenti a confronto

Un Past President che ha fatto la storia del comparto sicurezza ed un nuovo Presidente cui spetta raccogliere complesse sfide evolutive sul fronte sia tecnologico, sia economico. Due visioni e due generazioni a confronto per un'intervista doppia in esclusiva.

“Gli interessi particolari possono convergere” intervista a FRANCO DISCHI, Presidente di Assosicurezza dal 2001 al 2016 e futuro Segretario Generale.

FRANCO DISCHI, Presidente di Assosicurezza dal 2001 al 2016 e futuro Segretario Generale

Com’è nata Assosicurezza e con quali obiettivi? Quali sono stati, a suo avviso, i principali traguardi raggiunti dall’Associazione e cosa resta da fare?

Circa 15 anni fa, al mio debutto alla Presidenza di Assosicurezza, il comparto era in pieno sviluppo e il mercato in estremo fermento: molte imprese guidate dai fondatori desideravano imporsi anche a livello europeo, incontrando peraltro le medesime difficoltà di oggi. Era quindi fondamentale fare massa critica, ma le Associazioni di categoria erano frammentate e non riuscivano a coagularsi sotto un’egida comune. Si è riusciti sì ad unire installatori e integratori, ma gli interessi di costruttori e distributori erano distinti e contrapposti, quindi nel 1995 si decise di dar vita ad una nuova realtà: Assosicurezza. L’accoglienza d’impatto non fu delle migliori: le istituzioni e la politica non ci prendevano in seria considerazione. Non potendo contare su nessun appoggio, l’Associazione è quindi stata impostata come un’azienda: l’attività era totalmente basata sul volontariato, doveva generare dei ricavi per autosostenersi e non erano previsti rimborsi: questo generò una forte motivazione interna. Gli obiettivi dell’Associazione erano dare un segnale al mercato in termini di qualità dei prodotti, coerenza nella conduzione degli affari e integrità assoluta nei confronti dei clienti, oltre ad uno sviluppo dell’attività associativa con un orizzonte almeno europeo.
Il periodo pionieristico partorì comunque varie novità positive, come l’istituzione dei vigili di quartiere su impulso dell’allora assessore alla sicurezza di Milano Paolo Del Debbio (ora anchorman televisivo), l’istituzione ben 14 anni fa di un corso di laurea breve (in seguito diventata anche magistrale) presso l’università di Bologna dedicato, tra l’altro, alle tecnologie di sicurezza e che annoverava professori a contratto e tecnici tra le fila dei soci di Assosicurezza. Le lezioni si svolgevano in un laboratorio che rappresentava le migliori tecnologie, donato dall’Associazione grazie una convenzione che continua tuttora a generare opportunità di occupazione. Assosicurezza ha peraltro dotato di laboratori anche alcune scuole professionali i cui docenti, da noi formati, erano ufficiali dei Vigili del Fuoco. Un’altra importante collaborazione si è stretta con i carabinieri del Nucleo Tutela Patrimonio Culturale, che hanno prestato aiuto alle Diocesi nella catalogazione delle opere d’arte ecclesiastiche. Alcune diocesi hanno addirittura stipulato convenzioni con Assosicurezza per garantire ai Sacerdoti la possibilità di installare sistemi di sicurezza certificati dagli enti normativi a prezzi vantaggiosi. Particolarmente sensibile al problema dei vandalismi nelle Chiese, Assosicurezza ha peraltro più volte protetto i luoghi di culto a titolo gratuito: da S. Cristoforo sul Naviglio alla basilica di S. Ambrogio, con la consegna delle chiavi del sistema di sicurezza nelle mani dell’Arcivescovo di Milano a Natale. Pro futuro...ritengo che la prima sfida sia quella di collaborare con le altre Associazioni in principio su iniziative comuni, per poi giungere a comprendere e far comprendere che gli interessi particolari si possono regolamentare pur convergendo magari sotto un’unica federazione.

Dal suo osservatorio, come si è modificato il mercato in questi anni ed a quali sfide è chiamato a rispondere?

Come tutti, anche il nostro settore ha vissuto sconvolgimenti e trasformazioni epocali.

Il primo problema, ancora attuale, è la gestione della successione tra i fondatori originari delle imprese, che non possono eternamente stare al passo con le innovazioni, e le nuove leve – che possono essere parenti o manager (e qui può sorgere il problema). Il panorama degli addetti ai lavori è infatti completamente cambiato: il security manager è passato in pochissimi anni dall'essere un esperto di tecnologie e procedure mutuate da un'esperienza sotto le forze armate ad essere un fine conoscitore di sicurezza informatica, finanza e bilanci. Se prima al security manager veniva infatti assegnato un capitolo di spesa per assicurare l'azienda, oggi ad un budget da spendere per la sicurezza corrisponde un obbligo di "saving" pari o addirittura superiore da realizzare. Sul versante delle aziende manifatturiere, la crisi ha dimostrato quali erano in grado di reggere il mercato e quali no. Spesso le nostre aziende sono state sottocapitalizzate: in caso di congiuntura sfavorevole diventavano sempre più marginali, fino a scomparire. L'azienda italiana che vuole prosperare deve necessariamente spostare il focus dal prodotto al cliente e puntare sulla qualità ritagliandosi qualche prodotto/sistema che possa essere considerato un'eccellenza. Ovviamente per puntare al cliente occorre attrezzarsi con lo stock coinvolgendo in modo stretto i fornitori e garantendo un eccellente supporto al cliente.

Se dovesse sintetizzare in uno slogan i suoi anni da Presidente, quali parole userebbe?

Entusiasmo e gratificazione. Entusiasmanti e gratificanti sono infatti stati i miei anni da Presidente perché ho sempre inseguito, com'è mia natura, una crescita che passa attraverso lo sviluppo delle attività dei soci e quindi dell'Associazione, tenendo però presente che il lavoro doveva generare indipendenza economica per perseguire gli scopi sociali.

> "GLI INTERESSI PARTICOLARI POSSONO CONVERGERE"

RAFFAELE DE ASTIS, nuovo Presidente di Assosicurezza

> "*mpariamo dal passato guardando avanti"* **intervista a RAFFAELE DE ASTIS, nuovo Presidente di Assosicurezza.**

Quali sono gli obiettivi del suo mandato per il prossimo triennio? La sua politica associativa si muoverà sul solco della continuità o ci sono novità in cantiere?

L'obiettivo principale come Associazione è quello di rinnovarci pur tenendo fermi i nostri valori. Cambiare sì, ma senza dimenticare chi siamo e da dove veniamo. Dobbiamo inoltre continuare a coinvolgere sempre più aziende del settore e cercare di essere sempre più vicini alle imprese e al mercato. Dobbiamo infine continuare a fornire servizi e rappresentanza a tutti gli associati e ricercare sinergie ed alleanze con altre Associazioni del settore, come pure di altri mercati verticali.
In questi anni il mondo è cambiato radicalmente: le aziende hanno dovuto mettersi in discussione e adattarsi con tempismo e grande capacità di decisione. Molte hanno saputo cogliere le opportunità derivanti dai forti cambiamenti sia esterni che interni al nostro piccolo e ancora giovane settore.

Come Associazione dobbiamo essere altrettanto dinamici. Le alleanze che in questi ultimi anni sono state strette tra aziende anche in parte concorrenti sono state il risultato di un necessario sforzo adattivo. Queste dinamiche hanno fatto cambiare punto di vista a diversi operatori, che anche dopo gli "scossoni" hanno continuato a credere che sia utile "fare" insieme ad altri.
L'Associazione è al servizio delle aziende, ma è anche fatta dalle aziende, che con la loro partecipazione e le loro idee possono fare ingranare quella marcia in più che oggi è più che mai fondamentale. Con una storia realmente pionieristica alle spalle come quella che può vantare Assosicurezza, sarebbe folle non muoversi nel solco della continuità, ma sarebbe altrettanto folle non guardare avanti e cercare nuove idee.

Quali sono, a suo avviso, i traguardi più complessi da raggiungere, sia sul fronte normativo, sia sul fronte del mercato? E come intende muoversi in queste direzioni?

L'armonizzazione delle norme europee è in alcuni ambiti quasi una chimera, più che un traguardo complesso. Dobbiamo continuare ad inviare i nostri esperti ai tavoli di lavoro dove si decidono le norme e la loro applicabilità. Come Associazione dobbiamo continuare ad informare i nostri associati e a proporre formazione a tutti i livelli, in particolare riguardo le norme di settore e quelle generali. Un esempio su tutti è il nuovo regolamento Europeo sulla Privacy, ancora poco conosciuto e sul quale è importante approfondire.
Sul fronte del mercato, l'internazionalizzazione è ancora per molte aziende un traguardo da raggiungere. Possiamo e dobbiamo invece diventare protagonisti, sia con aziende produttrici che esportano all'estero, sia con aziende di distribuzione che importano soluzioni e tecnologie. In un mondo globalizzato è però importante conoscere i mercati internazionali e attrezzarsi per tempo: informazioni, knowhow e preparazione possono davvero fare la differenza. Per l'internazionalizzazione Assosicurezza deve quindi continuare a cercare soluzioni creative come quelle che negli scorsi anni ci hanno contraddistinto - una su tutte il progetto Italian Security in USA. Dobbiamo inoltre agevolare con gli strumenti associativi a nostra disposizione tutte quelle aziende produttrici e di distribuzione che intendono attrezzarsi per affrontare o cominciare ad esplorare tutto ciò che succede oltre confine. Anche chi già opera all'estero può trovare utile quanto può essere messo a disposizione dall'Associazione per efficientare la propria attività o ampliare gli orizzonti.

Dal suo osservatorio, come si è modificato il mercato in questi anni ed a quali sfide è chiamato a rispondere?

Il mercato in questi anni è diventato sempre più competitivo: un'arena affollata, un mare con tanti pesci e tanti predatori. Il nostro è un settore che, rispetto ad altri, presenta però delle potenzialità specifiche e può ancora riservare spazi di crescita sia per le aziende già presenti sul mercato, sia per i nuovi attori che stanno entrando. Del resto il comparto sicurezza è sempre più compenetrato al mondo IT: le sfida tecnologiche, trasversali a tutti gli attori del mercato, non possono prescindere da questo fattore. Le minacce esterne sono sempre più sofisticate e le soluzioni tecnologiche da adottare devono essere dunque al passo con la velocità di chi ci "attacca".
Più in generale, le aziende sono chiamate a rispondere alla sfida del "tempo", della "qualità" e del giusto posizionamento.

Se dovesse sintetizzare in uno slogan il suo triennio da Presidente, quali parole userebbe?

Impariamo dal passato guardando avanti.

> "IMPARIAMO DAL PASSATO GUARDANDO AVANTI"

I migliori auguri di buon lavoro dalla Redazione di a&s Italy

ComNet è la soluzione per tutte le tue esigenze di comunicazione

GUARANTEED PERFORMANCE

TODAY - AND TOMORROW

Quando l'***affidabilità è fondamentale,*** i ***prodotti di trasmissione che scegli oggi*** influenzeranno le ***prestazioni della tua rete di comunicazione domani!***

ComNet - Soluzioni di Comunicazione a Lungo Termine

Fibra Ottica Rame Video Dati Audio Wireless Ethernet

- Solo ComNet è in grado di offrirvi una soluzione globale per la trasmissione su Rame, Fibra e Wireless
- I prodotti ComNet sono MADE IN THE USA
- Esclusiva Garanzia LIFETIME WARRANTY ∞
- Tecnici specializzati di provata esperienza possono supportare ogni vostra esigenza

www.comnet.net

comnet
Communication Networks

mgrasselli@comnet.net
+39 345 0855551

Vieni a trovarci per scoprire come ComNet può aiutarti

SICUREZZA 2017 | Fiera Milano Rho
15-17 Novembre | Stand H28

WWW.COMNET.NET MADE IN THE USA **LIFETIME WARRANTY** ∞

EEA
ELECTRONIC
EQUIPMENTS
ANTINTRUSION

Velvet DT evolution

FACTORY

AM BEDBUG

ANTIMASCHERAMENTO BEDBUG
Antimascheramento con filtro per piccoli insetti (cimici).

MADE IN ITALY

Ilaria Garaffoni

Bonus sicurezza: modalità di richiesta

Vi ricordate i 15 milioni di euro stanziati come credito d'imposta per le spese destinate alla sicurezza dei privati nel 2016? Bene, il 6/12/2016 è stato pubblicato in GU il decreto attuativo del Ministero dell'Economia e delle Finanze che definisce criteri e procedure di accesso al bonus. Il decreto conferma che l'agevolazione spetta solo alle persone fisiche – non nell'esercizio di attività di lavoro autonomo o di impresa, quindi esclusi artigiani e commercianti – per le spese sostenute nel 2016 per l'installazione di sistemi di videosorveglianza e d'allarme e per la stipula di contratti con istituti di vigilanza privata. Le spese possono afferire alle abitazioni private; se l'immobile è adibito ad uso sia personale che lavorativo, il credito d'imposta scende al 50%.E veniamo alle novità del decreto, ossia le modalità per ottenere in concreto il credito d'imposta.

Prima di tutto bisogna inviare, in via telematica, un'istanza all'Agenzia delle Entrate, in cui indicare l'importo delle spese agevolabili sostenute nel 2016. Purtroppo non si sanno ancora quale schema utilizzare per l'istanza e il termine di invio, demandati ad un provvedimento del direttore dell'Agenzia delle Entrate da emanarsi entro il 7 marzo. Quello che si sa è che, in base al rapporto tra risorse stanziate con la Legge di Stabilità 2016 e il credito d'imposta complessivamente richiesto, l'Agenzia delle Entrate determinerà la percentuale massima del "bonus" spettante a ciascun richiedente, che sarà comunicata con un altro provvedimento da emanarsi entro il 31 marzo 2017. Il credito d'imposta dovrà poi essere indicato nella dichiarazione dei redditi relativa al periodo d'imposta 2016, e sarà utilizzabile in compensazione. A tal fine, il modello F24 dovrà essere presentato esclusivamente tramite i servizi telematici offerti dall'Agenzia delle Entrate, pena il rifiuto dell'operazione di versamento. In alternativa, le persone fisiche non titolari di redditi d'impresa o di lavoro autonomo potranno utilizzare il credito spettante in diminuzione delle imposte dovute in base alla dichiarazione dei redditi. L'eventuale ammontare del credito d'imposta non utilizzato potrà essere fruito nei periodi di imposta successivi, senza alcun limite temporale.

Occhio: il credito d'imposta non è cumulabile con altre agevolazioni fiscali per le stesse spese. Se l'Agenzia delle Entrate dovesse accertare che l'agevolazione non spetta o spetta solo in parte, procederebbe all'immediato recupero.

TEMPI STRETTI

All'Agenzia delle Entrate spetta un discreto lavoro: dal 7 marzo restano infatti solo 24 giorni per spedire tutte le istanze, processarle, definire la ripartizione e comunicarla agli interessati. Lato contribuente, poiché il termine ultimo per conoscere l'esatto ammontare del credito scade il 31 marzo, si arriva giusto giusto a ridosso del 730. E lì bisognerà poi capire cosa sia più conveniente tra detrazione o credito d'imposta (che – lo ricordiamo - sono alternativi). Per capire cosa effettivamente convenga, l'unico modo è presentare l'istanza, e giù altro superlavoro per l'Agenzia. A meno che l'assegnazione del credito non dia per assunta la scelta. Staremo a vedere.

a&s ITALY
sale a quota 55.000
e da' i numeri...

55.000 le copie totali nel 2016	**70%** il market share raggiunto anche nel 2016	**9** le indagini pubblicate nel 2016	**6** numeri l'anno	**9.167** le copie a numero (sei) sottoposte a certificazione nel 2016
59.000 le copie previste nel 2017	**53** gli eventi a cui abbiamo partecipato in Italia e all'estero nel 2016	**968** pagine stampate nel 2015	**986** pagine stampate nel 2016	**132** i punti di distribuzione delle copie

Ksenia
security innovation

FULL WIRELESS ALL-IN-ONE

www.kseniasecurity.com

Piattaforma IP Wireless per la Sicurezza e Home Automation **lares wls 96-IP**

SEMPRE CONNESSO.

Ksenia
security innovation

www.kseniasecurity.com

www.omc2017.it

OFFSHORE MEDITERRANEAN
CONFERENCE & EXHIBITION

OMC 2017

TRANSITION TO A SUSTAINABLE ENERGY MIX:

The Contribution of the Oil & Gas Industry

29-31 March 2017
RAVENNA ITALY

18,000 visitors

688 exhibitors

1,200 delegates

REGISTER NOW ON
www.omc2017.it

OMC
CONFERENCE ORGANISER
conference@omc.it

YouTube

IES International Exhibition Services
EXHIBITION ORGANISER
exhibition@omc.it

Elvy Pianca

Edifici multipurpose: l'esempio dei casinò

Multipurpose buildings, ovvero edifici con destinazioni multiple. Come gestire, in questi siti particolari, un tema ampio e circostanziato come la sicurezza? Non si può che procedere per esemplificazioni. Parleremo dunque dei casinò come *caso di scuola* e riscontreremo che, mentre il mercato mostra segnali di ripresa, grazie al traino dei nuovi edifici nella zona Asia-Pacifico, e al retrofit di quelli europei e americani, l'evoluzione tecnologica verso l'IP consente non solo di utilizzare videocamere sempre più perfezionate, che coprono anche gli angoli più bui, ma anche strumenti di analitica per gestire le emergenze in tempo reale ed esaminare i dati in vista di strategie marketing, integrandosi con tutti gli altri sistemi come il controllo accessi, l'antincendio e molto altro ancora.

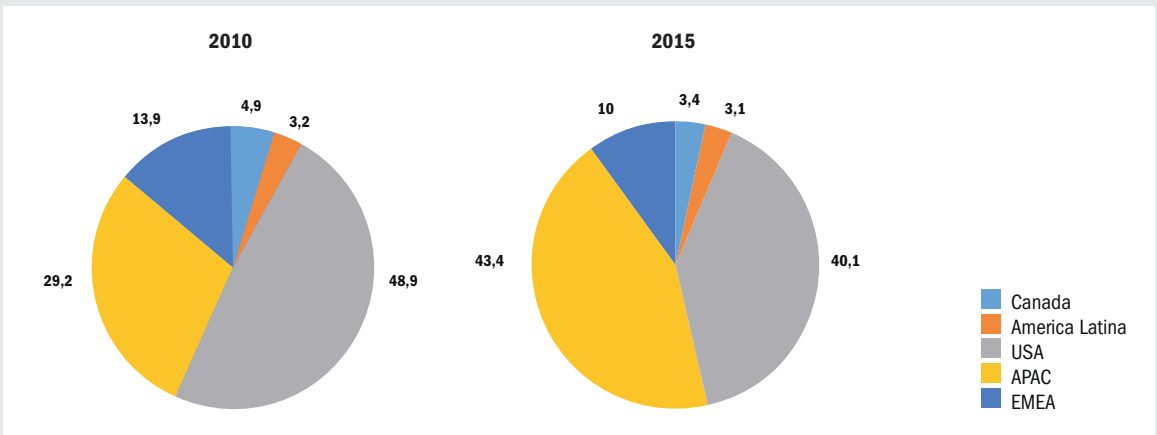
Li chiamano “multi-purpose buildings” e, secondo ANIE Sicurezza, che ha organizzato nell’ambito della mostra convegno “Sicurezza & Oltre 2016” proprio una sessione verticale sul tema, si tratta di aree con destinazioni multiple. Ad esempio hotel, uffici, stadi, poli sanitari, centri commerciali e quartieri fieristici. E’ intuitivo che un edificio nel quale convivono diverse funzioni - come, banalmente, uffici, abitazioni e, magari, negozi - o nel quale possono essere svolte attività varie - ad esempio, un hotel, in cui ci sono gli ospiti che soggiornano, ma anche chi vi si reca per una conferenza, una mostra o un evento – presenti delle esigenze di sicurezza anch’esse diversificate e, possibilmente, integrate. E’ quello che richiedono gli operatori del settore, i quali lavorano già da tempo in direzione di un’ottimizzazione e, appunto, di un’integrazione tra i vari sistemi, principalmente videosorveglianza, antintrusione, antincendio e controllo accessi.

CASINÒ

Sono ovviamente tanti gli edifici “multi-purpose”. In questo numero, vogliamo parlare di una categoria un po’ particolare: i casinò. Molto “americani” e scenari di numerosi film, questi edifici non servono solo, o per lo meno non unicamente, per il gioco. Ne abbiamo un esempio lampante proprio in Italia, dove il celebre Casinò di Sanremo ha ospitato, fino al 1977, addirittura il Festival della Canzone Italiana, e, oggi, fornisce la “location” a numerosi eventi culturali e, ovviamente, musicali, con concerti di cantanti che hanno conseguito la notorietà proprio sul palco del vicino teatro Ariston. Prima di arrivare alle soluzioni tecnologiche, partiamo, come sempre, dai numeri e, quindi, dai dati di mercato. In generale, il mercato della sicurezza nei casinò negli ultimi 10 anni ha subito i contraccolpi della recessione mondiale ed è ovvio che, se non ci sono soldi, non c’è nemmeno la possibilità, se non la voglia, di giocarseli. Secondo il PricewaterhouseCoopers’ (PwC) Global Gaming Outlook report, il 2010 è stato il primo anno, dal 2007, in cui i numeri del mercato dei casinò negli Stati Uniti, la “patria” di questi edifici, hanno ripreso, sia pure lievemente, a salire.

Per contro, negli ultimi 5 anni, le regioni EMEA hanno subito i contraccolpi più duri, e questo non solo per la crisi economica, ma per le nuove normative dei Governi, come, ad esempio, quella che ha proibito il fumo nei locali pubblici nei Paesi Europei e quella che ha limitato l’operatività delle case da gioco in numerose zone della Russia. Così, è successo che l’APAC (zona Asia-pacifico) ha superato l’EMEA nel mercato dei casinò, aumentando da 34.3 miliardi di dollari nel 2010 a 79.3 nel 2015, con un CAGR del 18.3%, e Macao ha annunciato che, nel 2013, il suo guadagno totale per ciò che riguarda i

ANDAMENTO DEI GUADAGNI IN PERCENTUALE DEL MERCATO MONDIALE DEI CASINÒ



Fonte: PricewaterhouseCoopers, rielaborazione a&s Italy

casinò ha settuplicato quello, e scusateci se è poco, di Las Vegas…E dire che, in Cina, il gioco, almeno sulla carta, è illegale…e quindi si aggira il problema frequentando le zone vicine, come appunto Macao, Singapore e le Filippine, dove stanno spuntando come i proverbiali funghi nuovi edifici davvero "multi-purpose", con spiagge attrezzate, hotel, ristoranti, centri commerciali e, per inciso, i casinò. In ogni modo, passata la recessione, il mercato statunitense ha ripreso a crescere e, per ciò che riguarda la sicurezza, si è decisamente puntato sui sistemi di videosorveglianza IP.

INTEGRAZIONE

Ma anche nei nuovissimi casinò asiatici, o nel retrofit europeo, l'esigenza di una sorveglianza "onnicomprensiva" è ormai diventata pressante, per consentire agli operatori di tracciare e tenere sotto controllo ogni singolo evento e garantire ai loro clienti quella sicurezza che è un valore ancora più indispensabile in edifici di puro entertainment. E non solo: dato che si tratta di strutture comunque complesse e, appunto, "multi-purpose", è anche indispensabile aggiungere alla normale routine di sicurezza le funzioni di analitica, per pianificare le operazioni, dirigere il "traffico" dei giocatori/visitatori e promuovere attività di marketing che non riguardano, magari, strettamente il gioco, ma gli eventi che si organizzano nell'edificio.

NON SOLO AL TAVOLO

Così dappertutto si assiste alla sostituzione, o, in alcuni casi, all'integrazione, delle vecchie telecamere analogiche con quelle con visione a 360° e HD, per "vedere" non solo quello che accade intorno ai tavoli da gioco o agli ingressi, ma in ogni angolo di sale e saloni, anche i più bui, grazie ai LED IR che, ormai, sono quasi di serie in tutte le videocamere. E, dato che alle persone, in particolare ai giocatori, non piace certo sentirsi "sorvegliato speciale", questi dispositivi sono ormai talmente "discreti" da potersi mimetizzare con facilità con l'ambiente. Di sicuro, per quanto evolute, le videocamere da sole non bastano, ed ecco così diffondersi i sistemi completi di videosorveglianza IP, magari con piattaforma aperta, in modo che siano integrabili con gli altri componenti della sicurezza, come, per fare l'esempio più banale, i sensori per il controllo degli accessi. Per esempio, l'analitica video che consente di effettuare non solo il conteggio delle persone, ma di elaborare anche quelle "heat map" che sono indispensabili agli addetti alla sicurezza, e al marketing, per capire quali sono, appunto, le zone più calde", frequentate, dello specifico edificio. Le immagini "catturate" dalle videocamere, poi, vengono registrate dai NVR e gestite dagli operatori, anche a distanza, tramite appositi software, che prevedono opzioni multiple di ricerca e, particolare non secondario, perché tutti conosciamo la "pesantezza" dei video, immagazzinate non più nei singoli dispositivi, ma in un cloud, senza, quindi, "sovraccaricare" le macchine in campo.

Le piattaforme software, ormai, sono davvero "intelligenti" e consentono di centralizzare tutti i dati che provengono dai diversi sottosistemi (ad esempio, anche l'antincendio…), di sottoporli in tempo reale all'operatore, di prendere delle decisioni, di qualsiasi tipo, in tempo più che reale…

Insomma, anche negli edifici "multi-purpose" la presenza di soluzioni sempre più integrate e con infrastruttura IT diventa sempre più numerosa e verso questa direzione si sta evolvendo il mercato…tenendo conto che ormai non basta certo più, in nessun edificio, raccogliere solo i video e i dati, ma analizzarli e decidere, subito, il da farsi.

Diamo più valore ai dettagli.

HD VIDEO CABLES

Nuova generazione
di cavi speciali per sistemi
di videosorveglianza

I cavi HD sono progettati per l'impiego con sistemi **analogici tradizionali, A HD, HD CVI, HD SDI, HD TVI, POC e 4K.** Consultare la documentazione tecnica per verificare le distanze massime percorribili in funzione della larghezza di banda impiegata.

BETACAVI

SEMPRE UN PASSO AVANTI.

info@betacavi.com

I prodotti BETA CAVI sono sviluppati in conformità dei requisiti tecnici richiesti dai migliori marchi di produttori di apparati:

BOSCH Invented for life · alhua TECHNOLOGY · HIKVISION · Panasonic ideas for life · SAMSUNG WISENET

Pierdavide Scambi(*)

Stadi sicuri: videosorveglianza e non solo

Questo numero di *a&s Italy* è dedicato ad una tipologia di edifici piuttosto vasta e variegata, e tuttavia caratterizzata da un denominatore comune, ossia la destinazione d'uso non univoca ma molteplice. Parliamo dei Multipurpose buildings, edifici asserviti cioè a più scopi: ospitalità, ma anche entertainment, o magari azienda sanitaria, ristorazione, palazzo uffici. Progettare la sicurezza in questa tipologia di edifici è quindi un caso diverso volta per volta, in base alla tipologia prevalente di struttura. In questo contributo parleremo di uno stadio.

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

Quando si parla di sicurezza in impianti sportivi, come ad esempio gli stadi o le arene polisportive, è necessario innanzitutto capire come prevenire e/o risolvere le più svariate crime situation, che possono spaziare dai piccoli furti alle possibili minacce terroristiche. Tale sfida si affronta grazie all'uso di attrezzature tecnologiche sempre più avanzate in modo da garantire la maggiore sicurezza possibile. La tecnologia infatti è diventata un validissimo alleato per proprietari/gestori di questi grandi impianti al fine di individuare in maniera tempestiva, prevenire e risolvere ogni tipo di problema possa insorgere.

LA NORMATIVA

Convivono spesso, in questo tipo di strutture, anche attività di ristorazione e commerciali. Concentrerei però, per la dimensione e la specificità di questi immobili di estesi volumi e altezze, l'analisi di solo alcuni impianti regolamentati da precise normative. In particolare la Circolare Ministeriale (Dipartimento della Pubblica Sicurezza - Osservatorio Nazionale sulle Manifestazioni Sportive) n.555/ONMS/183/2016 del 13 maggio 2016 per la messa a norma degli impianti.

Il complesso sistema di governo e gestione degli eventi specialmente calcistici, nonostante gli ultimi dati rassegnino un quadro di positività, continua ad essere caratterizzato da un progressivo deterioramento delle apparecchiature ove si disputano gare di campionati professionistici e dilettantistici. A tal fine, nell'evidenziare il ruolo di supporto della "Commissione dell'Osservatorio per la messa a norma degli impianti sportivi" (Istituita con decreto del Capo della Polizia in data 4 aprile 2010), si richiama l'attenzione sul puntuale rispetto della disciplina di settore, con particolare riferimento ai seguenti provvedimenti:

- Decreto Ministeriale 18 marzo 1996 e successive modifiche (criteri per la costruzione di impianti sportivi);
- Decreto Ministeriale 6 giugno 2005 (videosorveglianza e ticketing);
- Decreto Legislativo 8 febbraio 2007 convertito con legge n.41/2007 (misure urgenti per la prevenzione e repressione dei fenomeni di violenza connessi a competizioni calcistiche);
- Determinazione dell'Osservatorio n.26/2014;
- Documento della Task force sulla sicurezza delle manifestazioni sportive.

Dal complesso delle citate disposizioni emerge un preciso modello di organizzazione strutturale che, in sintesi, risulta improntato ai seguenti elementi basilari: la corretta configurazione dell'area riservata e dell'area di massima sicurezza, nonché l'idonea realizzazione dei varchi e dei tornelli.

Tralasciando le indicazioni del numero dei varchi di ingresso proporzionato alla capienza del settore e il numero di tornelli minimo, la suddivisione dei settori rispetto a visitatori (locali e/o ospiti), i sistemi di separazione tra spalti, spettatori e attività sportive (parapetti e fossati), concentrerei l'attenzione sull'esigenza che la descritta organizzazione strutturale venga integrata da un efficiente sistema di videosorveglianza. Le caratteristiche minimali dovranno essere: a) un numero idoneo (mai inferiore a due) di telecamere interne dedicate ad ogni singolo settore di tipo controllabile, che consentano di avere contemporaneamente una visione d'insieme ed una del particolare interessato; b) una telecamera dedicata ad ogni singolo tornello; c) un numero idoneo di videocamere per il monitoraggio dell'area di massima sicurezza; d) un numero idoneo di telecamere per il monitoraggio degli accessi, del perimetro dell'area riservata e la sorveglianza delle vie di afflusso principali; e) dispositivi di registrazione delle immagini; f) un numero idoneo di monitor tale da consentire la visualizzazione contemporanea delle telecamere; g) sistemi di controllo e di manovra delle telecamere realizzati in modo da consentire più interventi contemporaneamente; h) un impianto di energia sussidiaria; i) un idoneo correlato impianto di illuminazione (interno ed esterno), che consenta la corretta ripresa da parte del suddetto impianto di videosorveglianza anche in orario notturno. Per poter sorvegliare opportunamente le aree indicate (solitamente identificate in a maggior rischio e a basso rischio), si dovranno utilizzare: a) camere multimegapixel in tecnologia singolo sensore posizionate frontalmente rispetto ai soggetti da riprendere (dalla tribuna sud si visionerà l'intera tribuna nord e viceversa); b) camere brandeggiabili PTZ dedicate alla restante parte dello stadio ed al supporto puntuale dell'attività investigativa; c) opportuni sistemi di storage per la retention dei video; d) video management software ad uso e consumo del personale addetto alla sorveglianza; e) sala controllo, con dispositivi appositamente dedicati agli operatori.

RISOLVENZA

Il sistema di ripresa per uno stadio deve porre anche particolare attenzione all'aspetto della qualità delle immagini ricevute dalla sala controllo dove gli operatori lavoreranno. L'approccio tradizionale alla videosorveglianza vuole che si acquisiscano immagini sempre più dense di informazioni e di alta qualità e, magari, anche molte volte al secondo. Va però ricordato che quando si parla di capacità di risolvenza di una telecamera, ovvero della capacità insita nelle immagini di permettere il riconoscimento del minimo dettaglio desiderato, si deve sfatare il falso mito che questa sia misurabile semplicemente contando i pixel effettivi disponibili sul sensore di immagini montato a bordo della telecamera stessa: i pixel infatti sono una condizione necessaria, ma non sufficiente, per catturare i dettagli. Senza un numero minimo di pixel per una data area target non è possibile individuare un dettaglio ma il numero di pixel nativamente disponibile sul sensore determina il potenziale, non la qualità finale. Il comune fraintendimento è che un più alto numero di pixel generi sistematicamente una qualità finale migliore. La misura della capacità di risolvenza di una telecamera va misurata a valle di tutta la complessa catena di elaborazione che si frappone tra l'immagine finale su cui lavora l'operatore e la luce incidente sulla telecamera che viene riflessa dal bersaglio che si vuole vedere. Tipo e qualità delle ottiche, tipo e tecnologia del sensore di immagine, metodi di bilanciamenti ed elaborazione, tipo di algoritmi di compressione, forma di trasmissione e di decodifica possono deteriorare la qualità delle immagini compromettendo anche un buon rapporto nativo tra pixel e area inquadrata. A titolo di esempio, un'immagine catturata da un sensore da 1920x1080 pixel può essere migliore e risolvere maggiori dettagli di una immagine catturata da un sensore da 3840x2160 pixel se quest'ultimo è eccessivamente compresso o se il sensore ha caratteristiche ottiche di scarsa qualità. Secondo le prescrizioni delle più recenti emanazioni in materia di sicurezza negli stadi, la densità di informazione richiesta alle immagini catturate all'interno del catino sportivo deve essere maggiore o uguale a 180 pixel/metro per le zone a maggior rischio. Questa metrica dovrebbe, negli intenti del legislatore, rappresentare un valore di riferimento in grado univocamente di discriminare la riconoscibilità o meno di un volto nell'immagine per le finalità investigative. Perciò per le applicazioni in ambito stadio, dove il singolo fotogramma diventa l'informazione chiave per l'attività di indagine, si può prediligere la compressione MJPEG per i flussi Ultra HD che, contrariamente alla compressione H264 o superiore, permette di avere ogni fermo-immagine preciso e dettagliato senza artefazioni o perdite di informazione dovute alla ricostruzione temporale degli algoritmi predittivi tipici di compressioni troppo spinte, orientate a sacrificare la qualità dell'immagine a beneficio delle risorse necessarie per trasmetterla. Inoltre attraverso il cosiddetto "Edge Storage" (dischi SSD, dunque estremamente performanti e capienti, direttamente sulla telecamera), si è in grado di immagazzinare fotogrammi ad altissima risoluzione, Ultra HD, ed elevato frame rate (fino a 30 fps per elevata dinamicità nella gestione di video in rapido cambiamento) per il tempo necessario allo sviluppo dell'evento sportivo, rimandando costantemente alla sala di controllo un flusso scalato, tipicamente Full HD, e lasciando a necessità specifiche di indagine l'effettivo uso delle immagini archiviate all'interno della telecamera da parte degli operatori. Qualità dunque solo quando effettivamente necessario e non un continuo streaming da camera a sistemi di storage.

volonteweb.com

I record son fatti per essere battuti

Genia nelle sue 2 versioni a 4 o 8 canali video è l'entry level di una nuova famiglia di NVR GAMS, ma non per questo le sue doti possono passare inosservate. Infatti con lo Switch integrato PoE si possono alimentare le telecamere IP direttamente, creando sistemi Plug & Play in modo facile e veloce.

Genia

Caratteristiche: NVR GAMS embedded 4 flussi video espandibili a 8 e 4 ingressi di allarme switch 4 o 8 porte PoE (IEEE 802.3af) integrato - Onvif S - throughput 96Mbps (48/Rec+48/Play) - Linux embedded - H.264 - Fanless con ventola di emergenza termostatata - HD 1TB 3,5" - WD Purple Green Power per streaming video 24x7 uscite video indipendenti 1xPAL/1xVGA/1xHDMI - porta Lan up-link Gigabit - Firewall

CERTIFICAZIONE DI SISTEMA QUALITÀ DNV·GL ISO 9001

BETTINI
VIDEO & SECURITY TECHNOLOGY

GAMS
Digital Video Solution

Bettini Srl - Via E. H. Grieg, 23 - 21047 Saronno (VA) - Tel. +39 02 89651000 - Fax +39 02 93182042 - E-mail: info@bettinivideo.com - Sito web: www.bettinivideo.com

Marco Soffientini(*)

Videosorveglianza, PA e privacy: regole generali

Recentemente, l'Autorità Garante della Protezione dei dati personali si è occupata (provv. 10 novembre 2016, doc. web n. 5796716) di un'istanza di verifica preliminare ai sensi dell'art. 17 del Codice, avanzata dalla Città Metropolitana di Roma Capitale in relazione ad un sistema di videosorveglianza c.d. *intelligente*, da attivare presso gli accessi e le uscite di emergenza dell'edificio che ospita la sede dell'Amministrazione, per finalità di sicurezza degli accessi e di tutela del patrimonio. L'occasione è quindi propizia per parlare di videosorveglianza, PA e privacy.

L'impianto, costituito da telecamere collocate in corrispondenza dei tornelli e delle uscite di emergenza, si attiverebbe nei soli casi in cui dei sensori rilevino un tentativo di accesso non autorizzato all'interno dell'edificio, per effetto dello scavalcamento dei tornelli o dell'effrazione delle uscite di emergenza. Al verificarsi di uno di questi eventi, le telecamere avvierebbero una registrazione dell'evento e contemporaneamente farebbero scattare un allarme alla control room. Come evidenziato dal Garante, la richiesta di verifica preliminare ha ad oggetto un sistema di videosorveglianza idoneo a rilevare automaticamente, segnalare e registrare un comportamento o evento anomalo, quale può considerarsi

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

lo scavalcamento dei tornelli e l'effrazione delle uscite di emergenza, e pertanto rientra tra quelli per i quali l'Autorità, nel provvedimento generale in tema di videosorveglianza del 2010 (pubblicato in G.U. n. 99 del 29 aprile 2010 doc. web n. 1712680), ha previsto l'obbligo di richiesta di verifica preliminare.

SOGGETTI PUBBLICI

Il caso ci fornisce lo spunto per richiamare il § 5 del Provv. 08.04.2010, in base al quale i soggetti pubblici, in qualità di titolari del trattamento (art. 4, comma 1, lett. f), del Codice), possono trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (art. 11, comma 1, lett. b, del Codice), soltanto per lo svolgimento delle proprie funzioni istituzionali. Ciò vale ovviamente anche in relazione a rilevazioni di immagini mediante sistemi di videosorveglianza (art. 18, comma 2, del Codice). Inoltre, i soggetti pubblici sono tenuti a rispettare, al pari di ogni titolare di trattamento, qualora il trattamento sia effettuato tramite sistemi di videosorveglianza, i principi enunciati nel provvedimento 08.04.2010. Così, tornando al caso in esame, la Città Metropolitana di Roma Capitale può, in qualità di titolare del trattamento, trattare dati personali nel rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi (cfr. artt. 4, comma 1, lett. f); 11, comma 1, lett. b) del Codice). Alla luce delle esigenze di tutela della sicurezza, che trovano particolare riscontro in considerazione delle specifiche caratteristiche dell'edificio, e della sua destinazione, che lo espongono ad un livello di rischio elevato, con conseguente necessità di contrastare efficacemente eventuali intrusioni da parte di soggetti non autorizzati, l'Autorità Garante ha ritenuto proporzionato e, quindi, ammissibile il trattamento dei dati personali sottoposto a verifica per le finalità di sicurezza degli accessi alla sede, delle persone e dei beni.

VERIFICA PRELIMINARE E CARTELLI

Dalla lettura del caso, si evince che anche i soggetti pubblici sono tenuti a presentare istanza di verifica preliminare ai sensi dell'articolo 17 del Codice Privacy, qualora intendano installare, ad esempio, impianti c.d. intelligenti e cioè quei sistemi di videosorveglianza in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli e, all'occorrenza, registrarli.

Si tratta di sistemi particolarmente invasivi, capaci di incidere nella sfera di autodeterminazione dell'individuo e, quindi, sui suoi comportamenti. Per questi motivi, il sistema deve essere sottoposto a verifica preliminare ed è consentito solo in casi particolari, tenendo «conto delle finalità e del contesto in cui essi sono trattati, da verificare caso per caso sul piano della conformità ai principi di necessità, proporzionalità, finalità e correttezza» (artt. 3 e 11 del Codice).

Ovviamente, come accennato, i soggetti pubblici devono rispettare l'intero provvedimento in tema di videosorveglianza e così i cittadini, che transitano in aree sorvegliate, devono essere informati con "cartelli" (informative) visibili al buio, se il sistema di videosorveglianza è attivo in orario notturno, e qualora il sistema di videosorveglianza installato dal soggetto pubblico sia collegato alle forze di polizia, è necessario uno specifico cartello informativo, sulla base del modello elaborato dal Garante nel provvedimento sulla videosorveglianza del 2010. Pertanto, i Comuni, che installano telecamere per fini di sicurezza urbana, hanno l'obbligo di apporre cartelli che ne segnalino la presenza, salvo che le attività di videosorveglianza siano riconducibili a tutela della sicurezza pubblica, prevenzione, accertamento o repressione dei reati. La conservazione dei dati non potrà superare i 7 giorni, fatte salve speciali esigenze.

VIDEOSORVEGLIANZA DI STRUTTURE PUBBLICHE

Il caso affrontato e in generale l'attività di videosorveglianza svolta da soggetti pubblici ci fornisce lo spunto per evidenziare come esistano diverse attività, svolte da soggetti pubblici, che non sono tecnicamente qualificabili come "compiti", ed è questo proprio il caso, sottolineano i Garanti europei, dell'attività di videosorveglianza di strutture pubbliche. In questi casi, premesso che non si tratta di veri e propri compiti, c'è da domandarsi quale sia la condizione di liceità che consente ai soggetti pubblici di svolgere attività di videosorveglianza. Il gruppo dei Garanti Europei, già nell'aprile 2014, affrontò il problema con riferimento alla Direttiva 95/46/Ce, stabilendo che tale attività risultava lecita quando rispondeva ad un interesse pubblico riconducibile ai punti e) o f) dell'articolo 7 della suindicata direttiva. A questa considerazione, oggi, si può aggiungere quanto indicato dal regolamento europeo in tema di dati sensibili, che consente lo svolgimento di attività, che non possono qualificarsi come veri e propri compiti, in tutti quei casi in cui il relativo trattamento sia "necessario per motivi di interesse pubblico rilevante". (art. 9, comma 2, lett. g) Reg. UE.).

WE CHANGED THE RULES!

Tiandy

GARANZIA 5 ANNI

FINO A 5 ANNI DI GARANZIA

SOSTITUZIONE 36 MESI

SOSTITUZIONE IMMEDIATA FINO A 36 MESI

Tiandy Digital Technology Co., Ltd.
sales@tiandy.it | www.tiandy.it

NUOVE CENTRALI COMPATTE DI EVACUAZIONE VOCALE

Scarica il depliant

CENTRALI DI EVACUAZIONE VOCALE CERTIFICATE EN54-16

Sistema di evacuazione vocale compatto certificato EN54-16 per la gestione di messaggi di allerta ed evacuazione.
Disponibile con 2, 4 o 6 zone audio con potenza massima di 500W complessivi ripartibili liberamente sulle zone audio gestite. Incluso nell'unità un alimentatore certificato EN54-4, amplificatori, unità di controllo del sistema, microfono selettivo per invio allarmi.

Comelit®
Passion.Technology.Design.

www.comelitgroup.com

Filippo Novario(*)

Big Data nella Videosorveglianza: cyber security per la qualità dei dati

La videosorveglianza si avvia, per motivi tecnici e pratici, all'accumulo di importanti masse di dati. Parliamo di importanti influssi informatici, sotto il profilo digitale e telematico, che implicano la produzione e lo stoccaggio di masse di dati di volume sempre maggiore. Una massa di dati non deve essere confusa con i cosiddetti *Big Data*: la prima è una mera raccolta di dati, di tipo esteso o limitato; i secondi, invece, sono tecnologie e metodi per l'elaborazione di dati e conseguente estrazione di informazioni. I dati sono tasselli che recano descrizioni tecniche a cui è necessario "dare un senso". Si presentano come elementi tanto informaticamente semplici quanto tecnicamente fragili, alterabili e violabili, come le infrastrutture ICT che li producono, li elaborano e li contengono, implicando la necessaria disposizione di tecniche di sicurezza informatica e mitigazione dei rischi *cyber*. I processi analitici dei *Big Data* recano peculiari elementi di rischio *cyber*.

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

Questi consentono, da determinati elementi di *input*, di derivare molteplici *output* attraverso disposizioni algoritmiche correlate: da un *input* deriva un *output*, che diviene a sua volta *input* per un altro processo d'elaborazione, e così via. L'attività di analisi, conformata o scelta dal gestore dei dati, può anche fornire *output* eccedenti le necessità d'elaborazione, a volte in modo fortuito, attraverso elementi tecnici e di controllo: come accade ad esempio per i *log* di sistema. Le elaborazioni concatenate *input-output* possono conferire dati utili ad altri tipi di elaborazioni informatiche, disposte anche da altri soggetti o enti, favorendo il raggiungimento di *output* che esulano dai contorni della attività d'elaborazione primaria. Queste evidenze tecniche nel campo dei *Big Data* spostano l'attenzione verso il tema della qualità del dato per l'elaborazione.

LA QUALITÀ DEL DATO

Il dato, sotto il profilo proprio dei *Big Data*, non è tale perché reca descrizioni tecniche, è tale solo se genuino, raccolto senza alterazioni e così conservato, affinché possa conferire un *output* preformante. Deve quindi mostrare qualità durante i passaggi tecnico-logici del trattamento digitale: 1) Inserimento del dato; 2) Stoccaggio del dato; 3) Modificazione del dato; 4) Cancellazione del dato; 5) Elaborazione del dato; 6) Divulgazione/Condivisione dei dati.

Ogni passaggio tecnico mostra differenti peculiarità per la garanzia della qualità dei dati.

L'inserimento e lo stoccaggio del dato devono mirare alla non alterazione del dato inserito.

La modificazione e la cancellazione, invece, devono tendere all'aggiornamento del dato, così da alterarlo solo per diritto e volontà dell'utente, a seguito di sua ponderazione e lasciandone traccia.

Elaborazione, singola o attraverso processi "a catena", e Divulgazione-Condivisione dei dati, concernono l'uso del dato inserito, stoccato, modificato o cancellato, quale *input* di qualità per ottenere *output* diversi e altrettanto qualitativi. I momenti *ante* inserimento e *post* fruizione dei dati mostrano principi di tutela radicati in espresse regole giuridiche, ordinarie e speciali. I momenti tecnici prima indicati, invece, necessitano di tutele, oltre che giuridiche, soprattutto tecnico-informatiche, concernenti la gestione del dato e le attività algoritmiche d'analisi, portate di riflesso dalla sicurezza digitale e telematica delle infrastrutture ICT, con peculiari profili di *Cyber Security*.

CYBER SECURITY

La *Cyber Security* è una disciplina che presenta espliciti profili tecnici associati a impliciti profili giuridici, a fronte di questioni e soluzioni correlate di tipo informatico-giuridico, fondendo l'ICT *Security* con l'Informatica Giuridica e Forense per giungere alla garanzia della Qualità del dato. In particolare, le tecniche di *cyber* difesa sono orientate alla tutela dei dati nei loro momenti digitali-telematici, mentre le soluzioni tecnico-giuridiche sono orientate alla mitigazione del rischio *cyber* attraverso differenti soluzioni:

- Disposizione di tecniche *cyber security by design* e *by default*.
- Creazione e diffusione di *policy* e procedure.
- Conformazione dell'organizzazione aziendale per la *cyber* difesa.
- Disposizione d'attività d'accertamento tecnico dei dati.

Le attività di *cyber security* devono essere oggetto di una politica di *Governance* quale elemento primo per la tutela del dato, orientata alla creazione *cyber safe* dell'infrastruttura quanto al reperimento del *know how* necessario attraverso conoscenze interne o consulenze esterne. Deve altresì prevedere attività per il controllo dello stato dell'arte, attraverso *Assessment* svolti da personale interno o enti esterni e terzi, al fine di comprendere il rischio *cyber* esistente e indicare attività proattive all'ulteriore mitigazione del rischio e all'aumento della *performance*.

La *Big Data analysis* applicata alla videosorveglianza mostra alcuni elementi cardine concernenti la *cyber security* per la tutela della qualità del dato.

CONSERVAZIONE GENUINA DEI DATI

Durante le fasi di inserimento e stoccaggio dati, attività performanti da disporre concernono la *cyber security by design* e *by default*, associate a *policy* e procedure per la gestione del rischio *cyber*. In particolare: la disposizione

di tecniche per l'accesso limitato e controllato al sistema; la crittazione per l'interconnessione tra *device* utente e impianto di videosorveglianza; la presenza di *firewall* e tecniche di *alert security; la* disposizione di *tool* e/o tecniche per la cristallizzazione del dato, *forensics oriented.*

MODIFICAZIONE DEI DATI AD OPERA DELL'UTENTE

Le attività di modificazione e cancellazione dei dati sono evidentemente invasive, a fronte della piena disponibilità del dato, dal suo nuovo inserimento alla sua distruzione. A tal proposito divengono essenziali: il tracciamento delle attività digitali svolte dall'utente; l'elaborazione e la divulgazione di *policy* e procedure per gli utent; lo sviluppo di tecniche *user oriented*, con conferma per la modificazione e cancellazione dei dati; la disposizione di tecniche per l'accesso limitato e controllato al sistema.

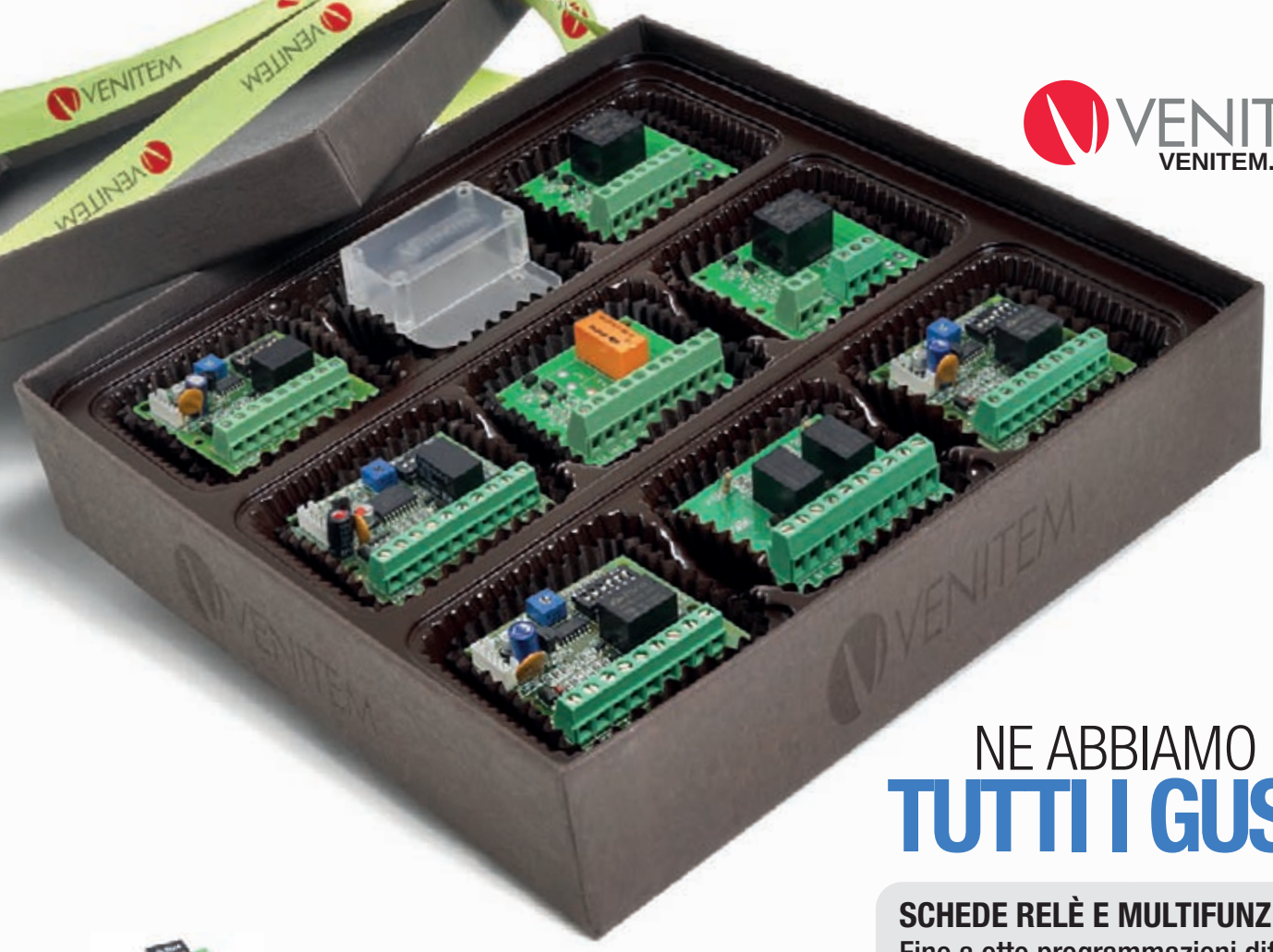
ELABORAZIONE E DIVULGAZIONE/ CONDIVISIONE DI DATI

Le tecniche di *cyber* difesa per la garanzia della qualità del dato nelle fasi di elaborazione-condivisione mostrano una caratura più informatico giuridica, fondata sulla necessita di essenziale trasparenza del trattamento dati. Questa ha il suo fulcro nella formalizzazione di autorizzazione, non vincolante o necessaria, per l'elaborazione e la divulgazione del dato anche a enti terzi, che possano utilizzarli per fini ulteriori e non compatibili con il fine primario e principale per cui il dato è stato conferito. L'autorizzazione deve essere conferita a monte della elaborazione dei dati, anche senza la necessità di esplicitare le proprietà tecniche dell'algoritmo di elaborazione, ben chiarendo, però, le attività svolte per mantenere un alto grado di qualità del dato.

IN SINTESI

La Qualità del dato è un tema centrale nella Videosorveglianza. La *Cyber security*, nella sua essenza informatico giuridica e forense, è la disciplina che può garantire la conservazione, la modificazione e l'elaborazione/diffusione dei dati secondo alti gradi di qualità. La sicurezza della qualità del dato, ed il suo inevitabile degradamento, se controllato e monitorato, nonché trasparentemente divulgato, può consentire una performante tutela dell'utente e dell'ente.

VENITEM
VENITEM.COM



NE ABBIAMO PER TUTTI I GUSTI.

SCHEDE RELÈ E MULTIFUNZIONE:
Fino a otto programmazioni differenti e con diverse temporizzazioni in un unico prodotto. Venitem è riuscita ad ottenere questa flessibilità nell'utilizzo delle schede relè, in grado di moltiplicare all'infinito la propria capacità di gestione. Numerose applicazioni **per impianti antifurto, TVCC e automazione domotica**, il tutto unito alla funzionalità del contenitore protettivo **DIN BOX** di misura standard, che consente l'installazione dei circuiti nei quadri elettrici e dove siano presenti numerosi cablaggi, e permette il montaggio in serie di più schede, grazie al comodo aggancio ad incastro laterale.

RA – Scheda per open collector con uscita a relè.
Circuito interfaccia a un ingresso da 35mA e un'uscita relè da 3A.

RA/T – Scheda a basso assorbimento per open collector con uscita a relè. Circuito interfaccia a un ingresso da1mA e un'uscita relè da 3A.

RA/2S – Scheda a basso assorbimento per open collector con due uscite isolate. Circuito interfaccia a un ingresso da 1mA e due uscite relè da 1A.

RN 12/24 – Scheda per open collector con due ingressi e due uscite a relè. Circuito interfaccia a due ingressi da 25mA e due uscite a due relè da 1A.

MTT – Circuito multifunzione per tutte le temporizzazioni - due ingressi da 1mA - un'uscita relè da 1A - un'uscita O.C.

MCX – Circuito multifunzione per contatti tapparelle, serrande, sensori inerziali, vibrazioni - un ingresso da 1mA - un'uscita relè da 1A - un'uscita O.C.

MCV – Circuito multifunzione per contatti tapparelle e magnetici (fino a 4 totali), un'uscita relè da 1A e un'uscita opto-isolata.

MTT/AND – Circuito multifunzione che mette in AND due ingressi da 0Vdc a 15Vdc - un'uscita relè da 1A.

DIN BOX – Contenitore plastico protettivo con possibilità di fissaggio su barra DIN

Fabrizio Cugia di Sant'Orsola(*)

Hacking e sicurezza delle reti: quale quadro regolatorio?

Mentre andiamo in stampa non sono ancora noti gli esiti o tantomeno i perimetri d'indagine del procedimento "*Eye-piramid*" sulla centrale di cyberspionaggio attiva a Roma, coinvolta nell'intercettazione sistematica di comunicazioni di personaggi politici e finanziari di alto bordo. Pur essendo chiari i probabili tornaconti del dossieraggio illegale e dell'uso di informazioni riservate nei cenacoli finanziari e politici nostrani, sarebbe piuttosto miope immaginare che una centrale "*degna di un servizio segreto di stato*" - come si legge nell'istruttoria - possa esser stata messa su e gestita per cinque anni da due privati per qualche scalata più rapida ai ranghi della Massoneria (bei tempi, viene da dire, quelli di Guenon, Evola e Garibaldi). Anche perché l'ENAV, la BCE, la Segreteria di stato vaticana, gli Studi legali capitolini e - perché no - l'ambasciata italiana in Messico c'entrano piuttosto poco con biglie nere e bianche, a ben vedere.

(*) Studio Cugia Cuomo e Associati **www.cugiacuomo.it**

È di poco tempo fa la notizia dell'hackeraggio di milioni di dati ed indirizzi email sul portale Yahoo e su siti di dating online. Il tutto a pochi mesi dal fenomeno mondiale dell'estorsione tramite malware Cryptolocker, capace di infettare milioni di PC in ogni parte del pianeta iniettando un dispositivo atto a congelare il sistema centrale, salvo sbrinarlo tramite riscatto in valuta Bitcoin. Per quanto le implicazioni penali dei casi appaiano sostanzialmente diverse, e per ogni giurista valga il brocardo romano "*suum cuique tribuere*", la domanda che sorge è il perimetro regolamentare applicabile, ossia il sistema di norme posto a suggello degli obblighi regolamentari a carico degli operatori di reti di comunicazioni, stabilito in modo inequivoco che ogni attacco cibernetico non può che passare per le reti fisse e mobili di comunicazioni gestite, che costituiscono un servizio pubblico fornito in regime di autorizzazione. La posizione degli operatori di rete in questi casi è, per così dire, ambivalente.

IL PRINCIPIO DI RESPONSABILITÀ

Da un lato sussistono chiari obblighi a loro carico di non discriminazione ed oggettività di condotta, direttamente confliggenti con un principio generale di sorveglianza sull'uso che si voglia fare delle loro reti. Secondo i canoni della net neutrality da ultimo rimarcata dalla FCC americana, i gestori non possono bloccare l'accesso a contenuti leciti, applicazioni o dispositivi non dannosi che circolano sulla Rete, secondo un principio generale di difetto di governance di Internet (*no blocking*, in USA emesso a seguito del caso 2015 *Verizon*). Tanto meno possono ridurre o digradare il traffico Internet per l'accesso a contenuti leciti, applicazioni o dispositivi non dannosi (*no throttling*), proprio nel rispetto della neutralità della Rete. Il che pone a loro carico un chiaro argine (e quindi parallelamente un principio protettivo di responsabilità) sulle verifiche sul contenuto o allegati di un file trasmesso. Sembrerebbe quindi implicitamente che, sempre parlando in termini generali (è ovvio, infatti, che il principio di responsabilità varia anche a seconda del tipo di rete gestita eventualmente sottoposta ad attacco: ad es. è probabile che le reti di accesso ENAV o BCE, ad esempio, siano gestite da operatori in regime di appalto speciale, con ciò che ne dovrebbe conseguire in termini di diligenza nell'adozione di sistemi di protezione da malware), un operatore di rete vada esente da responsabilità, nonostante i reati siano perfezionabili unicamente tramite le infrastrutture gestite. Tuttavia secondo principi generali di diligenza, peraltro applicabili anche in casi analoghi (si pensi, ad es., alle autostrade, dove i difetti di progettazione o di manutenzione stradale comportano possibili correità dei gestori di tali infrastrutture in caso di incidenti tra vetture in transito) la regolamentazione di settore impone specifici obblighi di tenuta e gestione in sicurezza delle reti a carico degli operatori, proprio a tutela dei clienti serviti e dei loro dati. Da tempo la regolamentazione e la giurisprudenza intervenute sul tema (in particolare – paradossalmente - la seconda, ma il tema ci porterebbe assai lontano) equipara Internet ad un servizio di telecomunicazioni al pari dell'offerta di servizi di rete fissa, mobile o larga banda. La Rete non costituisce più, in sintesi, un sistema informativo distinto dalle telecomunicazioni, ed ogni gestore di infrastruttura deve innanzitutto dotarsi di strumenti protettivi a tutela dei servizi prestati e dell'incolumità dei clienti, anche eventualmente per garantire *de minimis* la limitazione di ogni danno possibile.

LE FATTISPECIE

Nel caso della centrale di cyberspionaggio di Roma, l'attività illecita investe due distinte fattispecie, costituite da: i) l'intercettazione illecita di comunicazioni informatiche in modalità sistematica tramite spyware e ii) violazione della privacy ed uso illecito di dati personali. Nel primo caso si ricade nel reato di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.), perpetrato laddove si intercettino fraudolentemente comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi. Salvo che il fatto costituisca più grave reato, la stessa pena si applica laddove si riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni. Nel secondo caso (privacy) le politiche di sicurezza obbligatorie per operatori di comunicazioni comportano anche il rispetto alle disposizione di cui alle direttive del "Pacchetto Telecom" recepite dall'Italia attraverso il D. Lgs. 259/03 e la Direttiva 2002/58/CE, relativa al trattamento dei dati personali e al trattamento della vita privata nel settore delle comunicazioni elettroniche, che riflette le esigen-

ze di tutela dei dati personali, alla luce dell'evoluzione tecnologica delle reti di comunicazione elettronica. Ogni operatore di rete è tenuto in tal senso al rispetto delle disposizioni sulla sicurezza relative al trattamento dei dati personali sensibili e non, sia telefonici sia telematici, ad esempio indicando nel Documento Programmatico sulla Sicurezza ("DPS") *ex* art. 34 e All. B al Decreto Legislativo 30 giugno 2003, n. 196 la situazione attuale in cui si trova sul piano protettivo la propria rete e relativi sistemi di protezione.

GESTIONE SICURA DELLA RETI

Oltre a costituire reati-presupposto ai sensi del D.Lgs. 231/2001, e quindi passibili di forme di responsabilità amministrativa degli operatori di rete in caso di perpetrazione di reati posti in essere nel proprio interesse da posizioni apicali aziendali, tali fattispecie possono quindi essere anche scongiurabili o circoscrivibili anche mediante adozione di modelli gestionali intelligenti di rete. Tra gli obblighi dinamici di "gestione sicura" delle reti operate posti a carico degli operatori possono annoverarsi le disposizioni ISO/IEC in vigore, partendo da 27002:2005 (*Information technology – Security Techniques – Code of Practice for Information Security Management* e ISO 27001:2005, recante "*Information – Security Management System – ISMS)*", per la gestione della sicurezza in generale. Tali misure riguardano anche la tutela dei dati personali degli utenti dei servizi di rete e di connettività erogati, e risultano in linea con le disposizione del Codice per la protezione dei dati personali e delle disposizione del Garante per la protezione dei dati personali indicate a carico degli operatori di comunicazioni. Va infine considerato che tra gli obblighi di *compliance* nella predisposizione e messa in opera di politiche specifiche di protezione risultano anche quelli sul *disaster recovery* (tale è da intendersi un "blocco" del sistema effettuato, ad es., tramite malware Cryptolocker), come specificato nella Raccomandazione del Consiglio dell'OCSE del 25 luglio 2002 ("*Linee Guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione:-verso una cultura della sicurezza*"). Tale Raccomandazione chiaramente individua i seguenti principi a carico delle imprese di rete:

- responsabilità diretta degli operatori per la sicurezza dei sistemi e delle reti;
- principio di valutazione dei rischi (attendibilità, verificabilità, ecc.);
- principio di concezione e applicazione della sicurezza quale elemento essenziale dei sistemi e delle reti d'informazione;
- gestione della sicurezza (anche dinamica con riguardo all'evoluzione del portafoglio servizi e configurazione di reti ed apparati serventi);
- principio della rivalutazione della sicurezza dei sistemi e delle reti d'informazione.

Detti principi sono rinvenibili anche nella Risoluzione delle Nazioni Unite A/RES/58/199 del 23.12.2003 ("*Creation of a global culture of cyber-security and the protection of critical information infrastructures*") e nella Risoluzione del Consiglio UE del 2001 ("*Resolution on Network and information security*"), che sostanzialmente rinviano, quanto all'attuazione pratica, ai principi delle disposizioni ISO citate. La stessa Agenzia europea per la sicurezza informatica e delle reti (ENISA) ha identificato gli obblighi specifici nel documento generale *Network Security Information Exchange*, ("NSIE", del settembre 2009), focalizzato sui temi della sicurezza e della resilienza. Il NSIE ha da tempo indicato i principi relativi alle misure adottabili in tema di protezione e limitazioni di vulnerabilità dai cyber attacchi, estendendo sin dal 29 aprile 2010 una serie di obblighi specifici a carico degli operatori di reti per determinati tipi di servizi offerti (in particolare nel *cloud computing, real time detenction and diagnostincs, wireless networks, sensor networks e supply chain integrity*). Le parti offese potranno quindi riferirsi a tali norme obbligatorie.

Questione di prospettiva

surveye.it

Un problema va osservato da angolazioni diverse per capirne la corretta natura.

Competenza, professionalità e dedizione ci permettono di trovare
la migliore soluzione e garantire un servizio di alto livello.

Sempre al tuo fianco con impianti di:
**VIDEOSORVEGLIANZA, ANTIFURTO, RIVELAZIONE INCENDIO,
CONTROLLO ACCESSI, DOMOTICA, SUPERVISIONE.**

surveye®
FGS Brescia Security System

FGS Brescia s.r.l. Società Unipersonale - via Leonardo da Vinci, 8 - 25010 San Zeno Naviglio (BS)
tel + 39 030 349117 | fax + 39 030 3530932 | marketing@surveye.it

Per Björkdahl(*)

Interoperabilità, sorveglianza e Big Data nelle Smart City

Spesso le amministrazioni cittadine utilizzano sistemi di gestione video o altre piattaforme per visualizzare filmati, proteggere persone e proprietà, analizzare incidenti, valutare il livello di sicurezza urbano e determinare le misure adeguate rispetto ad eventi specifici (disastri naturali, interruzioni nei trasporti o in altri servizi municipali) o altre minacce alla sicurezza pubblica. Per gestire la sicurezza della città vengono anche utilizzati dati provenienti da sistemi antintrusione, controllo accessi, building automation e antincendio, assieme ovviamente alla videosorveglianza.

(*) Presidente dell'ONVIF Steering Committee **www.onvif.org**

Le città che implementano questo approccio "connesso" nei confronti della sicurezza e che utilizzano numerose fonti di dati sono denominate safe city. La maggior parte di esse possiede un'infrastruttura comune ed opera utilizzando sensori e/o telecamere in una rete municipale condivisa. Con l'utilizzo di questi sensori e dei dati sintetizzati provenienti dai numerosi e diversi dispositivi attraverso un'unica interfaccia, i rappresentanti delle istituzioni e delle forze dell'ordine possono disporre di una panoramica completa della sicurezza nelle loro aree di competenza.

LE TANTE FACCE DELLA SAFE CITY

L'integrazione di tutti questi sistemi permette ad un'Amministrazione Comunale di gestire la sicurezza nella sua globalità e da un unico punto di osservazione: il centro di comando. Ci sono però diverse sfide operative tecniche che accompagnano lo sviluppo dei sistemi che assieme danno corpo ad una safe city. L'interoperabilità continua a rappresentare una delle sfide più grandi, specialmente con i sistemi di gestione video, i dispositivi per la registrazione e le telecamere. Lo scenario più frequente è che i Comuni dispongano di diversi sistemi di gestione per il funzionamento della città prodotti da diversi costruttori, ognuno dei quali dotato di interfacce proprietarie per l'integrazione. Per connettere tutti questi sistemi, le Amministrazioni in genere adottano l'approccio "costruire una volta e mantenere all'infinito", anche quando il costo per l'integrazione dei diversi impianti si rende di fatto proibitivo. In un mondo in cui la tecnologia e le caratteristiche dei prodotti cambiano molto rapidamente, si tratta di un approccio poco proficuo: richiede infatti un impegno finanziario importante verso i produttori originari ed impedisce all'utente finale di cercare nuove soluzioni da vendor magari più evoluti, adatti allo scopo o semplicemente convenienti.

STANDARD D'ENTRATA

Ecco perché è utile disporre di standard solidi e ben definiti, in special modo per la videosorveglianza, che è in genere il cuore tecnologico delle safe city, visto che genera una grande quantità di dati. Gli standard, come quelli di ONVIF, offrono un link comune fra i diversi componenti di questi sistemi. Progettata specificamente per superare le sfide tipiche di ambienti multi-vendor, l'interfaccia comune di ONVIF semplifica la comunicazione tra le tecnologie di diversi produttori e promuove un ambiente interoperabile in cui i componenti del sistema si possono utilizzare in maniera intercambiabile, purché i dispositivi siano conformi alle specifiche ONVIF. Immaginiamo questo scenario: in un ambiente tecnologico multimarca le autorità spesso ricevono materiale video esportato in una moltitudine di formati e con una moltitudine di registratori per rivedere i filmati. Qui un approccio standardizzato – come quello ipotizzato dalle specifiche ONVIF - sia per il formato dei file che per i registratori associati aumenterebbe l'efficienza del processo ed aggiungerebbe la possibilità di includere metadati nei materiali esportati e nei report, tali da determinare, ad esempio, ora e luogo esatti dell'incidente registrato. ONVIF ha rilasciato una specifica che definisce un formato di file univoco per un'esportazione efficace del materiale registrato e ad uso forense. L'insieme di queste specifiche non solo rende possibile l'integrazione dei dispositivi in un sistema di sicurezza multimarca realizzato per contesti di safe city, ma offre anche un formato efficace per l'esportazione di file, che può velocizzare un'indagine post-evento quando le autorità stiano cercando di reagire il più velocemente possibile per identificare dei sospetti o diffondere informazioni.

CASI CONCRETI

Nel 2014, l'azienda appartenente ad ONVIF Meyertech ha aiutato la città di York (U.K.) a realizzare una soluzione safe city per gli spazi pubblici e il sistema dei trasporti. Usare un software di gestione video e delle informazioni Meyertech ha permesso alla città di integrare le telecamere IP con i tanti sistemi preesistenti nel centro di comando York Travel and Control Centre. La centrale di controllo della città monitora oltre 150 telecamere di diversi produttori dislocate in città e le istituzioni affermano che il nuovo sistema ha avuto un impatto immediato sui tassi di criminalità. L'integrazione di telecamere preesistenti e IP con un nuovo VMS, che si interfaccia con il software di gestione informazioni, è stato possibile grazie alla specifica video di ONVIF. Un altro membro ONVIF, Huawei, è considerato leader nelle soluzioni smart city. Huawei ha realizzato soluzioni smart city a Nairobi, Kenya, e nelle città cinesi di Nanjing e Shanghai. Il sistema di gestione video di Huawei è stato utilizzato nel progetto di Shanghai come parte integrante dell'iniziativa della costruzione di safe cities del Ministero Cinese per

la Sicurezza Pubblica. Una sfida importante del progetto è stata integrare nuove e vecchie tecnologie. Il VMS di Huawei ha utilizzato ONVIF per integrare le telecamere di produttori quali Dahua, Haikang, AXIS, SONY e altri.

UNO STANDARD MULTIDISCIPLINARE?

Nel futuro, ONVIF vede tutti i sistemi di sicurezza fisica adottare le stesse interfacce per l'interoperabilità, pertanto si sta adoperando per semplificare il lavoro dei membri nello sviluppo di uno standard multidisciplinare. Tale interfaccia omnicomprensiva potrebbe fornire un approccio esaustivo al tema dell'interoperabilità, coinvolgendo tutti gli elementi chiave (videosorveglianza, controllo accessi e altre operazioni essenziali) per un centro di comando di una safe city. Dal momento che la realizzazione della safe city e il concetto di Internet of Things operano sugli stessi principi che prevedono di connettere diversi sistemi e dispositivi, uno standard multidisciplinare per la sicurezza fisica giocherebbe un ruolo di rilievo nell'ulteriore sviluppo dell'Internet of Things. Molti all'interno dell'industria considerano gli standard un elemento importante sia per le safe city che per l'IoT. L'IEEE (Institute of Electrical and Electronics Engineers) sta già lavorando su standard IoT per le industrie tecnologiche e alcuni prevedono addirittura che potremmo vedere l'introduzione di standard globali per l'IoT entro la fine di quest'anno. Dalla predisposizione di standard minimi di interoperabilità si passerà quindi col tempo alla definizione di uno standard multidisciplinare per la sicurezza fisica perché elaborare sistemi multidisciplinari proprietari avrà sempre meno significato. L'industria non è certamente ancora a questo punto di maturazione, ma uno standard multidisciplinare per la sicurezza fisica si intravvede già all'orizzonte.

HIKVISION

DS-2XE6222F-IS
EXPLOSION-PROOF SPEED DOME
DS-2DF6223-CX(W)
EXPLOSION-PROOF BULLET CAMERA

INDUSTRIAL

INDISTRUTTIBILE SICUREZZA PER AMBIENTI ESTREMI

Le telecamere explosion-proof di Hikvision utilizzano custodie in acciaio inox 304 e 316L che garantiscono la massima resistenza verso i rischi di corrosione ed esplosione, e sono certificate IP68 contro la possibile penetrazione di agenti dannosi quali acqua e polvere. Ideali per applicazioni di sorveglianza in tutti gli ambienti ad alto rischio, ove si impongono le massime performance video anche in presenza di materiali pericolosi o corrosivi, come negli impianti di estrazione di gas e petroli, nell'industria chimica e mineraria, in ambienti marini o altamente salini.

- Full HD 1080p
- Ultra Low Light fino a 0.005 Lux
- Sensore CMOS a Scansione Progressiva 2MP
- WDR 120dB
- H.265+ Smart codec
- Funzioni di analisi video Smart 2.0
- Custodie in acciaio inox 304 e 316L
- IP68

smart 2.0

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

Filiale Milano
Viale Fulvio Testi 113
20092 Cinisello Balsamo, MI
T +39 02 92886311
F +39 02 92886399

Filiale Roma
Via Pontina 573
00128 Roma
T +39 06 94538790
F +39 06 94538791

Filiale Bologna
Via G. Fattori 4
40033 Casalecchio di Reno, BO
T +39 051 0393670
F +39 051 0393671

www.hikvision.com
info.it@hikvision.com

Manuela Delbono(*)

Sicurezza: il solo prezzo d'acquisto non è il vero costo del sistema

La situazione economica in cui versiamo ormai da tempo ha accentuato una tendenza già purtroppo presente in molti mercati, sicurezza inclusa: l'attenzione al prezzo. Oggi il mercato sembra avere totalmente smarrito il senso del *valore* di un bene per concentrarsi unicamente sul costo. Del resto, quante volte mentre noi stessi acquistiamo qualcosa, ci soffermiamo esclusivamente sul cartellino? Ma il punto è: siamo davvero sicuri di aver ottenuto il meglio acquistando al minor prezzo?

(*) Ufficio Marketing Surveye **www.surveye.it**

In ambito security questa domanda deve far particolarmente riflettere: un prodotto che, per competere sul mercato, punta tutto sul prezzo, è davvero in grado di mantenere quella qualità che un settore sensibile come la sicurezza esige? E chi acquista, è davvero sicuro di poter poi beneficiare della convenienza ostentata sventolando un prezzo più basso? Ebbene, il risultato il più delle volte è realmente sconcertante, soprattutto se analizziamo in profondità tutte le variabili in gioco.

LE VARIABILI IN GIOCO

Il processo d'acquisto si apre con una fase decisionale, nella quale non possono essere trascurati: qualità del prodotto; funzionalità operative che nel lungo periodo fanno risparmiare tempo e denaro; costi indiretti e intangibili; costi di riparazione e manutenzione del sistema; disservizi di un sistema inagibile che in ultima sede gravano sul cliente finale. La somma di queste considerazioni ci consente di affermare che un prezzo di acquisto più basso non è per sua natura sinonimo di valore a lungo termine o di migliore ritorno sugli investimenti. Come dunque quantificare ed individuare correttamente i costi diretti e indiretti in un sistema di sicurezza nell'arco del suo intero ciclo di vita? Un'analisi attenta ci porta a catalogare l'ordine cronologico delle varie attività che compaiono durante il ciclo di vita del sistema: dal suo acquisto all'utilizzo, fino alla sua disinstallazione. Se l'acquisto e la disinstallazione sono costi individuabili, non lo sono invece altrettanto quelli che, pur strettamente legati all'utilizzo, ricorrono tuttavia durante tutto il ciclo di vita. Questi ultimi costi sono infatti variabili e spesso sottovalutati, finendo non di rado col pesare in modo non indifferente sull'economia del sistema.

COSTI PREVEDIBILI E COSTI VARIABILI

Quando acquistiamo un sistema, alcuni costi sono facilmente prevedibili e quantificabili e vengono catalogati normalmente come costi del primo anno (con garanzia a copertura): hardware, software, installazione, integrazione. Nel dettaglio sono così riassumibili: progettazione; scelta dei materiali hardware/software; installazione e configurazione; collaudo; logistica; formazione; documentazione; oneri di sicurezza. Prevedibili sono anche i costi di smantellamento, che rappresentano una piccola quota del totale ma che possono essere significativi soprattutto se calcolati su investimenti. Ci si riferisce a costi per disinstallazione, smaltimento e documentazione.

Sono quindi le variabili post-installative, fuori garanzia, ricorrenti e spesso trascurate dagli acquirenti, che pesano in modo esponenziale sul lungo periodo nell'economia della commessa. Questo è dovuto ai guasti tipici durante il ciclo di vita dei prodotti e ai relativi costi per la sostituzione, che aumentano con il passare del tempo. Oltre a ciò, vanno considerate anche la qualità dei prodotti, con conseguenze ovvie sui costi a lungo termine, e le funzionalità e/o tecnologie specifiche necessarie. Altri fattori molto importanti sono inoltre la dimensione del progetto, l'applicazione nel settore, i requisiti di sistema ed altri attributi imprevedibili. Aspetti così riassumibili: manutenzione ordinaria e straordinaria; guasti; assistenza; aggiornamenti; integrazione/dimensione del sistema; formazione di nuovo personale; costi di esercizi (tipo corrente elettrica...). Comprendere tutte queste dinamiche aiuta a prendere decisioni oculate, considerando anche i costi nascosti e diretti, dalla consegna allo smantellamento. Conoscere e prendere in considerazione l'insieme di queste variabili significa, in definitiva, saper percepire il reale valore di un sistema di sicurezza. L'elemento critico per la decisione di acquisto è infatti rappresentato dalla percezione soggettiva che il cliente ha del costo. Oggi la tendenza del mercato ci porta a non riflettere sul valore che un prodotto può avere, dando invece troppa importanza al prezzo. Possiamo così dividere i clienti in due categorie: coloro che "comprano il prezzo" e quanti invece "comprano il prodotto". Sono questi ultimi quelli che cercano la soddisfazione di un insieme di benefici per loro importanti: sono quelli che valutano che le diverse offerte presenti sul mercato li soddisfano in modo differenziato, e sono quelli naturalmente disponibili a pagare un prezzo adeguato per ottenere i loro obiettivi. Sono questi ultimi che capiscono il perché un sistema di sicurezza non può essere acquistato solo per il prezzo.

Security FORUM

International Security Conference & Exhibition

CCIB
Centro de Convenciones Internacional de Barcelona

17 e 18 de maggio
BCN2017

VEDERE PER CREARE

#SFBCN2017

www.securityforum.es
info@securityforum.es
+34 914 768 000
@SecurityForumES

Peldaño

SORVEGLIA E PROTEGGE

SISTEMI SPECIALI DI SICUREZZA.

INSTALLAZIONE E ASSISTENZA H24 · GESTIONE ALLARMI · PRONTO INTERVENTO

SECURITYTRUST.IT

Security Trust

Giovanni Villarosa(*)

Proteggere il perimetro: sfide e tecnologie

La sicurezza fisica, nel suo insieme, comprende quel complesso di misure che consentono di prevenire e/o dissuadere l'accesso fraudolento all'interno di "strutture", siano esse *fisiche* (edifici, siti, etc) oppure *digitali* (server, dati, etc): si pensi, ad esempio, alla prevenzione da illecite *intrusioni logiche* ad un sistema informatico; oppure all'*intrusione fisica* di un sito ad alto rischio nucleare. Recinzioni, muri, tecniche di rivelazione intelligenti e misure di *sorveglianza elettronica*, rappresentano l'insieme delle possibilità per proteggere integralmente una infrastruttura dalle intrusione esterne; e questo perché è complessa la sicurezza richiesta in particolari infrastrutture: un aeroporto, un carcere, una centrale elettrica. Ma proprio come non basta solo porre un mattone (le tecnologie) sopra l'altro per costruire un muro (le difese), anche la protezione perimetrale richiede un buon "cemento" (i professionisti) che possa consolidare il risultato.

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

Questa *"coesione"* è rappresentata dall'installatore, dal progettista, dai professionisti nel loro insieme, che sinergicamente attuano attente pianificazioni, progetti pertinenti, avendo sempre chiari tutti gli scenari operativi sui quali operare: un'estesa area industriale richiede una protezione ben diversa da quella di un'azienda di piccole dimensioni; la giusta progettazione di una protezione fisica integrata deve rispondere, in maniera lineare, alla sua basica missione: prevenire l'evento in funzione dei molteplici scenari di minaccia.

Non dimentichiamoci mai questo assunto: la sicurezza è un sentimento, oltre che un dato di fatto! E poiché il senso di sicurezza può essere un sentimento molto soggettivo, beh allora il professionista deve sempre analizzare attentamente il punto di inizio da cui partire: l'analisi dei rischi.

Ogni bene, nel sue insieme, ha le proprie peculiarità, ed è in un certo senso "predestinato" a subire nel tempo determinati tipi di minacce, di attacchi, o semplicemente esposto all'azione criminale. Per questo motivo, l'analisi delle tipologie delle minacce alle quali potrebbe essere esposto l'edificio, l'infrastruttura, o tutti quei beni *"tangibili e intangibili",* come pure i profili dei potenziali attaccanti, rappresenta il primo e insostituibile atto che il professionista deve predisporre analizzando tutti i fattori di possibile rischio aziendale, ad esempio: quali sono i possibili scenari di minaccia? Chi sono e quali sono le finalità degli attaccanti? Come è strutturata l'azienda? Come è configurato il perimetro esterno? Quali e quale sicurezza hanno le protezioni fisiche passive? E' bene tenere sempre presente che la minaccia può derivare da due possibili scenari: da un lato troveremo tutte quelle azioni criminali mirate ai sabotaggi, aggressioni, effrazioni, furti o spionaggio; dall'altro tutte quelle azioni criminali non propriamente mirate, come gli atti vandalici, teppismo o violenze di matrice politica. Le risultanze di ciò rappresentano i danni presumibili, il potenziale di rischio, e pertanto si possono già prevedere gli obiettivi da proteggere e i punti nevralgici da sorvegliare più attentamente.

PROTEGGERE IL PERIMETRO

Già da questa prima analisi di rischio si possono dedurre le possibili misure di protezione attiva. Un professionista, installatore o progettista che sia, deve sempre ricordare questa semplicissima equazione: un bene è ben protetto solo se la durata della resistenza di una misura di protezione (passiva e/o attiva) è uguale o superiore al tempo di reazione necessario per l'intervento finale di verifica sui luoghi, da parte del personale di sorveglianza aziendale o degli organi di polizia.

Proteggere il perimetro di "aree sensibili" comporta l'impiego di tecnologie (sensori) atte a rilevare la violazione delle aree protette la cui affidabilità e capacità di rilevazione sia elevata; se consideriamo il perimetro esterno di una qualsiasi struttura, certamente sarà in qualche modo delimitato da "architetture" fisiche, siano esse recinzioni metalliche, cancellate o muri perimetrali; tutti questi elementi strutturali rappresentano *passivamente* il *"primo anello di sicurezza perimetrale"*, che l'infrastruttura possiede per "*default",* il più delle volte realizzate non con criteri imposti dalle regole proprie della sicurezza, ma da precisi e insormontabili obblighi e vincoli urbanistici: su questo, anzi da questo partirà il professionista, per poi realizzare la futura protezione perimetrale *"attiva"*.

Come detto, oltre a indicare i confini della proprietà, l'obiettivo delle misure di sicurezza passive consiste nell'impedire l'intrusione o gli spostamenti all'interno dei settori protetti. In molti casi, elementi naturali come fossati e terrapieni, siepi, fossi d'acqua o zone paludose, offrono già una buona protezione perimetrale *naturale*. Non bisogna comunque dimenticare che la *protezione meccanica* deve essere garantita con qualsiasi condizione meteorologica: il primo passo è, infatti, la progettazione e la realizzazione di dispositivi di protezione fisica passiva adeguati e durevoli.

Proteggere un perimetro aziendale, pubblico o privato che sia, richiede sistemi di rivelazione tanto reattivi, quanto precisi e affidabili; saper utilizzare questi sistemi presuppone, per converso, installatori e progettisti altamente preparati, skillati professionalmente. L'elettronica dedicata alla moderna sensoristica per l'antintrusione perimetrale è concepita per segnalare i tentativi di accesso non autorizzato con il massimo anticipo, ancora prima che l'intruso penetri nell'area protetta, traendone un vantaggio duplice: da un lato, questi sistemi rappresentano un importante fattore deterrente, scoraggiando sul nascere la maggior parte dei tentativi di intrusione; dall'altro lato, forniscono più tempo per intraprendere le necessarie azioni e reazioni di difesa. La rilevazione elettronica antintrusione diventa perciò

parte integrante con la struttura fisica; per la sensoristica l'adattabilità è la chiave di tutto per attuare una sorveglianza elettronica puntuale, efficiente ed efficace. Esistono diverse tecnologie perimetrali adatte allo scopo: si va dall'impiego di fibre ottiche ai cavi microfonici, dalle barriere ad infrarossi o microonde fino ad arrivare all'impiego più specializzato di sensori dedicati, che applicati alle recinzioni hanno la capacità *logica* di rilevare, e di discriminare in modo efficace, i tentativi di taglio, arrampicamento e sfondamento della recinzione stessa.

ALLARMI IMPROPRI

In linea generale è molto facile rilevare un'intrusione, quello che è difficile è rilevare soltanto l'intrusione. Ed questa la vera sfida tecnologica dei produttori di sensori perimetrali dalle alte prestazioni, perché è proprio su questo terreno che si confrontano tecnologie e scelte produttive. I professionisti che realizzano i sistemi perimetrali di sicurezza, invece, sanno che devono costantemente confrontarsi con una serie di problematiche di carattere ambientale: i cosiddetti *falsi allarmi o allarmi impropri* e devono essere in grado di poterli contrastare. Come? Un sensore cosa deve rilevare? Sul controllo di una recinzione è necessario rilevare e discriminare tre diverse tipologie di attacco: il taglio, l'arrampicamento e lo sfondamento del perimetro. Ad esempio, esaminiamo il più impegnativo, il taglio della recinzione, che viene generalmente eseguito con normali tronchesine, utensili facili da trasportare e occultare, e dove bastano pochi tagli per aprirsi un varco. Una tipologia di attacco molto insidiosa e fastidiosa, difficile da *"trattare"*, perché induce segnali di bassa intensità, complessi da processare; ora, indipendentemente dalla tecnologia implementata alla sensoristica, questi segnali generati non sono dissimili dai disturbi ambientali naturali, anzi, ma facilmente captabili dai sensori come: *"inganno",* falso allarme, allarme improprio, perché proprio la minima oscillazione della recinzione, una dilatazione termica, la pioggia, il vento, il movimento di vegetazione, etc., generano nel loro insieme, diversi segnali di disturbo. Ebbene il taglio è molto simile a gran parte di questi disturbi, ecco perché diventa difficile distinguere un taglio della recinzione dai naturali disturbi ambientali. Un efficace e efficiente sistema di protezione perimetrale deve essere progettato e realizzato tenendo in debita considerazione questa variabile primaria, che potrebbe sommarsi, negativamente, a scelte poco professionali da parte degli installatori e progettisti.

ELKRON
EGON

IL NUOVO SISTEMA ANTINTRUSIONE WIRELESS CON NOTIFICA VIDEO

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

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

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

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

Disponibile su iTunes

DISPONIBILE SU Google Play

elkron.it

ELKRON

La Redazione

C'era una volta il sensore: dal PIR al laser

"Mamma, cos'è quell'affare bianco appeso all'angolo della mia stanza?"
"Fa parte del nostro sistema d'allarme: avvisa mamma e papà se in casa c'è un movimento"...Davvero? E' tutto qui? In realtà dietro a un concetto così semplice si nascondono una quantità di innovazioni tecnologiche che consentono oggi applicativi e soluzioni ben più "high-tech" di quanto l'utente possa immaginare. E la corsa continua tuttora con l'integrazione della tecnologia laser, che offre a questi sensori un potenziale... *a prova di futuro*.

Il primo grande cambiamento che ha investito i sensori infrarossi passivi PIR (Passive Infrared Sensors) è stata l'adozione della tecnologia digitale. Rispetto ai sensori analogici, nuove funzioni e complessità si sono aggiunte all'equazione a tradizionale risposta binaria sì/no (sì – il sensore rileva un movimento e scatta l'allarme; no – nessuna rilevazione, si proceda con il monitoraggio ambientale). I sensori digitali sono oggi invece in grado di individuare le diverse fonti di calore (split o termosifoni) e di riconoscere che una mosca non è una potenziale minaccia alla sicurezza dell'ambiente, mentre un uomo sì. Determinando se un oggetto rilevato possa essere o meno fonte di pericolo, si minimizza anche la percentuale di potenziali falsi allarmi.

MICROPROCESSORI NEI SENSORI

Ma bilanciare correttamente l'accuratezza della rilevazione e la riduzione degli allarmi impropri è un equilibrio difficile da raggiungere ed è potenziale fonte di conseguenze anche drastiche se viene mal gestito: se però tale equilibrio si raggiunge in maniera efficace, allora è in grado di portare davvero grandi benefici agli utenti finali.
Con questa finalità I microprocessori sono stati incorporati nei sensori di rilevazione antintrusione: servono a quantificare digitalmente la frequenza del segnale ed essenzialmente operano come "banca dati" per un ampio raggio di scenari prima di alimentare quell'intelligenza che occorre al sensore per determinare correttamente ciò che rappresenta – o non rappresenta – una potenziale minaccia di sicurezza. L'ispirazione è venuta dai sensori per esterni: lì i microprocessori hanno dimostrato di saper operare con grande efficacia per discriminare gli effetti ambientali, meteorologici, il fruscio della vegetazione dovuta al vento, gli animali vaganti, etc. Così la tecnologia a microprocessore è stata portata anche nei sensori per interno.
I PIR per interni sembrano uguali ai sensori digitali tradizionali, invece I relé output sono completamente silenziosi: quando vengono allarmati, il sistema non produce alcun suono per evitare che I soggetti da proteggere possano inquietarsi.

CONNETTIVITÀ

Ora che I benefici della tecnologia digitale sono assodati e consolidati anche per il lungo periodo, quale direzione prenderà l'evoluzione tencologica dei sensori? La parola d'ordine sembra essere Connettività. Una prima opzione si può ravvisare nell'integrazione con un ampio raggio di impianti dedicati al "sistema casa": soluzioni di buil-

Dai PIR analogici all'IoT: in che direzione si sta evolvendo lo sviluppo tecnologico per la sensoristica?

Risponde Mark Cosgrave, European Sales Manager OPTEX

In un mondo ormai integralmente connesso, dove ogni singolo oggetto e device risulta ormai integrato e collegato e dove temi come l'Internet of Things dominano il dibattito sullo scenario tecnologico del futuro prossimo, i sensori rivestono un ruolo di particolare importanza. Sono infatti i primi tasselli del mosaico perché rappresentano i primi elementi di attivazione di ciascun allarme.
I sensori continueranno quindi ad evolversi attraverso partnership tecnologiche sempre più complesse, diventando elementi e parti di soluzioni sempre più ampie e complesse per la home automation, ma anche per la creazione di edifici sempre più smart e città sempre più smart. E ovviamente anche per applicazioni di security e, sempre più spesso, di safety.
La tecnologia di rilevazione ha fatto enormi passi avanti rispetto ai primi PIR analogici sul mercato: se c'è una certezza nel prossimo orizzonte tecnologico, è che i sensori continueranno a svilupparsi e ad evolvere.

www.optex-europe.com

ding management, automazioni, gestione delle persone anziane e di fasce deboli, controllo degli accessi. Tutto questo a condizione che l'integrazione sia semplice e immediata: in questo modo gli utilizzatori ne trarrebbero evidenti benefici (il sensore potrebbe, tanto per fare un esempio, essere collegato ad una telecamera: tramite app si potrebbe notificare ai genitori quando I figli rientrano a casa, etc). Questi sensori di nuova generazione potrebbero inoltre aiutare a ridurre l'impronta familiare di carbonio con l'accensione delle luci esclusivamente quando viene rilevata la presenza umana.

I SENSORI LASER

Se per I sensori PIR si è ormai raggiunto l'apice dell'evoluzione tecnologica, quanto meno nel breve termine, nuovi sviluppi si profilano invece all'orizzonte di altre tecniche di rilevazione. Una di queste tecnologie è il time of flight ("tempo di volo") usato negli scanner laser o sensori che consistono di un illuminatore infrarosso e una telecamera. La tecnologia "time of flight" misura la fase di tempo tra l'emissione di una luce all'infrarosso o di un raggio laser e la riflessione di quello stesso raggio contro il sensore. Ogni oggetto che si incontrerà nell'area di rilevazione restituirà il segnale indietro al sensore, consentendo quindi una mappatura della scena particolarmente accurata. Questa tecnologia, che non dipende da nessuna fonte di luce, può essere utilizzata per una moltitudine di applicazioni.

APPLICAZIONI

I sensori laser sviluppati sulla tecnologia time of flight presentano degli algoritmi sofisticati e una configurazione personalizzabile del software, che consente agli utilizzatori di definire l'area di rilevazione e le zone e di identificare dimensioni, velocità e distanza degli oggetti all'interno di una scena. Il laser può anche adattarsi ad un ambiente con modifiche successive (terreno irregolare, accumularsi di neve o fogliame, etc) ed essere configurato per rilevare - oppure ignorare - oggetti di dimensioni predefinite. Il sensore laser si può quindi adattare ad una grande varietà di applicazioni: può ad esempio allarmarsi solo in presenza di soggetti di dimensioni pseudo-umane e, magari, ignorare oggetti di dimensione veicolare (o viceversa); nelle gallerie d'arte l'algoritmo può essere configurato per rilevare ad esempio delle mani che si avvicinino troppo a dipinti o altre opere d'arte.
E le applicazioni superano la sfera di operatività della sola security per abbracciare anche la safety. I sensori laser sono ad esempio parte di un'importante soluzione su scala nazionale volta ad individuare eventuali persone intrappolate nei passaggi a livello: I sensori sono direttamente collegati al sistema di segnalazione, che in caso di attraversamento non del tutto sicuro, blocca in automatico il treno in arrivo. Ancora: I sensori laser sono stati testati con successo per rilevare chi intende gettarsi sotto a treni e metropolitane. La tecnologia "time of flight" consente inoltre di sviluppare sensori dotati di illuminatore infrarosso e di receiver, che possono mappare la scena in 3D ricreando forme e dimensioni di tutti gli oggetti rilevati ed individuando, ad esempio, se in una camera di compensazione sono presenti una o due persone, o se qualcuno sta trainando un trolley o spostando un oggetto. Un'applicazione particolarmente utile, quest'ultima, per proteggere aree di alta sicurezza e rilevare l'introduzione di oggetti non consentiti in aree riservate o sigillate.

riscogroup.it

RISCO GROUP

ProSYS™ Plus

Una singola piattaforma per tutte le applicazioni

ProSYS™ Plus di RISCO Group: il nuovo Sistema di Sicurezza Ibrido Grado 3 sviluppato per grandi progetti commerciali.

- **Espandibile:** fino a 512 zone
- **L'architettura "Super Ibrida"** utilizza le piu avanzate tecnologie di comunicazione come multisocket IP, 3G e WiFi
- **Un rivoluzionario Sistema di Licenze:** si acquistano solo quelle necessarie per una gestione efficiente e puntuale dei costi.
- Gestione da remoto con l'applicazione, **basata sul Cloud** per smartphone
- Compatibile con **l'intera gamma** di rivelatori commerciali e industriali
- **Telecamere IP integrate** con il sistema di sicurezza per la video verifica live in HD
- **Completamente integrato** con il software di supervisione SynopSYS Integrated Security&Building Management™

Per maggiori informazioni visitate il sito **www.riscogroup.it**

RISCO Group S.R.L | Via Robecco, 91 – Cinisello Balsamo (MI)

App Store Facebook

Play Store iRISCO

La Redazione

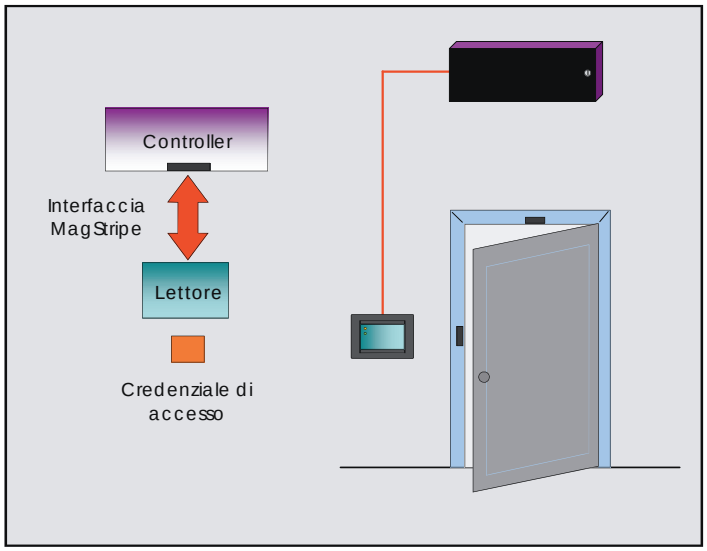
Controllo accessi: l'interfaccia Magstripe

Insieme a Wiegand, MagStripe è una delle interfacce (fisiche e logiche) più diffuse per far comunicare tra loro un'unità elettronica di controllo accessi (Controller) e i propri lettori di credenziali. Nata negli anni Settanta insieme alle card con banda magnetica, occupa ancora oggi il posto più alto del podio in fatto di sistemi di connessione. Com'è fatta e come funziona? E perché è così poco amata? Nel precedente numero di a&s Italy abbiamo esplorato il mondo Wiegand e dintorni; ora è la volta di quello MagStripe.

I tecnici, si dice, la preferiscono Wiegand. Chi progetta e produce sistemi elettronici di controllo accessi ritiene (e a ragione) che sia questa l'interfaccia più semplice ed economica per far comunicare tra loro un Controller con i rispettivi lettori di credenziali (cfr a&s Italy n. 42/2016). I tecnici, tuttavia, sanno bene che, in questo campo, a farla da padrona non è l'interfaccia Wiegand bensì un'altra "vecchia signora" delle connessioni punto a punto: la MagStripe. L'interfaccia MagStripe – forma contratta di "magnetic stripe" – nasce ufficialmente nel novembre del 1974 insieme alle carte magnetiche e ai relativi lettori a opera della American Magnetics Corporation, che nel 1987 ne registrò il nome (trademark poi cancellato nel 2008). All'origine, questo tipo di interfaccia era esclusivamente riservata ai lettori di carte con banda magnetica (a scorrimento, a inserimento, motorizzati ecc.). Col passare del tempo, visti il successo e la diffusione a livello globale, la stessa interfaccia ha finito con l'essere adottata (in emulazione) dalla maggior parte dei produttori di lettori che sfruttano anche altre tecniche di riconoscimento (PIN, carte e transponder RFId, impronte biometriche ecc.). Rispetto alla sua coetanea Wiegand, è molto più complicata da gestire ma decisamente più potente e sicura, oltre che standardizzata. Per non far torto a nessuno, gran parte dei lettori (e dei Controller) di qualità disponibili in commercio integrano entrambi i tipi di interfacce.

L'INTERFACCIA BALLERINA

Per comprendere come funziona l'interfaccia MagStripe occorre innanzitutto rifarsi alla tecnica e alla normativa ISO/IEC, con cui vengono registrate e lette le carte di identificazione e di pagamento dotate di banda magnetica. Essa, infatti, nella versione originale, altro non è che l'*output* del circuito elettronico, integrato nel lettore, che decodifica le inversioni di flusso registrate su una delle tracce e captate dalla testina, secondo lo standard F2F (registrazione a doppia frequenza a coerenza di fase). Questo tipo di interfaccia prevede, a livello fisico, tre segnali: *Card Present*, *Clock* e *Data*. *Card Present* (in breve CP o RCP) è, in pratica, un segnale di "lettura in corso" della traccia magnetica nella quale sono stati registrati i dati. Normalmente a uno, va a zero dopo che viene rilevato un congruo numero di inversioni di flusso (generalmente non inferiore a cinque e non superiore a 15) e ritorna a uno dopo un certo tempo

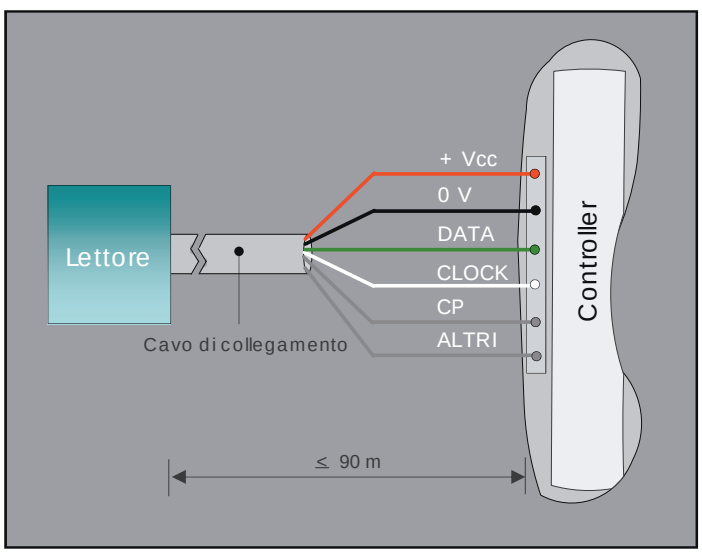


MagStripe è un'interfaccia di comunicazione (logica e fisica) tra il lettore di credenziali (tipicamente di card con banda magnetica) e la rispettiva unità di controllo accessi (Controller). Insieme alla Wiegand è il tipo di connessione punto a punto più diffusa. © a&s Italy All rights reserved

Negli ultimi trenta anni del secolo scorso, ogni lettore di carte magnetiche (stand alone o integrato in altre apparecchiature) prevedeva un'interfaccia MagStripe.

Valore Hex	Valore Bin	Carattere
0	1 0000	0
1	0 0001	1
2	0 0010	2
3	1 0011	3
4	0 0100	4
5	1 0101	5
6	1 0110	6
7	0 0111	7
8	0 1000	8
9	1 1001	9
A	1 1010	Riservato
B	0 1011	SS (Start Sentinel)
C	1 1100	Riservato
D	0 1101	Separatore
E	0 1110	Riservato
F	1 1111	ES (End Sentinel)

Nell'interfaccia MagStripe classica i caratteri sono solo numerici espressi su 5 bit (4 di dato e 1 di parità dispari). I caratteri Hex B ed F sono di controllo (inizio e fine testo) mentre l'Hex D è usato raramente come separatore di campi. © a&s Italy All rights reserved



La classica connessione MagStripe tra il lettore di credenziali e il Controller per accessi comprende due fili di alimentazione (0 V e +Vcc) e tre di segnali (CP, Clock e Data). Altri conduttori sono usati per pilotare i led e il beeper e per rilevare l'eventuale manomissione o rimozione del lettore. © a&s Italy All rights reserved

che è stata rilevata l'ultima inversione sulla traccia (di solito non inferiore a 5 ms e non superiore a 150 ms). *Clock* (CK, CLK o RCK), chiamato anche *Strobe*, è un'altra uscita del codificatore F2F (segnale di sincronismo) che indica (sul fronte di discesa) la presenza di un bit valido. La durata del ciclo dipende dalla densità di registrazione e dalla velocità di lettura (tipicamente è pari al 25-50% della durata del bit). *Data* (o RD) rappresenta il valore del bit (zero se il segnale è alto, uno se basso). Il valore è valido a decorrere da una frazione di tempo prima del fronte di discesa del clock (almeno 1 µs) e rimane stabile per tutto lo strobe stesso. Anche in questo caso, la durata del segnale dipende dalla densità di registrazione e dalla velocità di lettura (tra 80,63 µs e 3,39 ms).

COME FUNZIONA

Il modo di funzionamento dell'interfaccia MagStripe si può sintetizzare come segue. Al momento in cui inizia la lettura di una traccia registrata, il segnale CP va a zero. Segue un treno di impulsi sul segnale CK (uno per ogni bit letto). Sul fronte di discesa di ciascun clock viene acquisito il bit (zero o uno) disponibile sul segnale Data. I bit, opportunamente raggruppati, costituiscono i caratteri del testo. Al momento in cui terminano le inversioni di flusso sulla traccia, il segnale CP ritorna a uno (fine ciclo). Nell'interfaccia Wiegand, i segnali hanno una temporizzazione stabile. In quella MagStripe, invece, "ballano" in continuazione (ora più corti ora più lunghi) in base alla densità con la quale sono registrati i bit nella traccia magnetica (75 o 210 bpi) e alla velocità di lettura (tipicamente compresa tra 10 e 150 cm/s). Oltre ai tre conduttori principali (CP, CK e Data), a completare l'interfaccia elettrica sono previsti altri conduttori: 0 Volt (polo negativo dell'alimentazione e massa di riferimento dei segnali), Vcc (polo positivo, a 5 o 12 V), pilotaggio del led per segnalare l'avvenuta lettura o l'autorizzazione ad accedere, comando del dispositivo acustico (beeper), eventuale segnale di effrazione o rimozione del lettore ecc, A differenza della connessione Wiegand, l'abbinamento segnale-colore del filo non è standardizzato. L'alimentazione è comunque sempre contraddistinta dai colori nero (0 Volt) e rosso (+ Vcc), CK e Data viaggiano spesso i conduttori verde e bianco (Data0 e Data1 nell'interfaccia Wiegand) mentre l'abbinamento degli altri segnali è libero. La distanza massima per collegare il lettore al rispettivo Controller è in funzione dei driver di

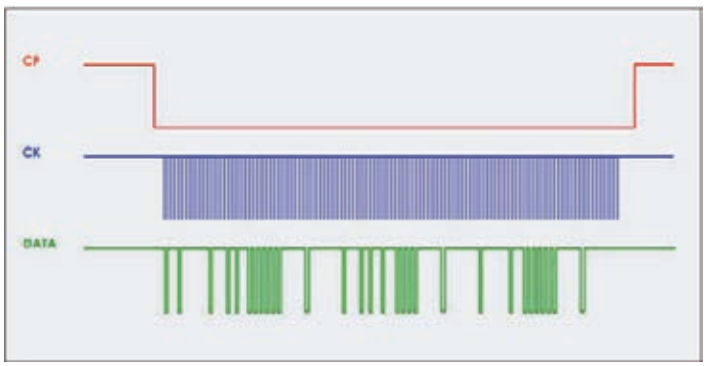
linea integrati nel lettore stesso e va da poche decine di centimetri a 150 metri; quella consolidata è di 90 metri.

LE REGOLE DEL TESTO

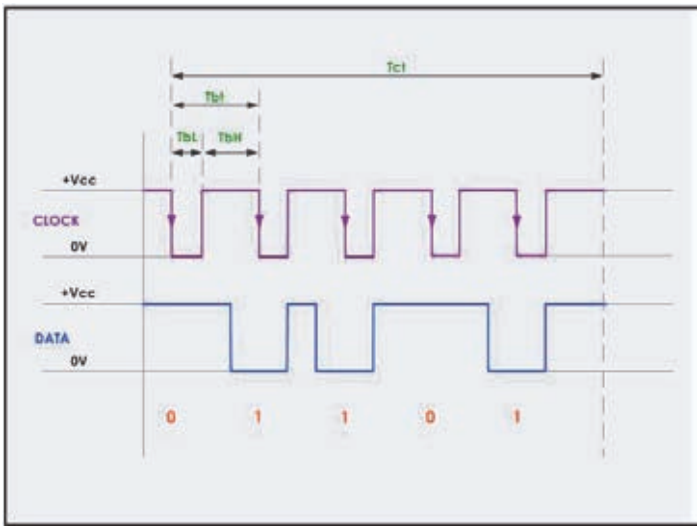
Il formato del testo trasmesso attraverso un'interfaccia MagStripe è regolato dallo standard ISO/IEC 7811; la lunghezza non può eccedere il numero massimo di caratteri previsto da ciascuna traccia magnetica secondo lo stesso standard. Per semplicità faremo riferimento alla sola traccia 2, la più diffusa, e al contenuto usato nei sistemi di controllo accessi: codice comune (Factory Code) di tre cifre seguito dal codice utente (User Code) di cinque cifre. La traccia 2, chiamata anche ABA (da American Bank Association) o impropriamente ISO2, è registrata a 75 bpi, è di tipo numerico e comprende un massimo di 40 caratteri di cui 37 di testo e tre di controllo. Il testo utile è costituito da solo cifre (nel nostro caso 8: 3+5); ogni cifra è rappresentata su cinque bit di cui quattro di dato e uno di parità (dispari). I caratteri di controllo hanno lo scopo di delimitare l'inizio e la fine del testo, separare eventualmente i vari campi e permettere al Controller di verificare l'integrità del testo stesso. La stringa di dati è costituita da un carattere di inizio (SS, Hex B), dal testo vero e proprio (nel nostro caso da otto cifre), dal carattere di fine testo (ES, Hex F) e da uno di controllo (LRC). LRC (Longitudinal Redundancy Check) è l'or esclusivo longitudinale (o somma binaria senza riporto) dei singoli bit che compongono i caratteri del testo, inclusi SS ed ES. Il bit di parità di LRC è calcolato su carattere LRC stesso (e non dallo XOR dei bit di parità dei caratteri del testo). Nel nostro caso il numero complessivo di bit utili attesi è di 55 (1 ES, 3 Factory Code, 5 User Code, 1 ES, 1 LRC x 5 bit ciascuno). A questi sono da aggiungere i cosiddetti bit di "sincronismo", sempre di valore logico zero, all'inizio del testo prima di SS (bit di testa) e alla fine dello stesso dopo LRC (bit di coda). I bit di sincronismo non sono significativi: servono al Controller per autosincronizzarsi all'inizio del testo (aggancio a SS). Poiché i badge magnetici possono essere letti dal lettore in entrambe le direzioni di movimento, il Controller deve essere in grado di incamerare il testo anche in senso inverso (da LRC a SS) e poi ricomporlo correttamente. Il verso di lettura è spesso sfruttato per determinare in modo automatico la causale di "timbratura" (entrata/uscita) nei lettori impiegati per rilevare le presenze al lavoro. In relazione al formato e al contenuto del testo, le dif-

MAGSTRIPE & FRIEND

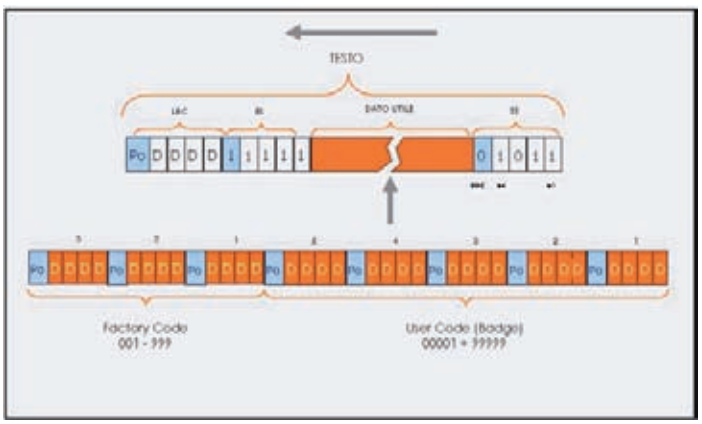
Le interfacce più usate tra un Controller per accessi e i suoi lettori di credenziali sono MagStripe e Wiegand. Oltre a questi due sistemi storici ne esistono altri meno noti ma altrettanto diffusi. Queste interfacce "non standard", tuttavia, nella maggior parte dei casi hanno il difetto di essere "proprietarie", ovvero più o meno chiuse al mondo esterno. Per contro, riescono a soddisfare le moderne esigenze di connessione fisica e logica che le due interfacce tradizionali, proprio perché datate, non sono in grado di assicurare. A livello fisico, le altre interfacce tra lettori e Controller operano generalmente su linee di comunicazione seriali TIA/EIA RS232 (punto a punto a breve distanza), RS422 o RS485 (bilanciate, punto a punto o multidrop a lunga distanza) e, più recentemente, anche via LAN (rete Ethernet 10/100 Mbps, TCP/IP). Nell'ambito dei sistemi di controllo accessi, la maggior parte dei protocolli di comunicazione su linee seriali prevede una connessione punto a punto, una trasmissione dati spontanea (cioè appena ultimata la lettura) e una struttura del testo libera o formattata. Nelle soluzioni più semplici, il dato letto viene inviato al Controller così com'è, senza formattazione e privo di caratteri di controllo; in genere non è prevista né la verifica dell'integrità del carattere né del testo. Il modello formattato, invece, prevede un tracciato record ben definito, con integrati o meno caratteri di controllo. Uno dei protocolli più diffusi di questo tipo è il cosiddetto "CR+LF" (ogni stringa di dati si conclude con la coppia dei caratteri CR ed LF). Linee seriali RS422-485 vengono spesso usate anche in connessione multidrop (bus) in modo da poter collegare più lettori a lunga distanza (1200 m) utilizzando un unico cavo dati a uno o due doppini. In questo caso, il colloquio tra il Controller e i vari lettori è regolato da un protocollo di comunicazione proprietario più o meno complesso. I lettori di credenziali, infine, oltre al controllo accessi, trovano largo impiego anche in altri campi come nell'automazione industriale, home e building automation. In questi casi, l'interfaccia è realizzata tramite mezzi fisici di connessione e protocolli di comunicazione specifici come, ad esempio, LonWorks, BACnet ecc.



L'interfaccia tra il lettore e il Controller per accessi è costituita da tre segnali: Card Present (ciclo di lettura in corso), Clock (sincronismo) e Data (valore del dato). Nella versione ridotta (Clock & Data) il segnale CP non è usato.



Il dato è disponibile sul segnale Data, in corrispondenza del fronte di discesa del clock. Il bit vale uno se il segnale Data è zero e viceversa. Nei tradizionali lettori di card con banda magnetica la temporizzazione dei segnali non è stabile ma legata alla densità di registrazione e alla velocità di lettura. © a&s Italy All rights reserved



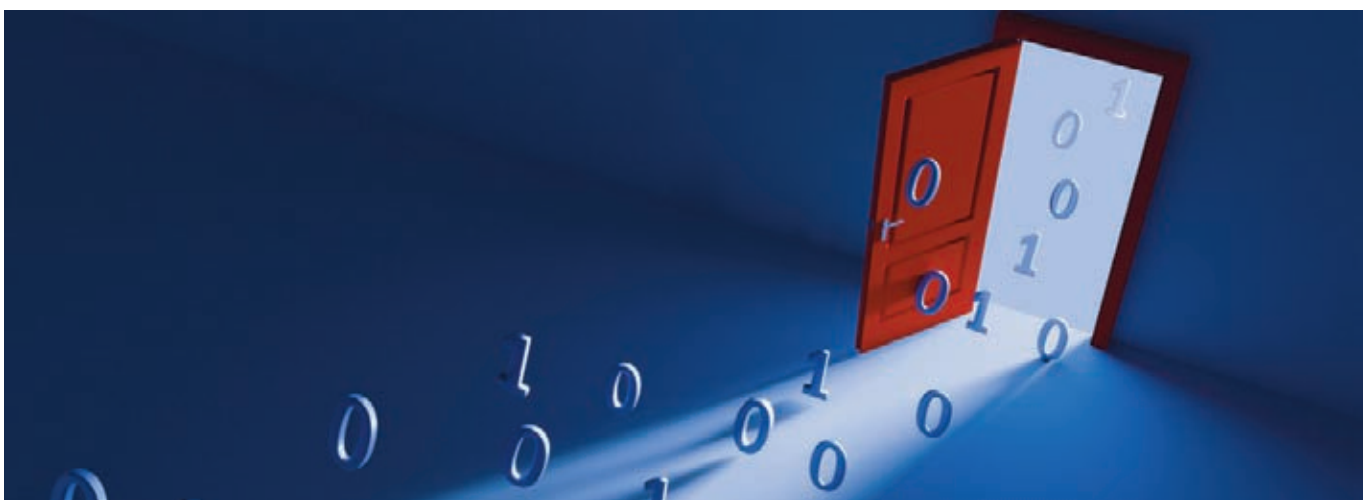
Il tracciato Magstripe prevede un carattere di inizio testo (SS), il dato utile (uno o più caratteri, massimo 37 nel formato traccia 2), un carattere di fine testo (ES) e uno di controllo (LRC). Nello standard industriale per accessi, il dato comprende due campi: Factory Code (comune a tutti gli utenti) e User Code (codice individuale). © a&s Italy All rights reserved

ferenze rispetto all'interfaccia Wiegand sono evidenti. Il dato utile può essere molto più lungo (fino a 37 cifre nel caso della traccia 2 contro le otto della Wiegand 26), il valore del dato ricevuto è univoco e non lascia spazio a interpretazioni, il controllo sull'integrità del testo è decisamente più efficace (frame di inizio e fine, VRC, LRC), è possibile determinare il verso di lettura ecc. Per contro, l'elaborazione dei dati da parte del Controller è molto più lunga e complessa nonché piena di trappole con conseguente possibile generazione di errori.

VARIANTI SUL TEMA

Nel corso dei decenni, all'interfaccia MagStripe primitiva, si è aggiunta una versione monca priva del segnale Card Present, assumendo il nome di *Clock and Data* o, in breve, *C&D*. Il modo di funzionamento è identico a quella tradizionale; viene solo ignorata la presenza del segnale CP. L'interfaccia MagStripe, inoltre, non è usata soltanto per connettere lettori di carte magnetiche ma anche altri dispositivi basati su tecniche di riconoscimento diverso, da ultime la RFId (Radio Frequency Identification) e la biometria (impronte digitali, geometria della mano ecc.). In questi casi, la variante significativa è la temporizzazione dei segnali. Nella soluzione in emulazione MagStripe, infatti, non essendo il timing più legato alla densità di registrazione della banda magnetica e alla velocità di lettura, la durata dei vari tempi tra un fronte e l'altro sono fissi. Fissi sì ma, tanto per cambiare, non uguali per tutti i produttori di lettori.

Da un decennio le carte di pagamento e di identificazione con banda magnetica (con lettori e registratori



GLOSSARIETTO

bit Binary unit. Ciascun elemento binario (zero o uno) che compone ogni carattere del testo.
bit di coda La stringa di bit a zero non significativi (bit di sincronismo) posta al termine del testo (dopo il carattere LRC)
bit di testa La stringa di bit a zero non significativi (bit di sincronismo) posta all'inizio del testo (prima del carattere SS)
carattere Ciascun elemento del testo rappresentato, nella traccia 2, da 4 bit (dato) e da un bit di parità (VRC)
carattere di controllo Quello riservato a funzioni di verifica o separazione dei campi nell'ambito del testo, in particolare SS, ES ed LRC
CK Clock. Segnale di sincronismo. Normalmente a uno, va a zero in corrispondenza di ogni bit valido
CP Card Present. Segnale di lettura in corso. Normalmente a uno, resta a zero per tutta la durata della lettura dei dati
C&D Clock & Data. Termine con cui è comunemente denominata l'interfaccia MagStripe ridotta, costituita dai soli segnali CK e Data
Data Dato. Valore del singolo bit (zero o uno) in corrispondenza del fronte di discesa del segnale di clock
ES End Sentinel, ETX. Carattere di fine testo. Nella traccia 2 corrisponde al valore Hex F
LRC Longitudinal Redundancy Check. Controllo di parità orizzontale, utile per verificare l'integrità del testo. È un carattere posizionato dopo ES, calcolato tramite l'or esclusivo longitudinale (o la somma binaria senza riporto) dei singoli bit che compongono il testo, inclusi SS ed ES
MagStripe Magnetic Stripe, banda magnetica. Termine con cui è comunemente denominata l'interfaccia fisica e logica tra un lettore di credenziali e il rispettivo Controller, derivato dall'output dei primi lettori di carte con banda magnetica
SS Start Sentinel, STX. Carattere di inizio testo. Nella traccia 2 corrisponde al valore Hex B
testo L'insieme dei caratteri registrati e letti, esclusi i bit di testa e di coda. Il testo utile è costituito da tutti i caratteri, esclusi SS, SS ed LRC; negli standard industriali di fatto è diviso in due campi: Factory Code (codice comune) e User Code (Codice Utente)
VRC Vertical Redundancy Check. Controllo di parità verticale, utile per verificare l'integrità del carattere. È costituito da un bit supplementare (bit di parità) il cui valore (zero o uno) è tale da far diventare dispari il numero di bit a uno che compongono il carattere.

al seguito) sono in declino, sostituite dalla tecnologia RFId-NFC e, in parte, dall'identificazione biometrica. È facile prevedere che anche l'interfaccia MagStripe finisca lentamente in soffitta. Già si sentono suonare in lontananza le prime campane a morto. Nessuno (o quasi) dei lettori RFId low cost made in China (modelli e quantità da capogiro), ad esempio, integra più questo tipo di interfaccia. Anche i cinesi preferiscono la Wiegand.

Testo	Valore Hex	Valore Bin	Calcolo LRC
SS (Start Sentinel)	B	0 1011	
1	1	0 0001	1010
2	2	0 0010	1000
3	3	1 0011	1011
ES (End Sentinel)	F	1 1111	0100
LRC	(4)	0 0100	

Esempio di calcolo del carattere LRC su un testo (SS 1 2 3 ES). LRC è l'or esclusivo longitudinale dei singoli bit. Il bit di parità (dispari) di LRC è calcolato sullo stesso carattere LRC e non sui bit di parità dei singoli caratteri che precedono.

IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

20-22 JUNE 2017 EXCEL LONDON UK

THE ONLY LARGE SCALE SECURITY EVENT IN EUROPE THIS YEAR

Over 10,000 security products to test & trial

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

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

Supported by:

ASIS INTERNATIONAL United Kingdom Chapter

bsia british security industry association

NSI Security. Improved

Your badge also gives you entry to:

IFSEC International

FIREX International

FACILITIES Show

SAFETY & HEALTH Expo

SERVICE MANAGEMENT Expo

POTENZA E TECNOLOGIA NEL SUO DNA

Basato sulle caratteristiche ereditate dal VX-402
VX-Infinity presenta infinite prestazioni
con la potenza di una elaborazione digitale

RIVELATORI A DOPPIA TECNOLOGIA PER ESTERNO

serie VX Infinity™

MODELLI CABLATI

VXI-ST : standard a 2 PIR
VXI-AM : con antimascheramento
VXI-DAM : PIR+microonda, antimascheramento

MODELLI A BASSO ASSORBIMENTO

VXI-R : standard a 2 PIR
VXI-RAM : con antimascheramento
VXI-RDAM : PIR+microonda, antimascheramento

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

Roberta Rapicavoli(*)

La dichiarazione di conformità

prevista dal DM 37/2008

L'art. 7 del decreto ministeriale 22 gennaio 2008, n. 37 ("Regolamento concernente l'attuazione dell'articolo 11-quaterdecies, comma 13, lettera a) della legge n. 248 del 2 dicembre 2005, recante riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici") individua, in capo all'impresa installatrice di impianti sottoposti all'ambito di applicazione della suddetta normativa, l'obbligo di rilasciare al committente, al termine dei lavori e previa effettuazione delle verifiche previste dalla legge vigente, apposita dichiarazione di conformità degli impianti realizzati nel rispetto delle norme di legge e delle norme tecniche. L'installatore deve predisporre la citata dichiarazione di conformità seguendo il modello allegato al DM 37/2008, così come modificato dal decreto del 19 maggio 2010, in cui sono definiti nel dettaglio le indicazioni da riportare e i documenti da allegare.

LA DICHIARAZIONE

Nello specifico, la dichiarazione contiene, nella sua prima parte, i dati della società installatrice e del committente, una descrizione schematica dell'impianto eseguito, precisazioni in ordine alla tipologia di intervento (se di tratta di nuovo impianto oppure di trasformazione, ampliamento o intervento di manutenzione straordinaria di un impianto già esistente), indicazioni sul luogo esatto in cui l'intervento è stato effettuato e sull'uso dell'edificio interessato (precisando se, ad esempio, lo stesso sia destinato ad un uso civile, industriale, di commercio o ad altro uso diverso).
Nella seconda parte del documento in esame sono invece contenute le attestazioni relative all'operato dell'installatore, che dichiara, sotto la propria personale responsabilità, che l'impianto è stato realizzato in modo conforme alla regola dell'arte, tenuto conto delle condizioni di esercizio e degli usi a cui è destinato l'edificio, avendo in particolare, rispettato il progetto redatto, seguito la normativa tecnica vigente, installato componenti e materiali idonei e controllato l'impianto ai fini della sicurezza e della funzionalità con esito positivo.

DOCUMENTI DA ALLEGARE

Oltre alle indicazioni da riportare all'interno della dichiarazione di conformità secondo il modello allegato al DM 37/2008 e sue successive modifiche, occorre poi prestare attenzione ai documenti che costituiscono parte integrante della dichiarazione e che, in quanto tali, devono essere allegati obbligatoriamente a quest'ultima per evitare di renderla, di fatto, incompleta e non ricevibile.

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

In concreto, la società installatrice dovrà allegare alla dichiarazione di conformità: la relazione contenente la tipologia dei materiali impiegati, il progetto dell'impianto (che deve comprendere le eventuali varianti realizzate in corso d'opera), lo schema di impianto realizzato (non necessario per progetti redatti da professionisti abilitati e non modificati in corso d'opera), il riferimento a dichiarazioni di conformità precedenti o parziali nel caso già esistenti (indicando l'impresa esecutrice e la data della dichiarazione), copia del certificato di riconoscimento dei requisiti tecnico-professionali della società installatrice e attestazione di conformità per impianto nel caso realizzato con materiali o sistemi non normalizzati. Rientra invece nella discrezionalità dell'impresa installatrice decidere se allegare o meno alla dichiarazione ulteriori documenti relativi all'impianto eseguito, come, ad esempio, eventuali certificati dei risultati delle verifiche effettuate sull'impianto prima della messa in esercizio o trattamenti per pulizia o disinfezione.

TEMPISTICHE E SANZIONI

La dichiarazione di conformità, debitamente compilata, completa dei suoi allegati e sottoscritta dal titolare dell'impresa installatrice e dal responsabile tecnico, deve essere rilasciata al committente e depositata, entro 30 giorni dalla conclusione dei lavori, presso lo sportello unico per l'edilizia, di cui all'articolo 5 del decreto del Presidente della Repubblica 6 giugno 2001, n. 380 del Comune ove ha sede l'impianto. A quali sono le conseguenze per la società installatrice che non osservi l'obbligo di rilascio della dichiarazione di conformità di cui all'art. 7 del DM 37/2008?
Oltre ai profili di responsabilità contrattuale per inadempimento nei rapporti tra la società installatrice e la committente, la mancata o incompleta emissione della dichiarazione di conformità da parte dell'installatore è punita, ai sensi dell'art. 15 del DM 37/2008, con la sanzione amministrativa del pagamento di una somma da euro 100,00 ad euro 1.000,00, determinata con riferimento all'entità e complessità dell'impianto, al grado di pericolosità ed alle altre circostanze obiettive e soggettive della violazione. Per completezza occorre però considerare che assolvere all'obbligo di predisporre e consegnare la dichiarazione di conformità dell'impianto, non solo esclude le conseguenze negative sopra indicate, ma rappresenta una garanzia per lo stesso installatore, che ha la possibilità di porsi al riparo da eventuali interventi di manomissione o cattiva manutenzione effettuati in un momento successivo rispetto alla data di rilascio della dichiarazione.

La certificazione degli esperti in Impianti di Allarme Intrusione e Rapina

Due nuovi profili professionali per il comparto della sicurezza.

Con lo sviluppo di tecnologie sempre più evolute e l'emanazione di norme che regolano il loro utilizzo, la competenza tecnica e di governance nel comparto della sicurezza sono oggi elementi fondamentali per differenziarsi dal mercato e per proporre un servizio completo di qualità.
Per valorizzare le conoscenze e competenze dei professionisti, TÜV Italia ha sviluppato un nuovo schema per la certificazione degli esperti e degli installatori, manutentori e riparatori di impianti di allarme antintrusione e rapina.

www.tuv.it/cei

TÜV SÜD
Italia

Scegli la certezza.
Aggiungi valore.

Nebbia di sicurezza

Abbiamo raggiunto un obiettivo impossibile:
rendere **invulnerabili** i nostri clienti.

aura
SICUREZZA

Numero verde
800944848

approfondisci su nebbiogeno.it

aura
SICUREZZA

Il nebbiogeno più bello

è anche il più avanzato

Tecnologia brevettata Vortex®

Il più sottile al mondo

Distribuzione specialistica

Mai più falsi allarmi

Gestione via web semplificata

Numero verde
800944848

approfondisci su nebbiogeno.it

ASIS
EUROPE

TRAVEL SECURITY,
DUTY OF CARE,
DEVICE THEFT
OR DATA LOSS

ALL OF THE ABOVE?

ASIS **EUROPE 2017**

FROM RISK TO RESILIENCE

MICO, MILAN **ITALY**
29–31 **MARCH 2017**

www.asiseurope.org

Tim Hewitt(*)

Rivelazione incendi IP: aumentare il valore e l'efficienza

In numerosi comparti il Protocollo Internet (IP) è diventato lo standard per il trasferimento di informazioni, dalla comunicazione alla voce, allo streaming video. La transizione alla comunicazione IP ha da offrire un maggior volume e una maggiore qualità di informazioni, il tutto in maniera più veloce, sicura ed economica. Rispetto ad altre, l'industria della rivelazione incendi è stata decisamente più lenta nell'adottare questa tecnologia, ma oggi si cominciano a vedere piccoli e positivi risultati. La comunicazione IP attualmente si utilizza in tre aree del mercato rivelazione incendi: monitoraggio allarmi antincendio, allarmi antifumo connessi e integrazione IoT. Vediamoli.

(*) Analista di IHS Markit https://ihsmarkit.com/

I servizi di monitoraggio allarmi antincendio sono generalmente legati ad altri servizi, che comprendono il monitoraggio allarmi antintrusione, la rilevazione video del fumo ed altri prodotti di security. Questo mercato è relativamente piccolo, rappresenta solo il 3% del mercato del monitoraggio degli allarmi antintrusione nella regione EMEA. Il "Plain old telephone service" (POTS, una tecnologia analogica di telefonia fissa) è stato usato tradizionalmente per facilitare la comunicazione tra il centro di monitoraggio e i pannelli antincendio in loco. Tuttavia, i sistemi moderni implementano l'uso di connettività IP e GSM in sostituzione del POTS. Numerosi sono i vantaggi di questo approccio. I provider delle telecomunicazioni stanno abbandonando l'uso del POTS, riducendo la quantità di investimenti nella rete. Gli investimenti in reti IP e GSM sono aumentati per decenni e la copertura è ormai molto affidabile nella maggior parte delle aree inurbate. Utilizzando una combinazione di IP e GSM si garantisce la ridondanza necessaria per i pannelli di allarme antincendio. Inoltre, l'uso del messaggio digitale che si avvale di reti IP o GSM per testare la connessione e lo status del sistema di allarme antincendio permette di condurre verifiche nell'arco di minuti, invece che ogni 24 ore (come accade quando si usa il POTS).

A LIVELLO ECONOMICO

I messaggi IP e GSM permettono all'informazione di venire trasmessa con più accuratezza e quindi di comunicare informazioni più complesse. Il posizionamento dei rivelatori antincendio e il numero di dispositivi attivati può fornire ai pompieri informazioni essenziali per contrastare l'incendio nel modo più efficace. Il crescente costo dell'affitto della linea offerta dalle aziende di telecomunicazione rende invece il POTS una soluzione a minor rapporto costi-benefici. Nei grandi sistemi antincendio con numerosi pannelli di controllo sulla rete, spesso è necessaria una linea telefonica separata per ogni pannello: ciò genera una notevole e continua spesa sui sistemi POTS. Le reti IP più probabilmente sono già parte dell'infrastruttura e dei costi correnti di un edificio e la connettività GSM è decisamente conveniente. Generalmente l'aggiornamento di un sistema con IP e GSM si pagherà da sé nel corso di uno o due anni con un risparmio sull'affitto della linea.

ALLARME ANTI-FUMO CONNESSI

I prodotti home connessi stanno sempre più aumentando, offrendo possibilità, servizi e informazioni all'utente finale. Gli allarmi antincendio non sono un'eccezione: i prodotti sul mercato spaziano dagli allarmi Wi-Fi antifumo connessi low cost, ai rivelatori di alta gamma multi-funzione come Nest Protect. Nella regione EMEA il mercato per gli allarmi fumo e monossido di carbonio si prevede crescerà da 50 mila unità nel 2016 a oltre 250 mila unità entro il 2020. La maggiore opportunità in quest'ambito arriva dalle installazioni smart home. Per i sistemi di sicurezza smart home è sempre più comune includere un allarme fumo connesso come standard, o come un extra optional. I sistemi di sicurezza smart home sono una delle aree di maggior successo per via della forte sinergia con i servizi connessi che generano nell'utente un senso di sicurezza. Gli allarmi fumo entrano bene in questa categoria e offrono ai provider di smart home security una modalità nuova per aumentare il valore dei propri prodotti e servizi.

Gli assicuratori stanno cominciando ad offrire servizi smart home con una particolare attenzione ai sistemi che riducono il numero o la gravità delle richieste di indennizzo da parte di chi ha sottoscritto la polizza. Ciò aumenta il valore dei sistemi antintrusione, antincendio e di allerta inondazione perché riduce i rischi legati alla proprietà. Molte assicurazioni ora offrono una riduzione dei premi ai clienti le cui case sono dotate di sistemi di sicurezza connessa e allarme fumo e in alcuni casi propongono essi stessi questi servizi, con una copertura assicurativa legata alla vendita di prodotti e servizi per la protezione dell'abitazione.

INTEGRAZIONE IOT

L'Internet of Things (IoT) è un trend in crescita in molte industrie, da quella dell'elettronica consumer alla logistica. L'industria delle attrezzature antincendio sta anch'essa cominciando ad approcciare questa rivoluzione per aumentare l'efficienza e offrire valore aggiunto. Il prerequisito che permette ai servizi di dialogare è la connessione a internet. Molti produttori di pannelli di controllo ora stanno includendo nei loro prodotti porte LAN (Local Area Network). Ciò permette al pannello di essere connesso

alla rete locale e, attraverso quest'ultima, a internet. Il valore aggiunto per il cliente si identifica su due livelli: un livello base del servizio offre al cliente l'informazione da remoto sul sistema antincendio. Questo può inviare al cliente una push notification o un alert via email quando rivela un errore o lancia un allarme. Un livello più avanzato di servizio può dare al cliente il controllo da remoto del sistema antincendio e permettere di configurare e testare il sistema da remoto. Tuttavia, il valore più grande dell'integrazione IoT risiede nell'aumento dell'efficienza del servizio e manutenzione. Un sistema connesso è in grado di allertare l'ingegnere di un errore nel sistema e dare informazioni sulla natura dell'errore prima di recarsi sul posto. Questo significa che l'operatore si può munire dei ricambi adatti all'errore riscontrato, diminuendo il tempo tra la rilevazione del problema e la sua risoluzione. Inoltre, alcuni errori si possono risolvere da remoto, riducendo enormemente i costi in termini di tempo. Essere in grado di rispondere ai malfunzionamenti velocemente ed in modo efficace è un assoluto vantaggio soprattutto per i progetti di un certo rilievo. La capacità di realizzare controlli regolari al sistema da remoto è un beneficio notevole perché riduce il costo del servizio e permette a un unico ingegnere di offrire un servizio di buona qualità a più clienti, oltre a permettergli di coprire un'area geografica più ampia perché si rendono necessarie meno visite, se non addirittura nessuna. Le nazioni e regioni con il costo del lavoro più alto, come la Germania, daranno più valore ai servizi connessi.

IL FUTURO DEL RILEVAMENTO INCENDI IP

L'integrazione IP permette ai provider di attrezzature antincendio di aggiungere valore ai loro prodotti offrendo funzioni aggiuntive, servizi e affidabilità. Tuttavia i due fattori principali che guidano le decisioni dei consumatori sono le normative e il costo. È improbabile che il cliente installi un sistema che ignori i requisiti richiesti da normativa ed è improbabile che scelga un prodotto premium che offre ulteriori protezioni al di là di ciò che viene richiesto dalla legge. Questi fattori inibiscono la crescita dei sistemi di allarme antincendio connessi, tuttavia la connettività IP si prevede sarà un fattore importante di differenziazione e un plus a prova di futuro per molti sistemi antincendio.

sistema radio linea ORO

Il sistema ORO 869 è quanto di più innovativo ed evoluto possa esistere nel modo della sicurezza senza fili

Il protocollo di trasmissione è bidirezionale e doppia frequenza operante sulle frequenze 868,00-868,60 MHz e 869,40-869,65 MHz. La bidirezionalità del protocollo permette alle periferiche di conoscere lo stato dell'impianto - Inserito/Disinserito - ponendo le stesse in condizione di Stand By ad impianto non inserito con un notevole risparmio di batterie; inoltre ad impianto inserito le periferiche operano senza inibizione **garantendo uno stato di sicurezza equivalente ad un sistema filare.** Nell'ottica di risparmio energetico il software è anche in grado di stabilire la distanza tra centrale ed ognuna delle periferiche dosando la potenza di uscita in funzione di essa.

Numerosi accorgimenti quali il FH (Frequency Hopping), il TDMA (Time Division Multiple Access) ed l'AES (Advanced Encryption Standard) **ne garantiscono la sicurezza e l'affidabilità contro attacchi esterni**. Il continuo dialogo tra centrale e periferiche elimina inoltre il pericolo legato a tentativi di disturbo delle frequenze (jammer).

Il protocollo di comunicazione radio permette di raggiungere una distanza di trasmissione fino a 1,5 km in aria libera. I settaggi di tutte le periferiche avvengono da centrale tramite tastiera integrata. **Il sistema è conforme agli standard EN-50131 (Grado 2)**.

1 **Centrale 8039-ISC001** • Centrale di allarme serie ORO con 64 zone via radio e 2 zone filari estendibili a 7. Tutte le periferiche possono essere settate direttamente dalla centrale. Operante sulle frequenze da 869,40 MHz a 869,65 MHz (1 canale) e da 868,00 MHz a 868,60 MHz (4 canali). La sicurezza e l'affidabilità delle comunicazioni sono garantite dal sistema FH, dal TDMA e dall'AES. Alimentazione 230 Vca, alimentatore switching 14,5 Vcc 2,5 A. Grazie ad un supporto a muro risulta semplice l'installazione e l'eventuale manutenzione della centrale.

2 **Radiocomando 8049-ISA008** • Tramite il Radiocomando bidirezionale serie ORO è possibile, con due soli tasti, selezionare tutte le 7 combinazioni di inserimento, parzializzazione, scelta dei programmi, disinserimento e panico.

3 **Sirena TRE 8048-ISS004** • Sirena autoalimentata serie ORO da esterno completamente in policarbonato resistente agli urti ed ai raggi UV. La sirena è stata progettata per il comfort dell'installatore con frontale apribile a cerniera a destra o a sinistra, senza necessità di rimuoverlo dalla base, e seconda copertura apribile a tavolino per riporvi gli attrezzi. Grazie alla funzione WIN (Wired Interface Network) è possibile utilizzare due differenti tipi di batteria (non inclusa): litio non ricaricabile e SLA ricaricabile.

4 **Rivelatore ITALO 8040-ISR027** • Rivelatore via radio serie ORO in tripla tecnologia, con funzione Pet Immunity, è composto da 2 PIR e 1 microonda a 24 GHz. Portata di rilevazione selezionabile da 3 a 12 m con apertura 85° e regolazione interna di 90°. Funzione WIN per scegliere il tipo di alimentazione, con batteria a litio (inclusa) o supplementare esterna. Funzione Antimascheramento. Installazione ad 1 - 1,2 m di altezza. Disponibile anche nella versione senza microonda.

5 **Rivelatore TENDA 8041-ISR028** • Rivelatore via radio serie ORO in tripla tecnologia, composto da 2 PIR e 1 microonda a 24 GHz. Può essere installato tra finestra e persiana o in esterno a protezione di qualsiasi varco con la staffa 1894SPB. Funzione WIN per scegliere il tipo di alimentazione, con batteria a litio (inclusa) o supplementare esterna. Funzione CWS per la desensibilizzazione di uno dei due PIR per determinare il senso di attraversamento (selezionabile). Funzione Antimascheramento. Rilevazione a tenda 4 m in altezza per 5 m in larghezza. Disponibile anche in colore marrone e nella versione senza microonda.

6 **Rivelatore 8042-ISR029** • Rivelatore da interno via radio serie ORO in doppia tecnologia composto da 1 PIR ed 1 microonda a 24 GHz. E' installabile ad un'altezza di 2,1 m e rivela fino ad un massimo di 12 m con 90° di apertura. Provvisto di snodo per il fissaggio a muro. Funzione WIN per scegliere il tipo di alimentazione, con batteria a litio (inclusa) o supplementare esterna. Funzione Antimascheramento.

7 **Rivelatore 8044-ISR031** • Rivelatore da interno via radio serie ORO in doppia tecnologia per installazione a soffitto, composto da 1 PIR ed 1 microonda a 24 GHz. Area di rilevazione ellittica, con asse maggiore 11,4 m e asse minore 5 m se installato a 4 m di altezza. Funzione WIN per scegliere il tipo di alimentazione, con batteria a litio (inclusa) o supplementare esterna. Funzione Antimascheramento.

8 **Rivelatore 8045-ISR032** • Rivelatore magnetico via radio serie ORO per porte o finestre. Colore bianco. Disponibile anche nella versione marrone.

9 **Scheda 8050-IST001** • Scheda programmatore telefonico GSM da alloggiare all'interno della centrale art. 8039-ISC001. Con funzione TTS (Test To Speach) per la registrazione dei messaggi vocali e la gestione da remoto tramite SMS della centrale.

italiana sensori
per i professionisti della sicurezza

ISO 9001:2008
Sistema di gestione della qualità
I prodotti ITALIANA SENSORI s.a.s. sono progettati e assemblati in conformità alle norme UNI EN ISO 9001:2008

Via Pordenone, 2 ROMA
T 06 92928252
info@italianasensori.it
www.italianasensori.it

made in italy

Barbara Pandolfino(*)

Fascicolo Sanitario Elettronico: quale quadro regolatorio?

La smaterializzazione documentale attuata negli ultimi anni ha interessato anche il settore sanitario laddove la cartella clinica elettronica (CCE) - entrata in vigore l'11 Aprile 2014 – lascia il posto al Fascicolo Sanitario Elettronico. Senza volerci addentrare nell'analisi dell'articolato processo amministrativo di c.d. "smaterializzazione" , interessa qui porre l'attenzione sull'adozione di misure di sicurezza che inevitabilmente interessano il trattamento, la gestione, l'archiviazione e soprattutto la privacy dei dati contenuti nelle cartelle stesse. Cosa accadrebbe infatti se abili hacker informatici riuscissero ad accedere ai server delle strutture sanitarie all'interno dei quali sono custodite le cartelle cliniche di migliaia di pazienti, avendo quindi accesso a dati sensibili, attinenti al bene costituzionalmente tutelato della Salute? Quali ripercussioni, in campo civilistico e penalistico, vi sarebbero in capo ai titolari del trattamento, vale a dire quei soggetti obbligati a garantirne l'inviolabilità?

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

Sappiamo che con la Circolare del Ministero della Sanità n. 61 del 19 dicembre 1986 n. 900.2/AG 464/260 : “le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre che costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario”1. Affinché il fascicolo sanitario elettronico mantenga nel tempo lo stesso valore probatorio di quella cartacea, si rende necessario ed indispensabile un corretto processo di conservazione digitale. Mentre la Cartella Clinica Elettronica veniva utilizzata per la gestione organizzata e strutturata dei dati riferiti ad un paziente durante un ricovero o cura ambulatoriale, il Fascicolo Sanitario Elettronico (in vigore con decreto dal Novembre 2015) è quel fascicolo formato con riferimento a dati sanitari da diversi titolari del trattamento che contiene tutti i dati identificativi ed amministrativi dell’assistito, quali referti, verbali di pronto soccorso, lettere di dimissioni, consenso o diniego alla donazione degli organi e tessuti e cartelle cliniche.

ATTIVITÀ PERICOLOSE

Tutta l’attività di gestione e trattamento dei dati personali, con contenuti sanitari, risulta talmente delicata da rientrare nella categoria delle c.d. “attività pericolose”: un trattamento dei dati personali sanitari in violazione dei precetti normativi può spingere l’interessato (paziente) a chiedere il risarcimento dei danni subito a seguito di tale inosservanza, ai sensi dell’art. 2050 codice civile2
Nel caso di richiesta di risarcimento danni da parte del soggetto che ritiene leso il proprio diritto alla privacy, il titolare del trattamento, se vuole evitare la condanna, deve dimostrare di avere adottato tutte le misure idonee a evitare il danno: la cosiddetta inversione dell’onere della prova. Non è dunque il danneggiato (paziente) a dover dimostrare che chi deteneva i dati (medico/struttura ospedaliera) non è stato attento, ma è quest’ultimo a dover dimostrare di aver fatto tutto il possibile per evitare il danno. Garantire la privacy di simili dati significa porre in essere non solo tutte le misure minime di sicurezza necessarie (all.B 679/13) volte ad evitarne la distruzione o la perdita (anche accidentale), ma anche negare l’accesso da parte di soggetti non autorizzati, il trattamento non consentito o non conforme alle finalità della raccolta. Queste ovvie considerazioni appaiono di semplice e pronta attuazione nell’ambito di strutture complesse, quali ad esempio nosocomi, case di cure e ricoveri, dotati quasi tutti di veri e propri manuali contenenti le linee guida per i responsabili e gli incaricati del trattamento dei dati personali. Ma cosa accade invece nel piccolo studio medico?

I precetti normativi sono scrupolosamente adottati nella salvaguardia e nella cura della gestione dei dati?

DUE MISURE DI SICUREZZA

Il Codice iin materia di trattamento dei dati personali individua due tipi di misure di sicurezza, entrambi da adottare:

a. le misure minime di sicurezza – previste nell'allegato B) del Codice medesimo, denominato "Disciplinare Tecnico in materia di misure minime di sicurezza" (artt. da 33 a 36), riguardano sia i trattamenti effettuati con strumenti elettronici che quelli effettuati senza strumenti elettronici;
b. le misure idonee di sicurezza (art. 31). Adottare misure idonee di sicurezza significa migliorarle – annualmente - in base al progresso della tecnologia, alla natura dei dati trattati, alle caratteristiche dei trattamenti nonché ai rischi nell'uso dei dati.

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- tracciabilità degli accessi e delle operazioni effettuate;
- sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.

Nel caso di Fse, devono essere, poi, garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.

ILLECITI PENALI

Oltre alla previsione normativa di cui all'art. 2050 codice civile, è bene rammentare che il Testo Unico sulla Privacy prevede anche illeciti penali e violazioni amministrative. Nella finalità didascalica che questa trattazione si vuole porre ci limiteremo a citarne solo alcuni, a titolo meramente esemplificativo. Nell'ambito degli illeciti penali si configura l'art. 167 del Codice Privacy, il c.d. " trattamento illecito dei dati": "salvo che il fatto non costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione della normativa è punito, se dal fatto deriva nocumento, con la reclusione da sei mesi a tre anni". Mentre all'art. 169 recita: "chiunque, essendovi tenuto, omette di adottare le misure minime previste, è punito con l'arresto sino a due anni o con l'ammenda da 10.000 a 50.000 Euro. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo tecnicamente necessario. (…) Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato".

ESTOTE PARATI

Dalle brevi considerazioni svolte, appare quanto mai importante far sì che *tutte* le realtà sanitarie (piccole o grandi che siano) che trattano dati sensibili attinenti al bene salute siano consapevoli della "granata pronta ad esplodere" che hanno per le mani. Non trovarsi pronti a fronteggiare l'abilità tecnologica di soggetti privi di scrupoli, con adeguati sistemi antivirus, potrebbe nuocere gravemente sia a livello di responsabilità professionale che – ben peggio- a titolo di responsabilità penale e civile.

THINK SAFETY.
THINK NEW.

NON RIMANERE NEL DUBBIO. VIDEOVERIFICA.

Sicurezza e tranquillità, in tempo reale.

GenesyVEDO è la centrale di allarme firmata WolfSafety.
Un sistema rivoluzionario che integra il tuo impianto di videosorveglianza esistente e invia in tempo reale, e direttamente sul tuo smartphone, le immagini della telecamera dell'area indicata. Con l'app WolfCasaMia saprai subito se la segnalazione ti conferma un intruso o semplicemente l'agilità del tuo gatto.

www.wolfsafety.it - www.genesyvedo.it
info@wolfsafety.it

WOLF SAFETY
COSTRUTTORI DI SICUREZZA

La Redazione

Turchia: tra luci e ombre, il mercato della sicurezza

Pubblichiamo una recente indagine sul mercato turco, che rappresenta un interessante ed imparziale indicatore per possibili investitori italiani su quell'area geografica. Alcuni attori del mercato turco non hanno osservato o riferito di cambiamenti sostanziali nel 2015 (ultimo anno finanziariamente esplorabile), mentre quelli dotati di strutture meno solide sono stati colpiti profondamente dall'incertezza. Ciononostante, la maggior parte delle aziende ha registrato una crescita attestabile su una percentuale pari a +10.

La ricerca, messa a punto da una delle nostre riviste consorelle, ha identificato in 700 milioni di dollari il valore delle vendite per la sicurezza elettronica realizzate nell'anno 2015. Se a questa cifra aggiungiamo la cifra prodotta dalle vendite degli altri segmenti del comparto sicurezza, il valore complessivo del mercato potrebbe aggirarsi sui 6 miliardi – in crescita peraltro nel 2016. Con nuovi attori presenti sul mercato, però, la scacchiera competitiva sta cambiando. Aumenta il numero di aziende, ma mentre alcune crescono, altre lottano per guadagnare piccole fette di market share. Le aziende più robuste e dimensionate, vantando importanti legami con il settore telecomunicazioni e consumer, riescono infatti ad utilizzare e vendere la tecnologia efficacemente, surclassando i competitor. La diminuzione dei costi di produzione ha poi portato notevoli cambiamenti nella stessa gamma di prodotti disponibili, tali da qualificare il 2015 come un "anno di transizione" per la Turchia. Vediamo come.

TRANSIZIONE

Il 2015 è stato un anno di transizione per la Turchia. La crescita della domanda e dei competitor ha fatto evolvere la stessa tecnologia: si sono registrati infatti importanti sviluppi nei prodotti IP-based, i cui costi si sono peraltro abbassati repentinamente, e i prodotti HDCVI hanno riscontrato un discreto successo per rinnovare il vasto parco analogico esistente. Nuovi software hanno poi consentito di analizzare più dati e meglio, con importanti conseguenze in termini di efficienza del business per l'utente finale.

PECULIARITÀ

Rispetto al resto del mondo, la Turchia soffre, in termini di espansione, a causa delle restrittive leggi locali su fusioni e acquisizioni. Inoltre a livello globale il settore si è spostato verso il B2B e B2C, due business che in Turchia ancora non si sono consolidati. In questo senso il paese sembra vivere una forma di arretratezza. La domanda dei clienti pare tuttavia essere cambiata e concentrata più sull'investimento in prodotti e soluzioni di sicurezza maggiormente integrata.
Si rileva poi un elemento frenante di matrice sociale, ossia il generale miglioramento dei diritti dei lavoratori che ha, per converso, portato taluno a considerare il lavoro di addetto alla sicurezza come un impiego provvisorio o saltuario: questo sta riducendo la qualificazione degli addetti alla security, quando invece per far crescere il settore occorrerebbe l'ausilio di personale altamente professionalizzato.

ELEMENTI FRENANTI

Tra i fattori che nel 2015 hanno influenzato negativamente la crescita del comparto si annoverano l'incertezza politica, le elezioni, i tassi di cambio fluttuanti e il terrorismo – che ha portato nuove aziende a entrare nel settore security turco, aumentando però nel contempo la competizione.

UN 2016 COMPLESSO

Nell'analizzare l'anno 2016 per l'industria turca non si può non citare il fallito colpo di stato del 15 luglio scorso, quando carri armati sono scesi per le strade nell'intento di rovesciare il presidente Recep Tayyip Erdoğan. Senza entrare in valutazioni politiche che non ci competono su genuinità e reali finalità del presunto golpe, non possiamo però non menzionare l'incertezza, anche economica, che ha seguito quei drammatici momenti. Se da un lato, stando ai nostri inviati, pare che tale incertezza non abbia intaccato le previsioni positive di chiusura d'anno degli operatori del comparto sicurezza, dall'altro ha però senza dubbio ostacolato o rallentato alcuni progetti in essere. Per delle valutazioni più specifiche sull'anno 2016, ci riserviamo quindi di attendere il prossimo report.

Sul fronte squisitamente tecnico, l'analogico in HD sta soffrendo a causa di ritardi dei produttori di chipset e problemi nei processi di produzioni dei registratori compatibili. Ma secondo la maggioranza degli intervistati, il vero problema del 2015 è stato il recupero crediti. Fenomeno non certo alieno alle imprese del Belpaese.

MERCATI VERTICALI

Il 2015 ha registrato una certa stagnazione negli investimenti pubblici e la transizione verso gli investimenti in edifici di edilizia residenziale, ospedali, istituzioni scolastiche. Restano interessanti i verticali relativi al controllo di traffico, tribunali e centri commerciali. In aumento anche l'interesse delle imprese del settore per i complessi residenziali e il settore edilizio in generale. Tra i principali progetti messi in opera nel 2015, si annoverano porti, terminal e la metro di Instambul, oltre a tutti i progetti legati al controllo del traffico, specialmente in termini di controllo elettronico dinamico degli incroci e videosorveglianza nei tunnel. Interessanti anche i progetti MOBESE per il G20 ad Ankara, Antalya, Nevşehir e Gaziantep per la sicurezza delle città.

IP VS. ANALOGICO

Nonostante qualcuno affermi che in Turchia la migrazione verso l'IP si sia già conclusa, l'analogico è in realtà ancora molto presente. Non si vende più ma c'è, quindi i sistemi HDCCTV rispondono a diversi bisogni. La capacità di analisi video, la praticità e adattabilità dei sistemi IP sono tuttavia innegabili. Soprattutto grazie all'aumento dei sistemi integrati e dell'Internet of things, i sistemi di sicurezza futuri si svilupperanno quindi senza dubbio sulla base di protocolli Internet. Tra i prodotti più gettonati, attualmente si annoverano le telecamere 3-5 MP e 4K e gli allarmi wireless e indirizzabili. In aumento i prodotti integrati e la domanda di dispositivi ibridi per la registrazione. Molto apprezzate le telecamere fisheye, il cui costo è peraltro in diminuzione, le dome con capacità zoom, tutti i prodotti che danno buone performance con scarsa illuminazione e le risoluzioni Full HD e 4K.

IN CRESCITA: IOT

L'Internet of Things sta diventando una realtà sempre più tangibile: i principali cambiamenti riguardano i nuovi prodotti sul mercato, con la crescita dello smart home. Dal momento che l'IoT, l'intelligenza artificiale e la realtà virtuale hanno visto concretizzarsi enormi investimenti, non v'è dubbio infatti che entreranno anche nel settore security, partendo proprio dalla home and building automation. Qualcuno degli intervistati da a&s Türkiye si spinge a dire che "tempo 10 anni e non esisteranno più sistemi che non colleghino tutti i dispositivi esistenti". Con l'IoT si integreranno infatti TVCC, sistemi antincendio, controllo accessi, sistemi di gestione degli edifici: i sistemi parleranno tra loro e il risultato sarà semplicità e funzionalità. Dopo le oscillazioni del 2015, le aspettative di chiusura per il 2016, nonostante i disequilibri politici che hanno caratterizzato lo scorso anno, restano positive. L'integrazione giocherà un ruolo importantissimo e l'evoluzione tecnologica aumenterà esponenzialmente le opportunità, consolidando il concetto di smart city e smart home.

Allarmi professionali sviluppati per le persone !

Allarmi innovativi di altissima qualità con più di 25 anni di esperienza e reputazione a livello mondiale.

Tutto per il tuo business in un unica soluzione con l' APP MyCompany ed applicazione WEB browser.

Un sofisticato sistema per la formazione e il supporto tecnico.

Un design senza tempo in una forma pratica e facilmente comprensibile.

www.jablotron.it

JABLOTRON
CREATING ALARMS

Olga Inshakova(*)

Il mercato russo della Security & Safety

Il mercato russo della sicurezza, comprensiva di Security e Safety, ha tutte le carte in regola per svilupparsi per diversi anni: le grandi infrastrutture del paese, l'estesa area geografica da coprire e l'alto numero di potenziali minacce offrono ampia materia sulla quale lavorare. Tuttavia negli ultimi anni l'industria della security, tradizionalmente dominata da vendor stranieri, è cambiata radicalmente assieme al mutato scenario economico e politico locale. Il Rublo debole e le sanzioni internazionali hanno portato ad una graduale sostituzione dell'import con sempre più intensi sforzi di localizzazione dell'industria. Chi intende proporsi al mercato russo deve quindi più che mai conoscere le dinamiche che lo muovono. L'importante magazine di settore Groteck ha realizzato per *a&s Italy* un vademecum per le imprese interessate ad approcciare il mercato russo.

(*) Groteck Business Media **www.groteck.com**

Chi intende accedere al mercato russo potrebbe incorrere in alcuni ostacoli all'entrata: dal regime normativo gravoso ai diritti per la proprietà intellettuale inefficaci, dalla corruzione diffusa e uno stato di diritto inadeguato, fino all'applicazione discordante di leggi e regolamenti. La mancanza di trasparenza, in generale, rende la competizione molto complessa, anche a causa della presenza di aziende di proprietà o comunque controllate dallo Stato che dominano i settori strategici dell'economia. E' quindi bene sapere che gli investimenti nei grandi settori strategici sono sempre soggetti al controllo governativo. Nuove leggi nel settore IT rendono poi difficoltosa la fornitura di merci e servizi ad aziende tecnologiche estere. Ad esempio, la Risoluzione del Governo Russo Nr. 1236, in vigore dall'inizio del 2016, chiede alle agenzie governative di dare la priorità a software russi sulla base di un registro pubblicato e aggiornato dal Ministero delle Comunicazioni. Secondo questa nuova legge, le agenzie possono comprare un software all'estero solo quando non è disponibile un omologo di origine russa. Inoltre, il 21 luglio 2014, il Presidente Putin ha firmato la Legge Personal Data On-shoring 242-FZ, che richiede alle aziende di immagazzinare i dati personali dei cittadini russi solo su server situati fisicamente in Russia. Questa legge ha reso difficile la scelta di soluzioni IT cloud-based. Da quando la Legge è entrata in vigore, l'1 settembre 2015, il Russian Federal Service for Supervision in ambito Telecomunicazioni, IT e Comunicazione di massa è abilitato a multare le aziende che violano la legge e restringere l'accesso ai loro siti Web.

PROIBIZIONI E RESTRIZIONI ALL'IMPORT

L'import e l'export di merci in Russia avviene secondo una lista unificata di commodity ristrette all'import nell'Unione Economica Eurasiatica (EAEU). La lista è stata approvata con Risoluzione del Collegio EEC Nr.134 (16 agosto 2012). Ulteriori documenti che regolano il settore sono il Customs Union Agreement su Licensing Regulations of International Trade del 9 giugno 2009, e il Decreto della Federazione Russa Nr.1567-p del 23.09.2010. Il 7 agosto 2014, a seguito delle sanzioni in risposta alla crisi in Ucraina, la Russia ha imposto un divieto di un anno sulle importazioni di alcuni prodotti agricoli e alimentari dagli USA, Unione Europea, Canada, Australia, e Norvegia. Il 24 giugno 2015 la Russia ha esteso il divieto fino all'agosto del 2016.

SETTORI PIÙ PROMETTENTI

Immense distese territoriali, numerose risorse naturali, oltre 142 milioni di consumatori e un grande bisogno infrastrutturale: la Russia rimane un mercato molto goloso per gli esportatori internazionali. La Russia è del resto la dodicesima economia più grande al mondo per PIL nominale e la sesta per potere d'acquisto (dati Fondo Monetario Internazionale). Secondo la Banca Mondiale, il PIL pro capite 2014 era di $12.736, il più alto fra le nazioni BRICS (Brasile, Russia, India, Cina, e Sud Africa). I salari sono alti, la forza lavoro competente e formata e i consumatori cominciano ad essere molto sofisticati. Anche se la Russia si è ripresa velocemente dalla crisi finanziaria del 2009, la crescita economica è rallentata in modo deciso; di conseguenza il PIL nel 2015 si è contratto, lasciando spazio a una crescita piatta o a un segno leggermente negativo nel 2016. I principali partner russi per il commercio sono Cina, Olanda, Germania, Italia, Turchia, Giappone, USA, Ucraina, Sud Corea e Polonia. L'appartenenza all'Organizzazione Mondiale del Commercio (WTO-dal 2012) ha creato potenziali opportunità per l'export e gli investimenti offrendo al paese nuovi benefici: trattamento più liberale per export servizi e service provider, un più forte impegno per la protezione della proprietà intellettuale, accesso al mercato sotto quote specifiche per nazione e tariffe, miglioramento della trasparenza nella regolamentazione commerciale e un meccanismo di risoluzione delle dispute WTO (World Trade Organization, Organizzazione mondiale del commerci) più efficace.

LA SICUREZZA

Con l'accesso della Russia nella WTO, molte aziende straniere stanno pensando di entrare nel segmento safety e security che prima era inaccessibile, anche con forniture per la safety in penitenziari, attrezzature per il controllo carcerati e vari tipi di abbigliamento protettivo. Nel segmento Security & Safety la quota di prodotti importati va dal 50% al 95%. Gli esperti pensano che fino all'80% del controllo accessi, circa il 50% di allarmi antintrusione e antincendio e oltre il 95% dei sistemi TVCC siano importati. Inoltre, le attrezzature prodotte

localmente generalmente contengono dal 60% al 95% di componenti importati. I sistemi professionali sono importati da USA, Europa (Gran Bretagna, Germania, Francia, Italia e Polonia), Giappone e Israele, anche se la maggior parte dei componenti che compongono questi sistemi viene dalla Cina. I prodotti cinesi, taiwanesi e coreani sono più popolari nelle regioni russe lontane da Mosca e da San Pietroburgo.

I PRINCIPALI BUYER

Il Governo russo è tra i principali compratori di sistemi per safety e security, con acquisti per oltre 800 milioni di dollari nel solo 2013. Cifre che aumentano ogni volta che iniziano nuovi progetti edilizi afferenti a grandi eventi, come ad esempio la Coppa del Mondo FIFA nel 2018. Il crimine e il terrorismo rappresentano poi minacce costanti alla stabilità nelle regioni centrali e meridionali, vista anche l'incerta situazione politica nel Nord del Caucaso. Non a caso, forse, la Russia sta attivamente rimodernando il proprio sistema frontaliero. Generalmente queste opportunità di mercato seguono iniziative sponsorizzate dal governo, che ha anche dato inizio a cospicui investimenti in ambito stradale, spendendo circa 80 milioni di dollari in telecamere per il controllo del traffico e sistemi di registrazione per violazioni del codice stradale. La riorganizzazione della polizia ha visto poi lo stanziamento di altri 6,5 miliardi di dollari e richiesto l'acquisto di attrezzature per lo scanning nei luoghi pubblici e l'installazione di attrezzature. Attualmente i dipartimenti investigativi stanno acquistando e mettendo a regime nuovi dispositivi per i test forensi. Infine, un programma continuo, concentrato sul rinnovamento dell'equipaggiamento dell'Esercito Russo, stima lo stanziamento di ben 750 miliardi di dollari da qui al 2020, generando opportunità significative per chi serve il settore militare. Questo sul fronte government.
Anche gli enti privati, principalmente di area Retail, Oil&Gas, industria, trasporti, banche, energia, sono comunque buyer importanti per un'ampia gamma di attrezzature security, tanto che rappresentano l'82% dell'intero volume di mercato.

ALTRI VERTICALI E PROSPETTIVE OTTIMISTICHE

La forza del mercato Security & Safety sta nella sua innovazione costante e nella competitività dei prezzi: la continua introduzione ed adozione di nuove tecnologie genera continue opportunità di mercato. Il segmento TVCC è il più importante e comprende IP video, registrazione, identificazione personale e sistemi di riconoscimento facciale. Nel 2015, i sistemi TVCC hanno totalizzato 1,2 miliardi di dollari (ovvero il 55% del complessivo mercato di attrezzature). Assieme a progetti di impianti sportivi e aggiornamento di infrastrutture e trasporti, il Governo russo ha stanziato circa 312 milioni di dollari nel corso del 2016 per implementare questa tecnologia presso stazioni di metro e treni, aree ed edifici pubblici. Oggi però i sistemi TVCC e di controllo accessi si fondono in un unico mercato, utilizzando applicazioni di cloud computing e immagini a maggiore risoluzione. Si registra anche una maggiore domanda di attrezzature antincendio e di soluzioni di gestione delle emergenze, inoltre, inoltre ci si concentra molto sulla prevenzione degli attacchi terroristici. In campo residenziale e commerciale gli allarmi e i servizi di sicurezza rappresentano un altro segmento promettente: negli ultimi tre anni ha raggiunto i 100 milioni di dollari di vendite. Ancora sul fronte dei servizi, tra i settori più promettenti si individuano il trasporto e la gestione di valori e contanti.

COSA SI VENDE DI PIÙ

A livello di vendita, le miglior performance per il 2016 e le previsioni di import per il 2017 sono rappresentate da: soluzioni IP-based (sorveglianza, rilevazione giorno/notte e sistemi infrarossi) soprattutto se di alta gamma; sistemi di controllo accessi; sistemi antintrusione/antincendio, specialmente per i luoghi pubblici; sistemi integrati; attrezzature biometriche, identificatori e lettori; dispositivi antiterrorismo, specialmente attrezzature per individuare esplosivi; sistemi antirapina, rilevazione radar e dispositivi per la registrazione; cloud computing per TVCC/sistemi di accesso; abbigliamento per la protezione personale di polizia/esercito. Secondo gli esperti, se non si verificheranno eventi finanziari o politici in grado di impattare negativamente sul mercato, questi dispositivi nei prossimi tre anni potrebbero registrare un tasso di crescita annuale del 10-15%.

SAFE CITY

Safe City è una rete automatizzata dotata di avanzati sistemi di allarme e risposta alle emergenze e include tutti i servizi e le agenzie municipali, controlla tutte le

strutture a rischio comunali, l'ambiente, strade e piazze. La somma spesa per il progetto Safe City è impressionante: 392,8 milioni di dollari ogni anno fino al 2018 per raggiungere una spesa totale di 2,1 miliardi di dollari. Il progetto Safe City verrà realizzato in tutte le città russe entro il 2020 e una spinta allo sviluppo verrà con la Coppa del mondo FIFA 2018. E' da rimarcare che già oggi Safe City si basa principalmente su prodotti e tecnologie estere, specialmente per la raccolta informazioni, i sistemi di comunicazione, l'analisi e l'elaborazione dati, i sistemi di informazione geografica e i sistemi di controllo del processo. Anche il segmento delle telecomunicazioni è dominato dai vendor stranieri (solo il 40% è russo). Soluzioni per connettere telecamere, sensori, control room; sistemi per trasferire, immagazzinare e analizzare immense quantità di dati, dispositivi IT ; software moderni: questi sono solo alcuni degli aspetti in cui è possibile un intervento nei progetti Safe City.

SPORT

Gli stadi a Kaliningrad, Rostov-on-Don, Samara, Saransk, Volgograd ed Ekaterinburg saranno tutti dotati di nuovi sistemi di sicurezza perimetrali, sistemi di controllo accessi per veicoli e staff, luci di emergenza e aree in sicurezza per telecomunicazioni e server. La spesa su questo capitolo supererà i 12 milioni di dollari. Lo stadio di Mosca Luzhniki sostituirà i sistemi TVCC per 500 mila dollari, mentre Ekaterinburg ha bisogno di un centro di comando nuovo, dotato delle ultime console di controllo, sorveglianza e tecnologie per le comunicazioni security. Secondo l'ufficio stampa del Ministro dello Sport il budget di Stato coprirà circa 453 milioni di dollari per garantire la sicurezza della Coppa del Mondo 2018.

Questo contributo si basa su più fonti: dalle interviste dirette a buyer in ambito Safe City, Retail, Oil&Gas, Industria, Trasporti, Banche ed Energia (che rappresentano l'82% del volume del mercato russo della security e che hanno visitato TB Forum powered by Intersec), ad altre fonti indirette: U.S. Department of Commerce, The Global Retail Theft Barometer, BMI Research, Memoori Research e media russi di punta quali Security&Safety Magazine.

RETAIL

Antenne Electronic Article Surveillance (EAS), etichette e tag sono state le soluzioni più popolari per evitare i furti, e sono utilizzate dal 73% dei retailer. Vengono ampiamente utilizzate soluzioni spider-wrap e pod/container security, tattiche di inventario avanzate, dispositivi con cavo sicuri.

OIL&GAS

La progettazione e installazione di attrezzature affidabili, sicure e robuste è una priorità nell'Oil & Gas, che richiede sistemi speciali per operare in ambienti pericolosi, marittimi e a rischio esplosioni. Sia che si tratti di sicurezza o controllo accessi in raffinerie, impianti di gas, linee, depositi o stoccaggio, i sistemi di sicurezza integrata sono necessari e richiedono i seguenti componenti: protezione perimetrale, videosorveglianza, controllo accessi, cancelli e barriere, citofoni, rilevazione intrusi perimetrale, Public Address Systems e Supporto e Servizi di Manutenzione.

soluzioni | tecnologie | normative

IP Security forum 2017

19ª edizione

NUOVA FORMULA

BARI • 26 MAGGIO 2017

un evento di:

ETHOSMEDIAGROUP

event.secsolution

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

in collaborazione con:

a&S ITALY
Tecnologie e soluzioni per la sicurezza professionale
www.asitaly.com

ETHOSACADEMY
informare & formare
www.ethosacademy.it

secsolution
security online magazine
www.secsolution.com

registrazione su: **www.ipsecurityforum.it**

IN UNA PAROLA, TANTE SOLUZIONI.

sferica.net

SiCUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

DOVE PRODOTTI E STRATEGIE CREANO SOLUZIONI

Fiera Milano, Rho

15 - 17 NOVEMBRE 2017

INTERNATIONAL NETWORK

BRASEG
BRAZILIAN TRADE SHOW FOR OCCUPATIONAL SAFETY AND HEALTH, AND FIRE PROTECTION
www.braseg.tmp.br

EXPOSEC
INTERNATIONAL SECURITY FAIR
www.exposec.com.br

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

www.sicurezza.it

FIERA MILANO

L'evoluzione della sicurezza per home e retail

In questi anni di crisi economica, e con il conseguente aumento dei furti in appartamento e attività commerciali, proteggere se stessi, la propria famiglia e la propria casa, e nel contempo avere la possibilità di controllare da remoto gli eventi attraverso tecnologie nuove e performanti, è diventata una necessità sempre più impellente.

Deatronic, da quasi 40 anni sul mercato nazionale antintrusione e videosorveglianza, offre soluzioni per la sicurezza per la casa e per le attività commerciali a 360 gradi. Grazie alla partnership con colossi mondiali quali CROW e alle soluzioni professionali TVCC HUAWEI, Deatronic si afferma quale leader fortemente consolidato nel settore sicurezza. Per essere sempre sicuri, protetti e videocontrollati.

SICUREZZA E CONTROLLO

Il nuovo sistema di allarme a marchio CROW che Deatronic lancia sul mercato è *Serenity™*.

Alte prestazioni, affidabilità e semplicità di utilizzo rendono *Serenity™* la soluzione ideale per applicazioni in ambito residenziale e piccolo commerciale. Il sistema permette infatti di tenere sotto controllo la gestione della propria casa, come pure della propria attività, coniugando sicurezza e controllo. *Serenity™* si presenta come una centrale di allarme completa e performante, caratterizzata da una forte componente innovativa.

UN'OPERA D'ARTE WIRELESS

L'innovativo sistema di allarme *Serenity™*, progettato per adattarsi all'ambiente come se fosse un'opera d'arte, si basa su una tecnologia

senza fili e totalmente wireless. Il display LCD grafico e la tastiera a sfioramento touch sense contribuiscono a un design piacevole. L'interazione touch e la nuova interfaccia utente basata su un display LCD grafico semplificano poi notevolmente la gestione quotidiana del sistema.

VIDEOVERIFICA DEGLI ALLARMI

Il primo vantaggio della centrale *Serenity™* è la videoverifica degli allarmi.
Con sensori a raggi infrarossi passivi con fotocamera incorporata, *Serenity™* permette di generare e trasmettere immagini immediatamente al manifestarsi dell'evento, attraverso notifiche e /o mail. E' evidente che l'immediata trasmissione delle immagini permette di intervenire con estrema tempestività e con la massima efficacia, perché le immagini consentono di individuare esattamente la tipologia di allarme e le migliori risposte da mettere in campo.

SEMPLICITÀ

Il secondo vantaggio della centrale *Serenity™* è la programmazione semplificata con tastiera touch screen. Il sistema touch, ormai di diffusione massiva grazie alla pervasività di smartphone e tablet, semplifica notevolmente la gestione quotidiana del sistema. Lato installatore, la programmazione e l'installazione sono facilitate.

CLOUD E REMOTAZIONE

Il terzo vantaggio di *Serenity™* è la sua gestione via cloud, che permette di controllare e gestire il sistema di allarmein qualsiasi momento e ovunque.
Gli altri punti di forza di *Serenity™* sono il controllo da remoto utilizzando un qualsiasi browser web o l'app per smartphone "CrowCloud", la trasmissione degli allarmi alle Vigilanze via TCP/IP e GSM/GPRS, la possibilità di verificare un allarme in corso attraverso la trasmissione di immagini via internet e l'utilizzo della tecnologia via radio bidirezionale.

TELECAMERE INTEGRATE

Inoltre, *Serenity™* fornisce una soluzione semplice per la sicurezza delle persone (anche anziani e disabili che rimangono soli in casa) grazie alle telecamere integrate su ogni sensore, sia esso da interno o da esterno, e integra funzioni di domotica come la gestione di luci, porte del garage, caldaie, condizionatori ecc.

CARATTERISTICHE TECNICHE

La Centrale di allarme *Serenity™* presenta queste caratteristiche principali: Full Radio con tastiera di comando touch-sense integrata, alimentatore 9Vcc 1,3Ah, dotata di 32 zone radio bidirezionali (2 zone filari a bordo scheda), 16 uscite radio (3 uscite filari a bordo scheda). Gestisce fino a 4 aree con 8 diversi programmi di inserimento, timer e fasce orarie. Completa di sirena piezo interna, comunicatore PSTN, ricetrasmettitore radio, modulo audio, microfono e altoparlante, modulo TCP/IP, lettore di prossimità (tag) e batteria 7,2 Vcc / 2,05 Ah (inclusa). Dotata di porta mini USB per la connessione al PC con il software di configurazione EasySerenity. Dimensioni (L x H x P) 291 x 165 x 35 mm. E' dotata inoltre di app per smartphone Android e iOS: CrowCloud Connect e App per tablet Android: Serenity Keypad.

IN SINTESI

Con *Serenity™* è possibile godere dell'esperienza davvero unica in materia di sicurezza, comodità e controllo. Sicurezza delle persone, controllo continuo e dovunque, domotica, alte prestazioni, affidabilità e semplicità di utilizzo rendono *Serenity™* la soluzione ideale per applicazioni in ambito residenziale e piccolo commerciale.

Deatronic
Via Giulianello, 1-7
00178 – Roma
Tel. (+39) 06 7612912
Fax (+39) 06 7612601
info@deatronic.com
www.deatronic.com/

Sistema di controllo accessi semplice, sicuro...IoT

exivo è il primo sistema professionale sul mercato per la gestione della sicurezza che sfrutta le possibilità offerte dall'Internet of Things, proposto in modalità "Software as a Service". Non è necessario, infatti, alcun PC o server dedicato: bastano il dispositivo di controllo del varco, la connessione di rete e un browser per accedere alla piattaforma Web based. I costi mensili sono chiari e modulari, in funzione della dimensione dell'impianto e dei servizi richiesti. La piattaforma centralizzata opera su server con altissimi standard di sicurezza, dunque la protezione dei dati degli utenti è garantita ai massimi livelli.

SEMPRE NUOVE FUNZIONI

Aggiornamenti periodici della piattaforma consentono non solo la stabilità del sistema, ma anche un continuo rilascio di nuove funzioni da utilizzare. È possibile gestire e utilizzare in autonomia, oppure - nella fase di configurazione e nell'utilizzo quotidiano - mediante il supporto di un partner specializzato e certificato dormakaba. La procedura per

progettare, ordinare e installare è facile e veloce: il sistema è estendibile in qualsiasi momento, semplicemente ordinando nuovi dispositivi e tessere direttamente dalla piattaforma Web. I dispositivi si configurano facilmente, in automatico, una volta installati e connessi. Il sistema, inoltre, supporta lettori online, wireless e consente di introdurre anche sistemi di chiusura meccanici. *exivo* è una soluzione facile e intuitiva, ma anche comoda e flessibile: è possibile, ad esempio, assegnare, modificare o revocare i diritti di accesso degli utenti in tutta semplicità e in qualsiasi momento.

I BENEFICI

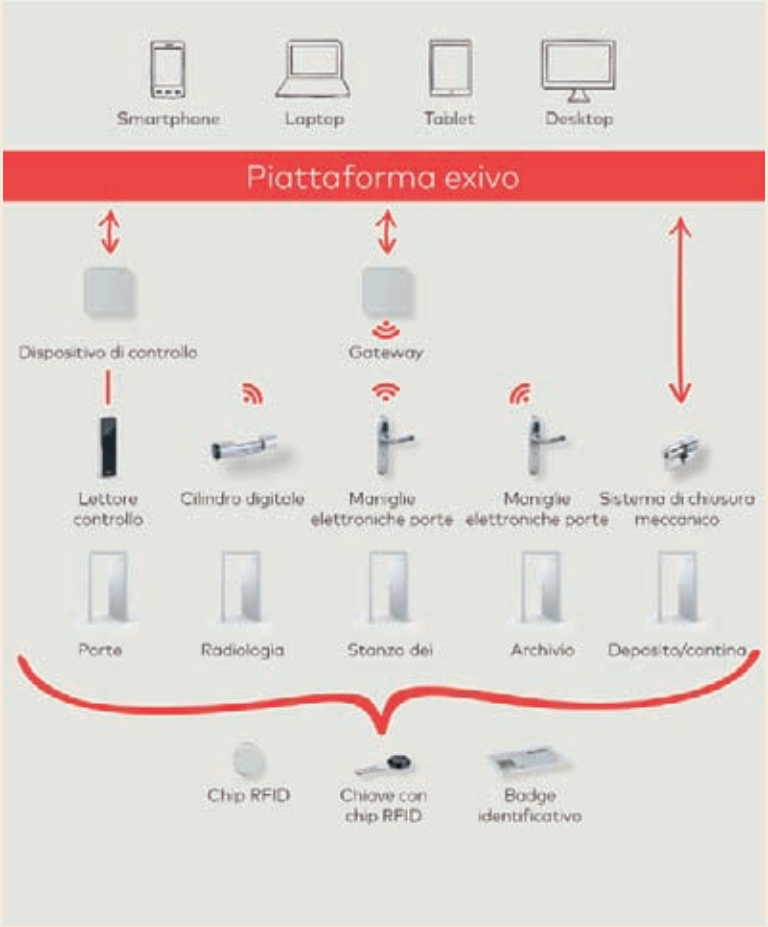
Tra i tanti vantaggi di *exivo*, segnaliamo: pianificazione e configurazione semplice tramite la piattaforma online; montaggio rapido senza alcuna

interruzione delle normali attività aziendali; semplice messa in servizio (grazie alla piattaforma centrale non sono necessari né un software particolare né un server dedicato); assegnazione e modifica dei diritti di accesso semplice e intuitiva; accesso da qualsiasi luogo tramite connessione Internet e controllo tramite smartphone, tablet; spese programmabili grazie a costi mensili costanti; retrofit su qualsiasi porta e varco; gestione integrata di chiavi e cilindri di chiusura meccanici (anche di aziende terze); semplice ampliamento delle funzioni grazie al continuo sviluppo della piattaforma; disponibilità immediata di aggiornamenti grazie alla funzione automatica di update della piattaforma centrale; massima sicurezza grazie alla gestione centralizzata su server sicuri e protetti.

EXIVO IN UNO STUDIO MEDICO

Oltre ai medicinali, alle sostanze chimiche e biologiche, nonché alle fonti di radiazioni per applicazioni medicali, i medici e i titolari degli studi devono proteggere anche costosi macchinari e informazioni riservate relative ai pazienti. Questo è ciò che prevede anche la Legge e non è un compito affatto facile in un contesto al quale hanno accesso con frequenza pazienti e fornitori.
La soluzione offre la massima sicurezza in modo semplice e a costi chiari e modulari.
Esigenze soddisfatte con *exivo*:

- Protezione di informazioni riservate sui pazienti
- Protezione dall'accesso non autorizzato a medicinali, sostanze chimiche e biologiche, nonché a fonti di radiazioni per applicazioni medicali



- Audit degli accessi in conformità con gli Istituti competenti di certificazione
- Accesso per il personale temporaneo e collaboratori esterni
- Protezione di infrastruttura e strumentazioni costose.

dormakaba italiana
www.dormakaba.it
Tel. +39 051 41 78311
Tel. +39 02 494842

Telecamere IP a prova di esplosione

Hikvision, numero uno al mondo nella produzione di sistemi e soluzioni innovative per videosorveglianza e security, ha rilasciato una nuova linea di telecamere IP, comprensive di modelli bullet e dome PTZ, certificate ATEX & IECEx per la resistenza in ambienti ad alto rischio. Si tratta di attrezzature estremamente robuste e capaci di resistere in atmosfere a rischio esplosione causata dalla presenza di miscela di gas, vapori o nebbie infiammabili o polveri combustibili (industrie metallurgiche, tessili, alimentari, estrattive, ospedaliere e farmaceutiche, aree con presenza di acidi e benzine hangar, aeroporti etc).

CERTIFICAZIONI

Le attrezzature che devono essere installate in zone a rischio di esplosione, compresi i dispositivi utilizzati all'interno o nei pressi di aree con atmosfere potenzialmente esplosive, rientrano nel campo di applicazione della Direttiva ATEX. La direttiva 2014/34/UE, entrata in vigore il 30 marzo 2014 e che ha abrogato la direttiva 94/9/CE dal 20 aprile 2016, impone la certificazione ATEX a tutti i prodotti commercializzati in UE, indipendentemente dal luogo di produzione, se installati in luoghi a rischio di esplosione (ad eccezione di casi particolari e ben codificati). Chi intende dunque immettere sul mercato europeo sistemi e dispositivi in aree a rischio esplosione deve mettere in campo le relative certificazioni. La prima è la certificazione ATEX, per l'appunto, e la seconda è la recente certificazione IECEx relativa ai prodotti elettrici destinati all'installazione in aree a rischio esplosione: uno schema internazionale volontario di certificazione delle apparecchiature

per l'uso in atmosfere esplosive che attesta la conformità ai relativi standard internazionali di prodotti e servizi.

A PROVA DI ESPLOSIONE

Hikvision sviluppa anche le soluzioni più specifiche per soddisfare sempre al meglio gli utenti dei principali mercati verticali: per gli ambienti a rischio esplosione, è disponibile una nuova linea di telecamere IP certificate ATEX & IECEx. Le ultime telecamere explosion-proof di Hikvision utilizzano custodie in acciaio Inox 304 e 316L che garantiscono la massima resistenza verso i rischi di corrosione ed esplosione, e sono certificate IP68 contro la possibile penetrazione di agenti dannosi quali acqua e polvere. Sono dunque ideali per applicazioni di sorveglianza in ambienti ad alto rischio, ove si impongono le massime performance video anche in presenza di materiali combustibili, come in impianti di estrazione di gas e petroli, nell'industria chimica e mineraria, in ambienti marini o altamente salini.

DARKFIGHTER

La nuova linea di telecamere explosion-proof incorpora la nota tecnologia DarkFighter di Hikvision, che garantisce la ripresa di immagini estremamente chiare e nitide anche in caso di luce decisamente fioca (fino a 0.005Lux in modalità colore e a 0.0005Lux in modalità bianco e nero).
Ad ulteriore sostegno e garanzia di qualità video, questa gamma di telecamere supporta peraltro sensori a scansione progressiva di tipo CMOS a 2MP e 4MP, risoluzione video full HD 1080p fino a 60 fps, triplo video stream, 3D Digital Noise Reduction e Wide Dynamic Range a 120dB.

H.265+ SMART CODEC

E per ridurre il consumo di banda (ed i notevoli costi di storage ad esso associati), queste nuove telecamere supportano il nuovo algoritmo di compressione brevettato da Hikvision H.265+.
Questo codec intelligente si basa sullo standard H.265/HEVC (High Efficiency Video Coding), al quale aggiunge però il vantaggio di ridurre drasticamente il bitrate di videosorveglianza attraverso tre tecnologie: Prediction Encoding, Noise Suppression (soppressione del rumore) e Bitrate Control.

ALL SMART

Ma non solo il codec in questa gamma è smart: oltre a supportare l'alimentazione 100v - 240V AC e PoE, la nuova linea explosion-proof di telecamere Hivision per usi in ambienti ostili e critici garantisce costanti performance video anche tramite altre funzioni intelligenti, quali: Smart Detection, Smart Tracking, ANPR etc. Queste telecamere supportano infine l'ingresso SD card per l'archiviazione a bordo fino a 128Gb.

I MODELLI

Per questa nuova linea di telecamere a prova di esplosione, attualmente sono disponibili il modello DS-2XE6222F-IS (2MP Explosion-Proof Network Bullet), il modello DS-2XE6242F-IS (4MP Explosion-Proof Network Bullet) e il modello DS-2DF6223-CX (W) (2MP Explosion-Proof Network Speed Dome).

Hikvision Italy
Via Abruzzo, 12
31029 - Vittorio Veneto (TV)
Tel. (+39) 0438 6902
Fax (+39) 0438 690299
www.hikvision.com/it

App iOS e Android per video verifica live

Le nuove versioni dell'APP VERSA CONTROL per iOS e per Android permettono la Video verifica e il controllo delle immagini in diretta dalle vostre telecamere da Smartphone e Tablet. L'integrazione della visualizzazione del video nell'App di casa SATEL rende più semplice e immediata la verifica dell'allarme, eliminando la necessità di passare in continuazione tra l'App dell'antifurto e l'App della videosorveglianza. Inoltre, l'interfaccia semplificata per la visualizzazione del video rende l'operazione più intuitiva per gli utenti meno esperti. E' possibile integrare telecamere IP, DVR o NVR semplicemente inserendo l'indirizzo del flusso video RTSP da visualizzare e non ci sono limiti al numero di telecamere collegabili. Non sarà più necessario attivare un servizio DDNS per la videosorveglianza poiché l'IP pubblico della rete viene rilevato automaticamente grazie al SATEL SERVER.

SICUREZZA SENZA RINUNCE

Con VERSA CONTROL l'utente può controllare da remoto la centrale VERSA PLUS, l'unica con ben 6 moduli integrati sulla scheda, dove tutti i vettori di comunicazione sono a disposizione dell'installatore per la configurazione e dell'utente per la gestione semplice, veloce sicura ed economica. L'integrazione di 6 moduli sulla scheda, la possibilità di un sistema ibrido o total wireless, permettono installazioni adatte a qualsiasi tipo di sito da proteggere, con il vantaggio di poter usufruire contemporaneamente di tutti i vettori disponibili. L'economicità di VERSA PLUS permette quindi la fruibilità del sistema per utenti e installatori esigenti senza costi di moduli aggiuntivi.

MODULI INTEGRATI

I moduli integrati sono: scheda di rete TCP/IP per gestione applicativi e per programmazione da remoto (ETHM-1 Integrato); linea telefonica PSTN (Integrato); GSM (Integrato con doppia SIM); GPRS (Integrato con doppia SIM); guida vocale (INT-VG Integrato); ascolto ambientale (INT-AV integrato).

GESTIONE DEL SISTEMA

La gestione e il controllo del sistema possono essere effettuati dall'utente tramite SMS, guida vocale interattiva abbinata sia alla linea telefonica PSTN che al GSM integrato, ascolto ambientale e tramite gli applicativi mobile.

SATEL SERVER

La peculiarità che rende ancora più accattivante la centrale VERSA PLUS è la possibilità di utilizzo del servizio server SATEL per applicativo mobile e telegestione, che permette la connessione attraverso il server dedicato per l'accesso senza configurazione del router. L'installatore pertanto può programmare e modificare delle impostazioni attraverso Ethernet e il modulo GPRS, con la facilitazione di aprire porte o configurare il router in automatico. Il Server SATEL offre un'assoluta immediatezza di configurazione e programmazione: in pochi minuti si accede all'applicativo mobile dedicato.

VERSA CONTROL

L'applicazione dedicata VERSA CONTROL per smartphone è gestita direttamente dalla scheda di rete ETHM-1 e il modulo GPRS integrati in centrale per una semplice e comoda gestione del sistema di sicurezza da remoto. L'immediatezza e la grafica accattivante rendono lo smartphone uno strumento indispensabile per la gestione quotidiana. Le versioni sono scaricabili gratuitamente per IOS e per Android e Windows. Con VERSA Control, da remoto è possibile: attivare e disattivare il sistema; cancellare allarmi; visualizzare lo stato del sistema; escludere o reincludere le zone; visualizzare gli eventi con funzione filtro; visualizzare i guasti con possibilità di cancellazione memoria; attivare e disattivare le uscite; notifiche PUSH.

EMAIL E NOTIFICHE PUSH

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

Satel Italia
Via Ischia Prima, 280
63066 Grottammare (AP)
Tel. (+39) 0735 588713
Fax (+39) 0735 579159
info@satel-italia.it
www.satel-italia.it

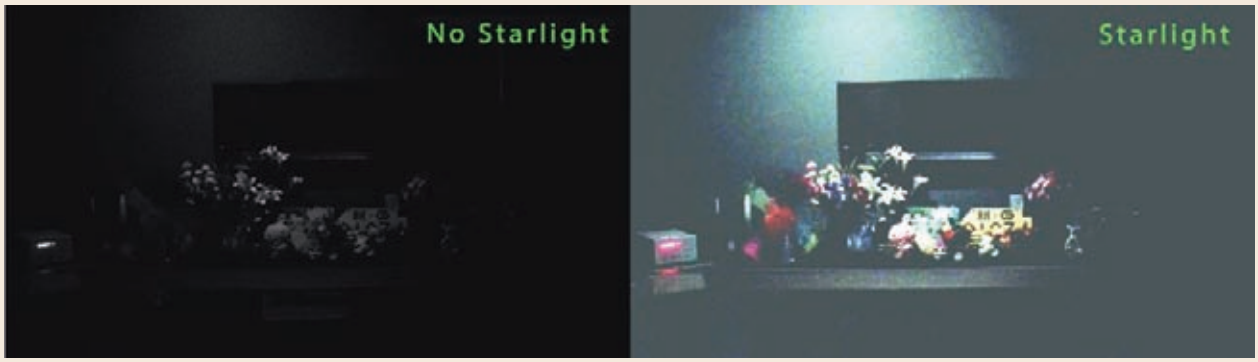
Zero cavi, più design e la garanzia a 5 anni

Tiandy, realtà appena sbarcata in Italia, ha sviluppato una telecamera focale fissa con tecnologia Starlight: il modello TC-NC214-S. La Gamma Cable Free mette al primo posto l'installatore e offre un articolo esteticamente gradevole e dal design poco invasivo, con linee eleganti e LED non visibili. Tiendy si è anche preoccupata del cablaggio necessario all'alimentazione delle telecamere, che tipicamente richiede l'uso di scatole esterne, ulteriormente invasive. Tiandy ha quindi sviluppato il prodotto partendo da queste linee guida:

1. telecamere Cable Free, prive di cavi e collegabili direttamente facendo arrivare il cavo di rete e la sua alimentazione (anche in PoE), garantendo così un'estetica più razionale, ma soprattutto semplificando l'installazione ed evitando scatole aggiuntive dove convogliare i cavi;
2. estetica decisamente gradevole dalle misure ridotte, vincitrici di molti premi;
3. IR non visibili, che garantisce una presenza discreta perché oggi, assieme alle caratteristiche tecniche, l'estetica è uno degli aspetti principali valutati dal cliente finale. Ma la differenza vera la fa il software! Infatti Tiandy esprime il meglio della sua Ricerca & Sviluppo proprio nei Firmware: tutte le telecamere contengono all'interno caratteristiche non presenti su prodotti della stessa fascia.

L'ANALISI VIDEO

Tutte le telecamere Tiandy integrano funzioni di analisi video come lo scavalcamento, l'abbandono oggetto e la rimozione oggetto, ma anche l'analisi di Parking, il Running, l'aggregazione folla e molto altro. Queste



funzioni sono integrate sulla Totalità dei prodotti Tiandy, che di fatto trasformano una comune telecamera in una soluzione decisamente più evoluta e completa.
Altre caratteristiche presenti che ne contraddistinguono gli indubbi vantaggi sono: 3Stream, che permette un ulteriore flusso di gestione; ROI, che garantisce una risoluzione più nitida dove necessario; SDCARD Slot, con una doppia funzione: la registrazione a bordo dell'evento che rende la telecamera indipendente e la garanzia di registrare in caso di perdita di risposta da parte del registratore, assicurando la continuità di servizio. Non va dimenticato poi che Tiandy è full Member Onvif. Tutti i prodotti sono in linea con le specifiche di protocollo, oltre a supportare nativamente prodotti come Milestone, Genetec, Axxon, Exacq, Digifort e molti altri.

STARLIGHT

Questo modello integra il supporto Starlight con visione a colori fino a 0.002 Lux, una delle chiavi fondamentali di casa Tiandy, che ritiene lo Starlight e la più recente tecnologia proprietaria Super Starlight due caratteristiche fondamentali oggi per telecamere ad uso esterno. Il perché è presto detto:

1. visione notturna ben oltre l'area tipica degli IR, senza essere vincolati quindi dal loro fascio;
2. nessun riflesso dovuto agli IR per oggetti vicini o per atti di manomissione (accecamento, etc.);
3. visione a colori che permette un miglior riconoscimento volti ed oggetti;
4. elevata nitidezza pari alla visione diurna che ne migliora decisamente la qualità di visione;
5. ridotti costi di illuminazione dell'area ripresa con un occhio all'aspetto green dell'impianto;
6. maggiore privacy poiché l'area scelta può essere sorvegliata anche con una illuminazione ridotta.

Il prodotto Tiandy arriva con l'obiettivo di coprire una fascia di mercato professionale che cerca, oltre al prodotto migliore, anche una realtà capace di assicurare qualità nel tempo e politiche di marginalità adeguate. Questo è uno dei primi obiettivi sul quale Tiandy lavora, offrendo inoltre una logica di garanzia completamente diversa: la garanzia diretta del produttore che alleggerisce l'installatore dalla gestione della riparazione. La scelta di Tiandy ha richiesto enormi investimenti, ma ha portato a due nuovi modi di gestire la continuità di servizio, tema sempre molto caro agli installatori. La sicurezza data dalla videosorveglianza oggi richiede continuità e, in caso di guasto, costringe gli installatori a dover gestire "muletti" in autonomia senza alcun supporto dal produttore. Tiandy ha deciso di affrontare questo aspetto dando l'opportunità di ottenere fino a 5 anni di garanzia sul prodotto e fino a 36 mesi di cambio prodotto immediato in caso di guasto.
Queste due modalità di acquisto prodotto permettono oggi di assicurare un nuovo standard di servizio: si vedrà come il canale affronterà tutto questo, ma di certo è una dimostrazione di sicurezza sulla propria qualità.

Tiandy Italia
sales@tiandy.it
www.tiandy.it

La videosorveglianza IP alla fase 3.0

Le reti e la loro complessità, ma anche le grandi opportunità di cablaggi per gli edifici, hanno rappresentato negli ultimi vent'anni la vera innovazione nell'impiantistica speciale, sia nel settore industriale e terziario, sia nel settore residenziale. Una delle molteplici applicazioni riguarda senz'altro il mondo della videosorveglianza, idonea a grandi strutture e grandi impianti, che ha mosso i primi passi semplificando il cablaggio degli impianti senza aggiungere ulteriori plus; di contro la complessità della programmazione degli apparati di rete, nonché delle apparecchiature destinate alla TVCC, ne hanno rallentato lo sviluppo, tenendo stagnante per oltre un decennio il settore della videosorveglianza su IP. L'evolversi della tecnologia degli apparati di rete, ma soprattutto degli stessi componenti come telecamere e apparati di videoregistrazione, ha portato ad un aumento notevole della qualità e della fruibilità delle immagini per le prime, così come la gestione di hard disk ad altissima capacità, oltre che di microprocessori ad altissima elaborazione, hanno consentito ai videoregistratori e alle telecamere IP una concreta applicazione.

COMPRESSIONE H265 E 4K

La nuova compressione video H265 lancia, definitivamente, le applicazioni della videosorveglianza su IP su larga scala, ormai proiettate a soppiantare nel breve termine la tecnologia analogica, che sarà sempre più povera di sviluppi e nuove funzioni, mentre il protocollo High Efficiency Video Coding (HEVC) H265 permette la semplice gestione di immagini oltre la risoluzione 4K, ormai una standard mondiale nel video. Visto il dimezzamento della quantità di banda sulle reti, la HEVC porta, pertanto, al raddoppio della capacità di reti già esistenti, rendendo possibile la gestione di grandi impianti con telecamere in 4K. Va da sé che a benefi-

ciare della notevole riduzione di banda sono gli apparati di videoregistrazione che, operando sempre in H265, archiviano con semplicità - e sempre più alta affidabilità - una notevole quantità di telecamere ad altissima risoluzione su hard disk di medie dimensioni, riducendo così le dimensioni degli NVR.
Ma la vera rivoluzione che ha portato l'H265 nella videosorveglianza è rappresentata dalle innovazioni che grandi aziende, come UNIVIEW(UNV), partner EUROTEK nel mercato italiano dal 2015, hanno portato avanti, dotando di smart function tutta la gamma di telecamere IP da tempo in H265.

UN FUTURO SMART

Le attuali telecamere IP sul catalogo EUROTEK - siano esse bullet, dome, fisheye, speed dome - tutte in H265, da 4 a 12 Megapixel, incorporano infatti speciali funzioni smart. Ad esempio la funzione *crossing line*, destinata ad aumentare e ottimizzare le protezioni perimetrali nella antintrusione, nonché la possibilità di delimitare un'area nell'immagine (area protetta) per facilitare la protezione su siti mobili, come cantieri mobili o deposito automezzi (*intrusion detection*), o altre funzioni come il conteggio delle persone (*people counting*) o il *face detection*, particolarmente adatte ad applicazioni nel retail e nella grande distribuzione. Completa la lista delle funzioni speciali l'*auto tracking* sulle speed dome di UNIVIEW, che rende estremamente efficace il controllo di grandi aree in esterno.

COMPRESSIONE HEVC

Notevoli benefici della compressione HEVC si ricavano poi nella centralizzazione delle immagini sia della singola telecamera che dell'NVR, che consentono di gestire con efficacia e velocità allarmi ed eventi, così come notevoli sono i vantaggi sulla APP di UNIVIEW con immagini in live, per una gestione totale degli impianti e per ricevere notifiche in ogni caso di evento.

MASSIMA SENSIBILITÀ

La compressione H265, unitamente alla funzione Starlight, rivoluziona poi l'applicazione delle telecamere IP di UNIVIEV soprattutto in aree esterne o a scarsa luminosità: la sensibilità della gamma Starlight è infatti circa dieci volte superiore allo standard, garantendo immagini chiare ed a colori con la semplice illuminazione tenue e riflessa fino a 0,002 Lux.
UNIVIEW aggiunge ancor più valore a queste innovazioni tecnologiche implementando l'H265 con un algoritmo proprietario definito U-code, che riduce l'archiviazione delle immagini fino ad oltre l'80%, permettendo così un elevato storage delle immagini. Già alcuni modelli ne sono dotati, ma ben presto questo concreto plus sarà presente su tutta la gamma delle telecamere IP di UNIVIEW.

LONG RANGE POE

Non ultima, ma di notevole importanza, la connessione Long Range PoE: permette un cablaggio con un semplice cavo di rete cat.5E tra un NVR UNV con Switch PoE e le telecamere IP UNV fino ad un massimo di 300 metri.
Completa la semplicità di gestione delle apparecchiature di videoregistrazione IP UNIVIEW, il Plug and Play ed autoconfigurazione tra NVR e telecamera dei flussi video. Considerando ancora la ricerca intelligente (smart search) e la sicurezza della rete (higher security), possiamo affermare che la videosorveglianza è ormai IP. EUROTEK, fin dal 2006, ha creduto nella videosorveglianza IP diffondendo da prima il concetto dei sistemi ibridi con la taiwanese AVERMEDIA, e adesso puntando fortemente sull'IP insieme ad UNIVIEW.

Eurotek
Via Gabriele d'Annunzio 22/D
20016 Pero (MI)
Tel. (+39) 02 33910177
acquisti@eurotek-srl.it
www.eurotek-srl.it

Nuovo chipset per telecamere con prestazioni estreme

Hanwha Techwin, leader mondiale del settore sicurezza, lancia la serie Wisenet X, una nuova famiglia di telecamere dotata di un chipset proprietario integrato e destinata a diventare un punto di riferimento per il mercato. Il chipset Wisenet 5 montato sulla serie Wisenet X offre altissime prestazioni, ed è al centro del vantaggio competitivo tecnologico di Hanwha Techwin. La serie Wisenet X è la prima famiglia di prodotti a usare questa soluzione a chip singolo. La gamma di telecamere da 5 megapixel e 2 megapixel rappresenta il nuovo punto di riferimento per il settore, non solo per le immagini straordinariamente nitide che le telecamere sono in grado di offrire, ma anche grazie alla maggiore velocità di elaborazione delle immagini e alle funzionalità potenziate. La serie Wisenet X offre inoltre WDR a 150 dB, stabilizzazione digitale dell'immagine tramite giroscopio e immagini nitidissime 24 ore al giorno grazie al miglioramento delle prestazioni con scarsa illuminazione. Inoltre, con l'esclusiva tecnologia di compressione WiseStream II di Hanwha Techwin, la serie Wisenet X offre livelli di efficienza e flessibilità di utilizzo che la contraddistinguono notevolmente rispetto alla media. Ma ci sono molti altri notevoli vantaggi, tra cui una gran varietà di applicazioni di analitica integrate a disposizione.

Immagini nitide senza sfocature - Con l'attuale tecnologia WDR un'immagine viene catturata componendo 2 frame con esposizioni diverse, mentre la serie Wisenet X con WDR a 150 dB usa 4 frame per creare un'immagine più naturale. La nuova tecnologia è stata sviluppata per rimuovere le sfocature offrendo immagini definite e vivide.

Giroscopio = Stabilizzazione più precisa - Il giroscopio è stato aggiunto alla tecnologia attualmente utilizzata nelle telecamere per ottenere una stabilizzazione più precisa, che si attiva quando vento o vibrazioni disturbano la normale operazione della telecamera, rendendo più stabili le immagini.

Colori anche con scarsa illuminazione - Il nuovo chipset montato sulla serie Wisenet X e l'avanzatissima tecnologia delle ottiche Hanwha Techwin permettono di visualizzare immagini a colori anche in ambienti con scarsa illuminazione senza l'uso di LED IR. Infatti, ora è possibile catturare immagini vivide a prescindere dall'ambiente e dall'orario di ripresa.

Oltre il 99% di dati in meno - Le telecamere Wisenet X sono dotate di compressione H.265 e WiseStream II, una tecnologia di compressione complementare che controlla dinamicamente la codifica dei dati, bilanciando qualità e livello di compressione in base alla quantità di movimento presente nella ripresa. Quando WiseStream II viene combinata alla compressione H.265, l'efficienza delle risorse di rete può essere migliorata fino ad oltre il 99% rispetto all'attuale tecnologia H.264. Una caratteristica importante, che rappresenta un notevole elemento di differenziazione delle telecamere della serie Wisenet X rispetto alla media di mercato.

Maggiore scelta di app di analisi - La serie Wisenet X offre molte e utili applicazioni di analisi. La funzione di analisi audio riconosce suoni critici come spari di arma da fuoco, esplosioni, grida e vetri rotti e fa scattare immediatamente l'allarme. Tra le altre applicazioni di analisi troviamo inoltre la gestione code, un'altra importante funzionalità che analizza le code che si formano in un negozio o in una banca per permetterne una gestione più efficiente.

Doppio alloggio SD e installazione via USB - Tramite la porta USB, la serie Wisenet X è in grado di collegare telecamere e dispositivi mobili via Wi-Fi. È' possibile verificare gli angoli di visione mentre si effettua l'installazione via smartphone. Il doppio alloggio per schede SD permette di salvare automaticamente sulla telecamera fino a 512 GB tenendo i dati al sicuro in caso di problemi di rete.

Per tutte le esigenze - La gamma di telecamere Wisenet X comprende tipologie di prodotti per varie applicazioni e varie modalità d'installazione, sia in interni che in esterno. Con la serie Wisenet X, Hanwha Techwin arriva a soddisfare la domanda di mercato proveniente da qualsiasi area della videosorveglianza. Con l'aggiunta della serie Wisenet X alle altre serie di recente lancio Wisenet Q e P, Hanwha Techwin ha formato una famiglia di prodotti completa, che va da dispositivi di livello base e dai costi contenuti a prodotti competitivi ad alte prestazioni, capaci di soddisfare sia le esigenze progettuali che le necessità dei clienti in tutti i settori verticali.

Hanwha Techwin Europe Ltd
Viale Brianza, 181
20092 Cinisello Balsamo (MI)
hte.italy@hanwha.com
www.hanwha-security.eu/it

La Redazione

Cosa riserva il 2017 per le imprese leader della vigilanza privata in Italia

Secondo le ultime rilevazioni dello Studio di Settore Plimsoll(*) "Servizi di Vigilanza Privata" (Novembre, 2016), che esamina le 634 imprese che controllano il 90% del mercato italiano, nell'ultimo anno, le imprese leader sono cresciute in media del 2,2% rispetto all'anno precedente, invertendo il trend negativo rilevato nel 2015 (-1%). Tuttavia, sebbene il volume di affari generato nell'ultimo anno sia pari a 3 miliardi di euro, gli elevati costi sostenuti per l'esercizio delle attività di vigilanza (armata e non) rendono l'attività di impresa mediamente poco redditizia.

(*) Plimsoll Publishing è leader mondiale nella pubblicazione di report di settore. Strumenti quotidiani di valutazione per dirigenti e manager da quasi 30 anni, gli studi Plimsoll costituiscono l'analisi più attendibile e approfondita delle performance commerciali e finanziarie di imprese in tutto il mondo. Con oltre 400 settori e microsettori monitorati ogni anno in Italia e 8000 in Europa, Plimsoll fornisce un'analisi intuitiva e dettagliata sulle imprese leader di ogni settore, sulle società a rischio e su quelle da tenere sotto osservazione. Attraverso l'esame degli ultimi 4 bilanci e con l'ausilio di grafici e classifiche di rendimento, ciascun report fornisce una diagnosi efficace sullo stato di salute di ogni impresa di un settore, ne esprime una stima del potenziale di crescita, ne valuta il valore di mercato e l'attrattività come obiettivo di acquisizione.

Buone notizie per il settore della vigilanza privata in Italia. Nell'ultimo anno, le imprese leader del mercato sono cresciute in media del 2,2% rispetto all'anno precedente, invertendo il trend negativo rilevato nel 2015 (-1%). Francia, Regno Unito e Spagna sono anche col segno più, con le imprese d'Oltremanica che registrano un +4,7%, le spagnole un +3,2% e le francesi un modesto +0,8%. Eppure, volgendo lo sguardo ai margini di profitto – quanti euro di utile lordo un'impresa genera da 100 euro di fatturato – emerge che le società italiane raggiungono a stento l'1%, contro i 3,9% delle controparti francesi, il 2,1% delle britanniche e l'1,8% delle iberiche. Lo Studio di Settore Plimsoll(*) "Servizi di Vigilanza Privata" (Novembre, 2016), nell'esaminare individualmente le 634 imprese che controllano il 90% del mercato italiano, evidenzia che, sebbene il volume di affari generato nell'ultimo anno sia pari a 3 miliardi di euro, gli elevati costi sostenuti per l'esercizio delle attività di vigilanza (armata e non) rendono l'attività di impresa mediamente poco redditizia.

CHI VINCE E CHI PERDE

Una impresa su 4, in particolare, è in perdita e poco più di 50 operatori sono stati in grado di migliorare la propria gestione operativa e incrementare i ritorni sulle vendite. Eppure ci sono anche imprese in buona salute: l'esame degli ultimi 4 bilanci e dei livelli di liquidità, stabilità operativa ed equilibrio del circolante aiutano a capire cosa abbiano in comune le aziende più redditizie e cosa facciano di diverso rispetto al resto del settore. Il team Plimsoll, che si è occupato della rilevazione dei dati e della stesura dello studio, evidenzia che uno dei fattori che maggiormente incide nella scarsa profittabilità delle società italiane sono i costi operativi, mediamente più alti rispetto a quelli sostenuti dalle controparti europee, che si servono in larga parte di società terze per la fornitura di personale. Un'ulteriore causa del mancato sviluppo del mercato della vigilanza privata è da ricercarsi nell'estrema frammentazione territoriale degli operatori italiani, che tendono ad operare su scala locale e stentano pertanto a realizzare significative economie di scala, soprattutto in presenza di una molteplicità di piccole-medie aziende intimamente connesse con il tessuto imprenditoriale comunale che competono per aggiudicarsi nuovi appalti. Una delle soluzioni per migliorare la redditività generale del settore sarebbe quindi quella di stimolare operazioni di acquisizione e consolidamento: un numero minore di società in un'area geografica specifica avrebbe maggiori prospettive di espansione e crescita, oltre che di riduzione dei costi. Lo studio Plimsoll evidenzia la presenza di 45 imprese con elevati livelli di liquidità che avrebbero i mezzi e la solidità finanziaria necessaria per crescere attraverso acquisizioni. Specularmente, 54 società italiane con fatturato inferiore ai 5 milioni di euro risultano al momento sottovalutate e vengono identificate come "potenziali obiettivi di acquisizione": sotto una compagine societaria differente, potrebbero sensibilmente migliorare i propri ritorni sugli investimenti, attualmente compressi da significativi oneri finanziari e debiti a medio termine.

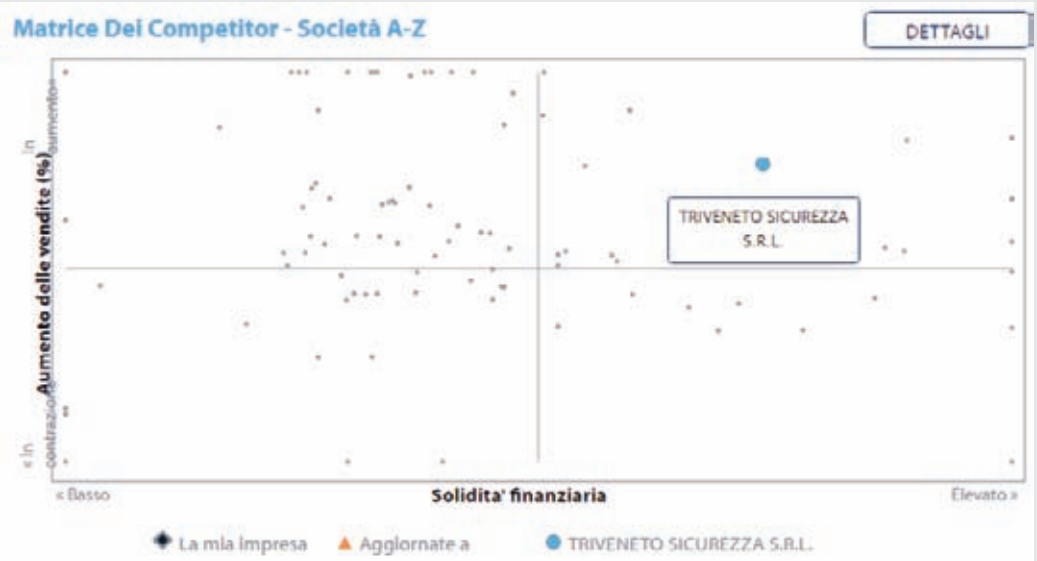
Per ulteriori e più dettagliate informazioni, potete consultare http://media.secsolution.com alla sezione libri-pubblicazioni: il sito è abilitato alla vendita online della versione full (comprensiva del volume in formato digitale e dell'accesso al Sito web per 12 mesi e nuovi bilanci) o della versione "solo studio" in PDF. Info: media@ethosmedia.it

CON I MIGLIORI AUSPICI

Nella pagina successiva, compariamo i posizionamenti competitivi di alcune imprese sulla base essenzialmente di due indicatori: andamento delle vendite e solidità finanziaria. A colpo d'occhio è possibile individuare le imprese più redditizie (che crescono cioè in fatturato e profitto), quelle che crescono in volumi d'affari ma senza un corretto equilibrio finanziario, quelle tendenzialmente in perdita e quelle, pur profittevoli e snelle, che rischiano però di perdere troppo fatturato.

L'auspicio per il 2017 è che il settore della vigilanza privata in Italia mantenga il trend di crescita positivo ottenuto nelle ultime rilevazioni ma che riesca nel contempo ad efficientare i propri processi operativi e organizzativi, magari intraprendendo politiche audaci volti a rafforzare la propria posizione sul mercato anche attraverso operazioni di acquisizione.

MATRICE DI POSIZIONAMENTO



La matrice dei competitor Plimsoll è uno strumento di benchmark che definisce il posizionamento di un'impresa rispetto ai propri competitor sulla base di due indicatori: andamento delle vendite e solidità finanziaria. Ciascuna impresa è identificata da un puntore: quanto più il puntore di un'azienda è posizionato verso l'alto tanto più l'azienda è in crescita rispetto all'anno precedente; quanto più il punto si sposta verso destra, tanto più l'azienda è redditizia e capace di ripagare i propri debiti commerciali e finanziari. La matrice è pertanto suddivisa in 4 quadranti. TRIVENETO SICUREZZA e tutte le imprese posizionate nel quadrante in alto a destra si configurano come le imprese più sane e vibranti del mercato: sono in crescita e hanno dei margini di profitto positivo, sufficienti a ripagare in misura congrua il capitale di debito e la proprietà. Il quadrante in alto a sinistra identifica le imprese che stanno aumentando i propri volumi d'affari a ritmi significativi, ma che non hanno ancora raggiunto un equilibrio finanziario soddisfacente: alcune di esse operano in perdita pur essendosi aggiudicati lucrosi appalti.
Il quadrante in basso a sinistra nell'immagine è popolato da imprese che – come SICURCENTER SPA - stanno perdendo quote di mercato e, contestualmente, stanno aumentando i propri debiti: si tratta di società tendenzialmente in perdita, che dovranno invertire la rotta nei prossimi 12-24 mesi per riguadagnare competitività. Le aziende posizionate sul quadrante in basso a destra hanno contratto i propri volumi di fatturato ma si trovano fuori dall'area di pericolo: si tratta di realtà molto snelle, profittevoli ma che rischiano, con l'erosione continua di fatturato, di osservare un deterioramento dei propri conti e di finire nel primo quadrante.

VITTORIO VENETO (TV)

Convergenza al calcio d'inizio:

Hikvision Total Solution Provider

"I guerrieri vittoriosi prima vincono e poi vanno in guerra", ossia: per vincere bisogna assicurarsi la vittoria mettendo preventivamente in campo uomini, mezzi, strumenti, progetti, idee e knowhow necessari per arrivare in battaglia con la certezza del successo. Questo il leit-motiv che ha accompagnato i due giorni di confronto e condivisione sulle strategie Hikvision per il 2017. Un confronto serrato, come serratissima è la tabella di marcia di Hikvision per il prossimo triennio. Con una chiusura del 2016 a + 33% rispetto al 2015, gli obiettivi 2017 parlano di 41% di market share in Italia e 50 milioni di fatturato. Un traguardo impegnativo soprattutto perché i distributori dovranno uscire dal sicuro perimetro della videosorveglianza, dove in soli quattro anni Hikvision ha conquistato la leadership, per abbracciare antintrusione, intercom, controllo accessi, sistemi di trasmissione video. Fulcro e perno di questa strategia di sviluppo è la piattaforma iVMS, che nella videosorveglianza aggiungerà feature e perfezionerà controlli, ma soprattutto accoglierà tutti i segmenti della security: intercom, controllo accessi, antintrusione. Il software diverrà dunque il cuore pulsante di più sistemi evoluti e convergenti, consacrando Hikvision nella sua nuova natura di Total Solution Provider. La convergenza è solo al calcio d'inizio.

www.hikvision.com/it

MILANO

From Risk to Resilience:

l'evento europeo di ASIS

Sarà Carlo Purassanta, General Manager di Microsoft Italia, a tenere il discorso inaugurale di ASIS Europe 2017 (Milano, 29/31 marzo) a tema " HYPERLINK "http://www.secsolution.com/notizia.asp?id=7121" \n _selfFrom Risk to Resilience". Purassanta metterà a disposizione le proprie conoscenze sul business digitale e sulla sua evoluzione, per aiutare a comprendere le necessità presenti e future delle imprese, dei consumatori e delle comunità, fissando i parametri ai quali i professionisti della sicurezza dovranno fare riferimento. Seguirà il dibattito tra i Security Leader a tema "Protecting Borderless Business". Rappresentanti di settori chiave dell'industria illustreranno i rischi e le sfide per gli operatori della sicurezza, dalla tecnologia in tutte le sue declinazioni, alle minacce cyber. Già confermata la partecipazione di Jaya Baloo (CISO, KPN), Werner Cooreman (CPP, PSP, Sr Vice President, Group Security Director, Solvay) ed Edmond d'Arvieu (CPP, VP Corporate Security, Sanofi). Il dibattito sarà moderato dal Prof. Martin Gill (Director, Perpetuity Research). Al convegno interverrà anche Gensèric Cantournet, Chief Security Officer della Rai, con uno speech sulla creazione di una struttura integrata della sicurezza a livello aziendale. Master Class, Executive Session e workshop formativi completano il programma dell'evento, che ospita anche il primo ASIS Europe Career Centre e una Technology & Solutions Track contemporanea all'esposizione.

www.asiseurope.org

MILANO

Panasonic e A.I.P.S.

unite nella formazione

Il 7 febbraio Panasonic ha organizzato con AIPS, Associazione Installatori Professionali di Sicurezza, un nuovo appuntamento formativo presso la propria sede.

Massimo Grassi, Sales Engineer, ha descritto *Panasonic Secure Communication*, una nuova soluzione che protegge i sistemi video IP dai pirati informatici e assicura la privacy nella trasmissione delle immagini sulla rete. Il suo intervento seguiva ed arricchiva la presentazione offerta durante la scorsa edizione del seminario (aprile 2016) sul passaggio dallo Smart Coding all'H.265 e sull'evoluzione tecnologica raggiunta nell'ambito della compressione a salvaguardia della qualità delle immagini. In questa edizione del seminario ci si è addentrati nei vantaggi della *Secure Communication* per gli installatori, dando risposta alle sempre più diffuse esigenze di ridurre la banda e di disporre di impianti al 100% certificati, secondo la legge.

E' seguito poi il contributo del Consigliere AIPS, Leonardo Lomma, sulle norme CEI 50132-7 e CEI EN 62676-4, e si è infine parlato di modulistica (Foglio di sopralluogo per impianti TVCC, Check-List per la manutenzione, etc) assieme a Matteo Sassanelli di A.I.P.S.

A fine lavori i partecipanti hanno svolto un test per verificare l'acquisizione delle competenze.

http://business.panasonic.it

SAN ZENO NAVIGLIO (BS)

Analisi evoluta delle targhe

a favore di smart city

Polizia, Vigili e Carabinieri, Sindaci, Vicesindaci ed Assessori: era altamente profilato il pubblico della giornata di studio targata surveye, Vigilate che si è tenuta il 23 febbraio scorso presso Sicurtec Brescia. L'originalità del tema - "La lettura targhe al servizio della collettività"- ed una modalità narrativa accattivante e moderna hanno portato l'uditorio in un 2020 dominato dalle informazioni, dove la tecnologia semplifica la vita degli amministratori locali e degli stessi cittadini. Lo scenario è quello della smart city, ma non è fantascientifico. Città più sicure, meno care, prive di sprechi, con servizi urbani di qualità, viabilità ordinata e rispetto per l'ambiente sono una realtà possibile già oggi. E con tecnologie già familiari alle Amministrazioni Locali., come la piattaforma X Scanner di Vigilate che gestisce, anche via *mobile*, i sistemi di lettura targhe per finalità sanzionatorie, investigative e di monitoraggio del traffico, servendo però più utenti ed interfacciandosi con le librerie ministeriali. Un "gestore di dati", dunque, essenziale per chiunque debba amministrare ecosistemi complessi e interconnessi, che richiedono informazioni, rapide, mirate e nel rispetto delle normative (a partire da quella privacy).

www.surveye.it

DUBAI (UAE)

Mercato in crescita:

il segreto di Intersec 2017

Un mercato in crescita che garantisce numeri di rilievo a Intersec. Questa la chiosa della 19a edizione della manifestazione, che si è svolta dal 22 al 24 gennaio a Dubai. Organizzata da Messe Frankfurt Middle East GmbH, la fiera ha ospitato circa 1300 espositori su una superficie di 56.000 mq, e ha accolto 33.500 visitatori da 129 paesi (51% internazionali). Forte la presenza degli espositori dall'Italia, al 7° posto nella Top Ten dei paesi per numero di espositori, nonostante – come *a&s Italy* ha rilevato, unitamente agli altri connazionali presenti - la scarsa visibilità dell'area collettiva, se paragonata, ad esempio, ai vivaci e potenti allestimenti di Gran Bretagna e Germania. Intersec è stata comunque l'occasione per esporre anche il progetto della fiera SICUREZZA, che quest'anno coinvolgerà anche il festival ICT. Il 23 gennaio, presso Il Conrad Hotel Dubai, Giuseppe Garri, Exhibition Manager di Sicurezza, nel presentare al pubblico internazionale l'edizione 2017 della manifestazione, ha anticipato una collaborazione decisiva nel segno della convergenza tra sicurezza logica e fisica: l'inclusione del festival ICT all'interno di SICUREZZA 2017come grande momento formativo ed espositivo che ne completa l'offerta.

www.intersecexpo.com

MILANO

Dahua Videotrend

"Together to the future"

Il Cinema The Space di Vimercate, lo scorso 18 gennaio, è stato sede del kickoff Dahua-Videotrend, *Together to the future*. Oltre 300 tra i principali player del mondo della security hanno condiviso i risultati del lavoro svolto nel 2016 da Videotrend, il cui CEO Pasquale Totaro ha anticipato che, anche grazie a una nuova partnership con Dahua, gli investimenti nel 2017 saranno davvero rilevanti. La nuova identità di Dahua, la più decisa strategia a breve, medio e lungo respiro tratteggiano un percorso che l'azienda intende compiere insieme ai partner. L'apertura è ampia anche sul versante project, con soluzioni e sistemi avanzati che coinvolgeranno attori di primo piano, come ha anticipato Luca Pari, project sales manager Dahua Italia: un autentico "Mondo Dahua", in cui convergono anche altri fattori ritenuti fondamentali, quali comunicazione, marketing e investimenti in brand awareness. Al termine dell'incontro è stato posto l'accento anche su un altro "valore" in cui l'azienda crede molto, quello della formazione: Tiziano Chiarini, responsabile formazione tecnica della nuova Dahua Academy, ha infatti parlato di una vera e propria "università" di formazione tecnica avanzata e delle iniziative in programma per il 2017.

www.dahuasecurity.com/it

MILANO

Axis 3.0,

soluzioni integrate per un mondo safe & smart

Una giornata interattiva e dal format originale, quella organizzata da Axis Communications presso lo Spazio MIL di Sesto San Giovanni (MI) il 15/12/2016. Dedicata agli operatori della sicurezza e agli utenti di alcuni mercati verticali, la giornata "Axis 3.0" ha presentato le novità e le soluzioni video di rete integrate con il controllo accessi, le funzionalità audio e i software intelligenti. È stata inoltre l'occasione per festeggiare i 20 anni dal lancio della prima telecamera di rete al mondo, delineare la visione, le prospettive, le strategie dell'azienda, costantemente motivata, anzi "ispirata", come ha esordito Edvige Maury, Responsabile della regione Sud Europa: "dall'innovazione, da una visione a lungo termine, dalla sostenibilità, al fine di contribuire a creare un mondo più smart e più sicuro, grazie alle soluzioni integrate, che pongono al centro il cliente e le sue esigenze". La giornata aperta, a cui erano presenti il management Axis Communications Southern Europe e i migliori partner tecnologici dell'azienda, è stata caratterizzata da un approccio esperienziale per il pubblico coinvolto, che ha preso parte alle visite interattive in alcuni scenari tipici di utilizzo, ricreati con grande cura di particolari, e all'applicazione in diretta delle soluzioni di videosorveglianza e business intelligence firmate Axis.

www.axis.com

TAIPEI (TW)

La security intelligente

a Secutech 2017

26.000 professionisti della sicurezza da tutto il mondo sono attesi a Secutech, dal 12 al 14 aprile 2017 a Taipei per scoprire il valore delle soluzioni intelligenti per la security, presentate da circa 450 espositori. In fiera si parlerà di Smart Retail con un negozio demo che mostrerà sistemi per l'EAS, telecamere panoramiche e giorno/notte, analisi dei punti caldi, sistemi POS, e-Tag, e piattaforme per la gestione back-end. Anche la Smart Factory avrà il suo posto in fiera con le tecnologie e i sistemi chiave che caratterizzano l'Industria 4.0, inclusi l'AOI, la machine vision, l'automazione industriale, la gestione energetica e tanto altro. Presenze irrinunciabili, le sezioni sul Trasporto Intelligente e le Safe City, con dimostrazioni sulla gestione del traffico, dei parcheggi e delle flotte, attrezzature di sicurezza mobile e dispositivi per la sicurezza personale. Non c'è Safe City senza Edifici Intelligenti, per questo verranno esposte soluzioni per il settore residenziale, commerciale e industriale, toccando anche i temi della BIM & MQTT, building automation, gestione security e safety. Segnaliamo inoltre SMAhome Expo, con soluzioni pronte all'uso, e il programma formativo nell'ambito di Apple HomeKit Gallery & Seminar, Z-Wave Academy e Cloud Service Platform Conference.

www.secutech.com

BARCELLONA (ES)

Security Forum 2017: evento

di riferimento in Spagna

Produttori, distributori, integratori, associazioni e forze pubbliche e private del comparto sicurezza si incontreranno a primavera per la nuova edizione di *Security Forum*, di scena a Barcellona il 17 e 18 maggio 2017.

L'organizzatore EDICIONES PELDAÑO, S. A., che è anche editore dell'importante rivista specializzata *Cuadernos de Seguridad*, partner di *a&s Italy* si prefigge di superare i già ottimi numeri dell'edizione 2016: quasi 6.000 visitatori, 59 aziende espositrici e 452 partecipanti alle molteplici conferenze proposte.

"Vedere per creare" sarà ancora una volta il motto di un evento caratterizzato quest'anno da una superficie espositiva con specifiche aree dedicate alle telecamere a circuito chiuso, integrazione dei sistemi, sicurezza fisica, sicurezza logica, il controllo accessi, l'IP.

Gruppi di esperti avranno occasione di riunirsi in tavole rotonde aperte per parlare di tecnologie dal punto di vista delle aziende e dei professionisti della gestione, consulenza e installazione di soluzioni. *Security Forum* avrà anche una parte congressuale dove gli esperti potranno scambiare idee su temi di attualità e rilevanza per l'intero settore.

www.securityforum.es

secutech

12 – 14 APRIL
TAIPEI, TAIWAN

20

YEARS OF CONNECTING SECURITY+IOT INDUSTRY

5

VERTICAL FEATURES

SAFE CITY
•
TRANSPORTATION
•
RETAIL
•
FACTORY
•
BUILDING

450

PREMIUM SUPPLIERS

FROM CHINA, KOREA, JAPAN, TAIWAN, MALAYSIA & U.S.

26K

INDUSTRY PROFESSIONALS WORLDWIDE

4

KEY TECH TRENDS IN 2017

SMART COMPONENTS
•
SOFTWARE
•
SMART SENSING
•
UHD

3

LIVE DEMO

INTELLIGENT VIDEO ANALYTICS
•
SECUTECH UHD SURVEILLANCE PERFORMANCE AWARD
•
DRONE & ROBOT APPLICATION PAVILION

REGISTER NOW

WWW.SECUTECH.COM

CONCURRENT SHOWS

SMhome

info security

fire & safety

RIVELATORI PER VIDEOVERIFICA

I rivelatori a raggi infrarossi passivi di Came (modelli 001SIRWLFC e 001SIRWLWFC) sono apparecchi provvisti di fotocamera incorporata per la videoverifica, dotata di illuminatore IR per riprese ottimali anche in condizioni di oscurità.
Utilizzando la trasmissione radio Dual band 868,65 Mhz e 433,92 Mhz bidirezionale o la connessione WIFI, a seguito di una rivelazione d'intrusione i rivelatori permettono di generare e trasmettere alla centrale fino a 20 immagini in QVGA o 10 immagini in VGA o, in alternativa, un video da 2 fps della durata di 10 secondi.
Se il collegamento al Cloud non è previsto, è possibile inviare un MMS o un e-mail contenente le immagini dell'evento. Inoltre, da remoto in qualunque momento l'utente può inviare un SMS per generare e ricevere immagini o filmati.

CAME
www.came.com/it/

TERMOSTATO PER INTERNO

Progettato per misurare e controllare la temperatura interna, il termostato JA-110TP / JA-150TP amplia la gamma di applicazioni di JABLOTRON 100 nella domotica con un semplice controllo di zona. Per commutare il riscaldamento vengono utilizzate le uscite programmabili della centrale. Possono essere installati fino a 4 termostati per 4 differenti impianti di climatizzazione tra loro indipendenti, integrabili nella APP MyJABLOTRON e nell'applicazione web per il controllo da remoto.
Si può impostare automaticamente la commutazione tra modalità economy, modalità di programmazione settimanale, modalità di impostazione manuale della temperatura o spegnimento, disattivare il riscaldamento se una finestra è aperta e inviare una segnalazione per surriscaldamento o congelamento.
Il termostato è prodotto sia in versione bus che in versione wireless e può essere controllato da un cursore.

JABLOTRON ALARMS
www.jablotron.it

TELECAMERE IP E SERVER VCN

Huawei mette a disposizione dei professionisti del settore prodotti per realizzare sistemi innovativi di videosorveglianza adatti sia al retail fino ad arrivare alle smart city. Fra questi, telecamere IP frutto delle più innovative tecnologie video fino a 4K, quali compressione video H.265 HEVC, funzioni intelligenti integrate sviluppate per la configurazione flessibile del sistema e l'implementazione rapida, Led IR invisibili, sensore Cmos Sony EXMOR R con BSI per un illuminazione perfetta anche in condizione estreme.
Fra le altre proposte: server NVR VCN fino a 512ch con funzioni RAID1 e RAID5, sistemi di elaborazione, codifica e archiviazione delle immagini scalabili e con ampia capacità fino a 248TB; sistemi modulari a energia solare con accumulatore e batteria di riserva per un'alimentazione affidabile e conveniente.
Tutto questo e molto alto ancora in collaborazione con Deatronic.

DEATRONIC
www.deatronic.com

RILEVATORE DOPPIA TECNOLOGIA VOLUMETRICO A TENDA

VELVET DT FACTORY EVOLUTION è il rilevatore doppia tecnologia volumetrico a tenda adatto a installazioni per esterno. Il rilevatore è composto da un sistema con doppio antimascheramento; antimascheramento infrarosso e antimascheramento della microonda.
Il rilevatore può essere regolato per funzionamento in attraversamento "a tenda" ed in avvicinamento "a corridoio". Inoltre, grazie alla funzione antimascheramento bedbug, con filtro per piccoli insetti (cimici), è ideale per le istallazioni da esterno dove è possibile che dei piccoli insetti si posino sulla zona sensibile della tecnologia "Infrarosso" e possano provocare danni. Il rilevatore ha una portata operativa di 12 metri (come da prove secondo EN 50131-2-4 Grado 2 CLASSE IV). Gli algoritmi di elaborazione ottimizzano automaticamente la rilevazione in funzione della temperatura.

EEA
www.eea-security.com

TERMINALI SOS PER SPAZI CALMI

In caso di incendio, la normativa prevede la realizzazione di cosiddetti "spazi calmi", definiti dal D.M. 09/04/1994 come un luogo sicuro statico, contiguo e comunicante con una via di fuga dotato di adeguate protezioni dal fuoco e dal fumo e dove le persone disabili si possano rifugiare in attesa di soccorso.
In questi locali è prescritta l'installazione di un sistema per chiamate di emergenza sia per allertare i soccorritori sia per consentire di comunicare con la persona ivi rifugiata per evitare situazioni di panico durante l'attesa.
HelpLAN è una famiglia di apparati per chiamate di emergenza Over IP (SOS) particolarmente adatti a tale scopo che sono dotati di un pulsante di chiamata a fungo e consentono di effettuare conversazioni in viva voce affidabili e di elevata qualità.

ERMES ELETTRONICA
www.ermes-cctv.com

NVR 4 CANALI PER TELECAMERE IP

UNVR4HP di EUROTEK è la soluzione semplice, sicura, pratica ed evoluta per la videoregistrazione della telecamere IP. Si tratta di un NVR 4 canali, con compressione immagini con protocollo h265 U. Code, registrazione ultra HD fino a 4k, gestione di manda 40 massima Mb, autoconfigurazione dei flussi video per la registrazione (massima risoluzione) il live (adattato alle uscite HDMI o 4K) e la visione da remoto, snella e veloce.
Presenta ingressi POE su tutti i 4 ch; uscite monitor in RS232, HDMI e 4K, funzioni smart. Possibile la gestione con cloud P2P, per il collegamento con la APP EZView App di UNV, veloce, intuitiva e abilitata alla gestione completa dell'NVR, oltre che la ricezione delle notifiche push per gli allarmi.
La centralizzazione è affidata al software EZStation, piattaforma unica per IP ed HD analogico.

EUROTEK
www.eurotek-srl.it

SISTEMA DI ALLARME CON CENTRALE BIDIREZIONALE

ONE è un innovativo sistema di allarme composto da una centrale antifurto wireless completamente bidirezionale BiTech, a batteria (pile torcia) e/o rete elettrica, con possibilità di video-verifica (fotogrammi) su richiesta o allarme.
La centrale ha 14 zone, 12 telecomandi, 1 Area; alimentazione con 6 pile torcia alcaline e/o rete elettrica (anche modello con alimentatore carica batteria); tastiera capacitiva retroilluminata e display Lcd; lettore di prossimità RFid integrato; video-verifica (fotogrammi) con tecnologia VTech; comunicazione in Gsm/Gprs (dati, messaggi vocali, Sms testo, e-mail); sirena piezoelettrica; storico eventi (256); programmazione da software (locale/remoto) o tastiera (Plug&Play). Possibile la gestione tramite APP MY-SICEP (iOS, Android) e Centrale Operativa MvsNET. Disponibile ampia gamma di accessori utilizzabili.

SICEP
www.sicep.it

CILINDRO MECCATRONICO

I nuovi cilindri meccatronici dormakaba, disponibili anche con funzione wireless, uniscono l'elettronica intelligente ad una meccanica affidabile e si integrano perfettamente e con facilità negli impianti di chiusura esistenti.
Le autorizzazioni all'accesso si basano sulla corrispondenza della fresatura meccanica con la validazione elettronica dei dati, contenuti nella dormakaba smart key.
L'elettronica integrata apre nuove possibilità agli utenti: le autorizzazioni di accesso possono essere regolate in base a profili spazio-temporali e le chiavi possono essere programmate o bloccate in modo rapido e semplice. Il cilindro meccatronico è disponibile in 3 versioni: compatto, con elettronica separata o integrata.

DORMAKABA ITALIA
www.dormakaba.it

RIVELATORE RADIO UNIVERSALE TENDA TRIPLA TECNOLOGIA

Il rivelatore TENDA 8032-ISR023 è stato progettato per essere utilizzato con qualsiasi sistema via radio e qualsiasi protocollo di trasmissione. E' installabile tra finestra e persiana/tapparella, o in esterno con l'ausilio del supporto 1894SBP. La rilevazione avviene mediante 2 PIR e 1 MW a 24 GHz; doppia funzione antimascheramento ad IR attivi, una per PIR. I 3 sensori possono essere gestiti in: triplo AND, MW in AND con ognuno dei 2 PIR, AND dei PIR con MW esclusa, triplo OR se implementata la modalità WIN. La funzione WIN permette di alimentare il dispositivo tramite fonte esterna, garantendo le prestazioni di un rivelatore filare senza alcuna inibizione. Una guarnizione di tenuta rende impermeabile il vano in cui è alloggiata la scheda elettronica, la scheda trasmittente e relativa batteria di alimentazione. Disponibile anche in versione marrone (8033-ISR024).

ITALIANA SENSORI
www.italianasensori.it

SENSORE INTELLIGENTE DA ESTERNO

Beyond è il nuovo sensore intelligente da esterno di RISCO Group - già disponibile in versione cablata e a breve anche radio – per soddisfare i requisiti di case private, siti industriali e remoti.
Grazie alla doppia tecnologia (DT) e combinando due canali a microonda in banda K e due canali PIR, offre prestazioni superiori, oltre a ridurre i falsi allarmi sfruttando le tecnologie di rivelazione progettate per l'ambiente esterno. Sway Recognition Technology (SRT) permette di riconoscere e ignorare gli oggetti che oscillano senza spostarsi come rami e arbusti; Digital Correlation Technology (DCT) assicura che siano considerate minacce solo quei soggetti che causano segnali simili e correlati in entrambi i canali PIR, mentre Direct Sunlight Immunity garantisce immunità alla luce solare, ignorando gli sbalzi di intensità luminosa sulla base di un esclusivo algoritmo.

RISCO GROUP
www.riscogroup.it

VIDEO MANAGEMENT SOFTWARE

Valerus è un nuovo VMS potente e intuitivo che è stato progettato per gli utenti di tutti i livelli. La progettazione e la realizzazione di Valerus è basata sulla facilità di installazione, l'interfaccia basata su web semplice da usare e uno standard di piattaforma aperta.
Valerus ha le caratteristiche per il monitoraggio della sorveglianza in tempo reale, la gestione centralizzata e la registrazione video ad alte prestazioni. Basato su veri e propri standard aperti per l'interoperabilità ottimizzata, vanta un'architettura thin client e le licenze centralizzate per la distribuzione e la gestione di una potente soluzione VMS. Sulla base di anni di esperienza nel mercato della sicurezza e con uno sguardo verso il futuro, questa nuova piattaforma supporta i sistemi di rete tradizionali ma è anche pronta per l'espansione nel mondo del cloud computing.

VICON INDUSTRIES
www.vicon-security.com

NVR FLESSIBILE E SCALABILE

Arteco 3000 è un NVR progettato per offrire semplicità d'utilizzo ed elevate prestazioni, in grado di soddisfare i più alti requisiti in materia di sicurezza.
Grazie alla possibilità di supportare fino a 12 telecamere IP con risoluzione Full HD ed all'architettura a 64 bit, Arteco 3000 è una soluzione flessibile e completamente scalabile, adatta per le piccole imprese, uffici, negozi e punti vendita distribuiti, così come per installazioni multi-sito di qualsiasi dimensione.
Bastano pochi minuti per installarlo e configurarlo grazie ad un'esperienza utente semplificata, supportata dalle innumerevoli soluzioni integrate e dalla compatibilità con i più recenti dispositivi di terze parti.

ARTECO
www.arteco-global.com/it/

CENTRALE D'ALLARME ANTINTRUSIONE E TVCC

La centrale d'allarme 8-20 zone di Venitem rappresenta una punta innovativa per il settore della sicurezza. Disponibile nella nuova versione XL, dimensionata per contenere al suo interno un alimentatore per telecamere (TSW 155 di Venitem – 13,8 Vdc 5A regolabili con caricabatteria integrato), oltre ad una batteria da 17 Ah, permette di integrare la gestione dell'impianto antifurto alla videosorveglianza. L'alimentatore è in grado di gestire fino a 8 telecamere e impostare la tensione di uscita per compensare la caduta di tensione dei cavi in impianti TVCC medio-grandi.
Una soluzione completa e performante, accompagnata da accorgimenti tecnici e pratici che ne rendono la gestione semplice e intuitiva, oggi ancor di più grazie alla nuova APP che permette un controllo completo della propria sicurezza ovunque ci si trovi.

VENITEM
www.venitem.com

TELECAMERA SPEED DOME H.265

SD9364-EH è l'ultima telecamera speed dome professionale di VIVOTEK, specificamente progettata per migliorare la sorveglianza nelle zone con ampia copertura e scarsa illuminazione. Dotata di illuminatori IR 250M e di uno zoom ottico 30x, SD9364-EH offre eccellenti immagini anche nelle situazioni più impegnative e con scarsa illuminazione. Il modello SD9364-EH adotta anche la più recente tecnologia a infrarossi di VIVOTEK, VAIR (Vari-Angle IR), che consente la regolazione ad angolazione variabile degli illuminatori IR, permettendo un'ampia copertura FOV e un'intensità IR altamente uniforme ed evitando gli hot-spot tradizionalmente associati all'illuminazione IR. Questa telecamera ha vinto il Taiwan Excellence Silver Award 2017.

VIVOTEK
www.vivotek.com

SISTEMA DI CONTROLLO DI SICUREZZA LOGICA E DEI GAS

Touchpoint Pro è un sistema di controllo di sicurezza logica e dei gas in grado di offrire flessibilità e connettività impareggiabili per il settore petrolifero e del gas. La piattaforma si adatta alle esigenze di tutti i siti, offrendo flessibilità totale, utilizzo intuitivo e possibilità di ridurre i costi.
E' la soluzione ideale per piccole e medie imprese. L'architettura flessibile permette di costruire l'intero sistema in base alle esigenze del cliente, ottimizzando le attività e i costi. Grazie a un esclusivo approccio modulare consente al cliente di costruire un sistema centralizzato, un sistema distribuito o una combinazione dei due, usando gli stessi componenti. L'architettura esclusiva può ridurre in maniera significativa i costi di cablaggio e i tempi di installazione e può essere facilmente ampliata o integrata in un sistema di arresto di emergenza dei gas.

HONEYWELL
www.honeywellanalytics.com/it-it

SENSORE VOLUMETRICO DA INTERNO UNIVERSALE

JET DT AM è il sensore volumetrico da interno universale ad infrarosso passivo e microonda a basso consumo completo di anti-mascheramento top della gamma JET di AVS Electronics.
Ha una portata di 15 metri e apertura a 90°, disponibile anche con la soluzione ad effetto tenda con lente opzionale dedicata e apertura 5° (mod. CLI).
Tra le sue caratteristiche, propone la rilevazione ad infrarosso basata su PIR con Tecnologia Quad che permette di migliorare la qualità della rilevazione e di effettuare efficaci analisi dei segnali prima di generare un allarme. Un soluzione che, abbinando PIR e lente di qualità permette, con gli opportuni settaggi, di discriminare animali di piccola taglia, dai 12 a 25 kg. È facile da installare a parete o a soffitto con una staffa dedicata, senza compromettere la rilevazione.

AVS ELECTRONICS
www.avselectronics.com

TELECAMERE CONVENIENTI CON ALTA QUALITÀ DI IMMAGINE

La serie AXIS P32 è una linea di telecamere convenienti che offrono una qualità d'immagine straordinaria in qualsiasi condizione di illuminazione.
Combinano la tecnologia Axis Lightfinder, che garantisce una sensibilità alla luce ottimale e un video a colori anche con una scarsa illuminazione, e la tecnologia Axis WDR Forensic Capture, per le attività forensi e in grado di offrire un livello straordinario di dettagli sia nelle aree chiare che in quelle scure.
Molti modelli sono dotati di illuminatori a infrarossi (IR) integrati che consentono di riprendere video di alta qualità nell'oscurità totale. Grazie a una configurazione e una manutenzione estremamente semplici, sono ideali per banche, punti vendita, strutture ricettive e istituti educativi e per i sistemi di medie dimensioni in settori come trasporti, sorveglianza cittadina, strutture sanitarie e industria.

AXIS COMMUNICATIONS
www.axis.com/it/

SISTEMA PER GESTIONE ACCESSI

Axxedo, il sistema creato da Bft per la gestione degli accessi, permette di creare tipologie di impianti distribuiti o centralizzati, con il completo e totale controllo delle funzioni anche in modalità offline. Inoltre, consente di gestire fino a 32 varchi dalla stessa centrale, con la possibilità di modificare in qualsiasi momento il numero e la tipologia dei varchi controllati, lasciando inalterata la configurazione di base. Axxedo è composto da tre centrali che si distinguono per tipologia di funzionamento: Q.bo SA, il sistema stand alone all in one con sensore crepuscolare integrato, Axxedo Stand Alone, la centrale con funzionamento master/slave che funge anche da modulo di espansione con un ingresso e un'uscita, e Cerebro, il "cervello" di Axxedo che permette una gestione totale e completa dell'impianto anche in modalità offline.

BFT
www.bft-automation.com

BARRIERE A INFRAROSSI ATTIVI PER ESTERNO

NEWTON LIGHT è la nuova gamma di barriere attive ad infrarossi con tripla ottica e portata fino a 200m. La gamma si caratterizza per un prezzo estremamente competitivo e un'affidabilità comprovata sul campo anche in condizioni atmosferiche avverse.
Uno speciale filtro per la luce solare permette di funzionare anche con illuminazione diretta fino a 50.000 lux; una serie di viti micrometriche, display e buzzer a bordo permettono di regolare con precisione e facilità la barriera. E' possibile selezionare fino a 8 frequenze differenti per il montaggio in modalità sovrapposta e di regolare tempo di interruzione del fascio tra 50 e 250ms. Completano le caratteristiche l'uscita allarme, tamper e disqualifica. Alimentazione: 12Vcc 100mA. Grado di protezione IP65.Temperatura di funzionamento: da -25° a +55°C. Regolazione ottiche: 180° orizzontale - 20° verticale.

CIAS
www.cias.it

RIVELATORE WIRELESS 868 MHZ BIDIREZIONALE

Timoteo Wind XT-W è il nuovo rivelatore wireless 868 MHz bidirezionale ad effetto tenda prodotto da Combivox. Ideale per la protezione perimetrale esterna di finestre, lucernai e facciate murarie con più aperture, garantisce una copertura fino a 12 metri. La Tripla Tecnologia di rilevamento (2IR+MW), con un'elaborazione continua e incrociata dei segnali ricevuti dai due canali ad infrarossi passivi e dalla microonda, garantisce immunità ai falsi allarmi. Il circuito di anti mascheramento della MW, che rileva l'avvicinamento di un ostacolo inviando segnalazione in centrale, lo rende sicuro contro i sabotaggi. Dotato di accelerometro MEMS contro l'effrazione, assicura affidabilità e semplicità d'installazione, eliminando i problemi delle imperfezioni delle superfici e agenti atmosferici. Il rivelatore è in grado di funzionare anche in presenza di piccoli animali (pet immune).

COMBIVOX
www.combivox.it

DEVELOPMENT KIT PER APPLICAZIONI IOT

EDCK 4001 è un nuovo kit di sviluppo Everyware Device Cloud che mette a disposizione l'hardware e il software necessari per prototipare, sviluppare, testare e integrare soluzioni IoT complete in grado di collegare sensori, dispositivi e cloud.
Il Development Kit ECDK 4001 offre un ambiente completo a sviluppatori software e ingegneri operativi che possono sviluppare i loro casi applicativi partendo da un kit realistico che integra tutti i componenti chiave tipici di un'applicazione IoT industriale (gateway, PLC, dispositivi in campo, protocolli di campo, servizi in cloud).
Il Development Kit EDCK 4001 comprende un ReliaGATE 10-11, il gateway IoT di Eurotech per applicazioni industriali basato sulla famiglia di processori Cortex-A8, e un PLC collegato a una scheda demo dotata di controlli digitali e analogici.

EUROTECH
www.eurotech.com/it/

RILEVATORE DI RADIAZIONI TECNOLOGIA BLUETOOTH SMART

identiFINDER R100 è il primo rilevatore di radiazioni personale del settore certificato IP67 e conforme al test di caduta ANSI (American National Standards). La classe di protezione IP67 dell'R100 ne attesta la protezione contro la polvere e l'immersione in acqua fino a 1 metro di profondità.
L'unità integra la tecnologia wireless Bluetooth® Smart, che facilita la registrazione e l'invio di informazioni sulle dosi di radiazione in tempo reale e di geotag tramite una APP mobile.
Tutti i modelli identiFINDER, compreso l'R100, condividono la stessa interfaccia utente intuitiva e ben collaudata, che attiva una risposta sinergica e coordinata alle emergenze, tra forze dell'ordine, Vigili del Fuoco e squadre specializzate in materiali pericolosi, dotati di un prodotto identiFINDER.

FLIR SYSTEMS
www.flir.it

APP PER SEGNALARE PERICOLI IN LUOGHI D'INTERESSE

Ricevere notifiche via smartphone su cosa sta succedendo vicino alla propria abitazione, alla scuola dei propri figli o all'ufficio è oggi possibile grazie all'App Shelly, gratuita e disponibile per i sistemi operativi IOS e Android.
Ogni volta che si entra nell'App Shelly la mappa della zona in cui ci si trova fornisce la situazione aggiornata di ciò che sta accadendo grazie alle segnalazioni della community Shelly che, attraverso un menù segnalazioni, può decidere se inviare un warning che può essere solo anonimo alla Community. È possibile segnalare 12 tipologie di potenziale pericolo o di disagio che si stanno verificando. Attivando la funzione "Sentinella", Shelly invia notifiche di eventi anomali come avvistamenti di persone sospette o moleste, incendio, furto e aggressioni intorno alla posizione predefinita, in genere l'abitazione.

DAITEM
www.daitem.it

MODULO DI RICONOSCIMENTO FACCIALE

Il modulo Omron HVC-P2 B5T prevede dieci principali funzioni: rilevamento di un viso, di una mano o di un intero corpo umano; riconoscimento facciale e di genere; stime relative a età, umore, mimica facciale, direzione dello sguardo e movimento delle palpebre. Per tutti questi parametri il modulo fornisce un valore corredato da una valutazione di attendibilità, permettendo così al programmatore di configurare la reazione appropriata per ogni singola applicazione.
Il modulo HVC ha un'architettura molto compatta e può essere integrato facilmente nei sistemi esistenti così come nei nuovi progetti.
Utilizzando la soluzione HVC di Omron, tutti gli sviluppatori embedded possono aggiungere ai loro sistemi delle funzioni di riconoscimento facciale senza bisogno di confrontarsi con gli algoritmi sottostanti né con il progetto della parte ottica.

OMRON ELECTRONIC COMPONENTS EUROPE
http://components.omron.eu

Elettromondo

L'EVENTO FIERISTICO CHE APRE NUOVI SPAZI AL MONDO ELETTRICO.

Un appuntamento imperdibile per i professionisti dell'elettricità con le novità, le idee e le soluzioni più innovative proposte dai produttori più qualificati del settore.

17-18 marzo 2017
RIMINI FIERA - Ingresso est

PARTECIPAZIONE:
Venerdì 17 marzo: 9.00 - 18.30
Sabato 18 marzo: 9.00 - 17.30
Ingresso gratuito con registrazione obbligatoria.

CONVEGNI CON CREDITI FORMATIVI E WORKSHOP

PRE-REGISTRATI E SALTA LA CODA
www.eventoelettromondo.it

Rimani sempre aggiornato sull'evento.
Metti mi piace!

EVENTO RISERVATO
AGLI OPERATORI DEL SETTORE

Elettromondo
SOLUZIONI PER L'ELETTRICITÀ

Un'iniziativa di

ELETTROVENETA

ELETTROFORNITURE FERRI

www.eventoelettromondo.it

a&s ITALY

ISSN 2037-562X a&s Italy

ANNO 8 – Numero 43 – febbraio 2017

Direttore responsabile
Andrea Sandrolini

Coordinamento editoriale
Ilaria Garaffoni
redazione@ethosmedia.it

Direzione Commerciale
Roberto Motta
motta@ethosmedia.it

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

Ufficio estero
international@ethosmedia.it

Pubblicità
Ethos Media Group srl
pubblicita@ethosmedia.it

Sede Legale
Via Venini, 37
20127 Milano

Direzione, redazione, amministrazione
Ethos Media Group srl
Via Caduti di Amola, 31
40132 Bologna (IT)
tel. +39 051 0475136
Fax +39 039 3305841
www.ethosmedia.it

Registrazione
Tribunale di Bologna al n° 8027 Dicembre 2009

Iscrizione al Roc
Ethos Media Group s.r.l.
è iscritta al ROC
(Registro Operatori
di Comunicazione)
al n. 19315 del 2 marzo 2010

Periodicità
Bimestrale

Grafica / impaginazione
www.zeronovecomunicazione.it

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

Rivista certificata secondo il Regolamento CSST

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

A.N.E.S. ASSOCIAZIONE NAZIONALE EDITORIA PERIODICA SPECIALIZZATA

CONFINDUSTRIA

CSST CERTIFICAZIONE EDITORIA SPECIALIZZATA E TECNICA

ADS A member of IFABC International Federation of Audit Bureaux of Circulations

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

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

INSERZIONISTI

vai su Secsolution | vai su a&s Italy | vai su Ethos Media Group

a&S ITALY

LO PUOI TROVARE ANCHE PRESSO QUESTE AZIENDE

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

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

CAMPANIA - **CIBF** - Via Galileo Ferraris, 185 - 80142 Napoli - Tel. +30 081 7349175 ● **DHS Benevento** - Piazza San Lorenzo, 2 - 82100 Benevento - Tel. +39 0824 25350 ● **DODIC ELETTRONICA** – Via Ferrante Imparato, 198 (CM2 lotto A5) – 80146 Napoli - Tel. + 39 081 5591787 ● **DSPRO Sicurezza ed Automazione -** Via Lima, 2/A2 - 81024 Maddaloni (CE) - Tel. +39 0823 405405 ● **GAM Service -** Via Nazionale delle Puglie, 178 - 80026 Casoria (NA) - Tel. +39 081 7591915 ● **PROFESSIONE SICUREZZA** – Via Romaniello, 87 - 81038 Trentola Ducenta (CE) - Tel. +39 081 18740456 ● **VITEKNA Distribuzione -** Via delle industrie, 33 - 80147 Napoli - Tel. +39 081 7524512

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

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

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

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

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

MARCHE - **ASCANI Elettrocomm** - Via Lame 113 - 63066 Grottammare (AP) - Tel. +39 0735 73731 ● **GIUDICI & POLIDORI** - Strada Provinciale - Valtesino, 299/16 - 63066 Grottammare (AP) - Tel. +39 0735 777446 ● **SICURIT - Marche – Abruzzo - Molise** - Via Guido Rossa, 12 - 60020 Ancona - Tel. +39 071 804514

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

PIEMONTE - **ABES** - Via Traversella, 13/A - 10148 Torino - Tel. +39 011 2290703 ● **DOPPLER** - Via Curiel, 14 - 10024 Moncalieri (TO) - Tel. +39 011 644451 ● **ELCA** - Viale Indipendenza, 90 - 14053 Canelli (AT) - Tel. +39 0141 834834 ● **GEDICOM** - SS 231 B.go San Martino, 32 - 12042 BRA (CN) - Tel. +39 0172 413649 ● **GEDICOM** - Via Bisalta, 3 - 12100 CUNEO – Tel. +39 0171 346672 ● **GEDICOM** - Via Druento, 150 – 10078 Venaria Reale (TO) – Tel. +39 011 436827 ● **GOBBO** - Strada Bertolla, 162 - 10156 Torino - Tel. +39 011 2735720 ● **ITALTECH** - Via S.Antonio Da Padova, 8 - 28068 Romentino (NO) - Tel. +39 0321 868537 ● **SICURIT Piemonte** - Via Lesna, 22 - 10095 Grugliasco (TO) - Tel. +39 011 7701668 ● **SMART** - Via Amendola 197 - 13836 Cossato (BI) - Tel. +39 015 980079

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

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

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

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

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

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

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

Satel®
ITALIA

VERSA CONTROL

NOVITÀ: APP VERSA CONTROL permette la **VIDEO VERIFICA** in tempo reale. Gli utenti possono monitorare il proprio sistema visualizzando il filmato live.

L'App consente anche di inserire, disinserire e visualizzare lo stato dell'impianto a distanza, consultare la memoria eventi, escludere i rivelatori e attivare dispositivi domotici.

E' disponibile per iOS, Android e Windows Phone.

SATEL Italia srl
Via Ischia Prima, 280 - 63066 Grottammare (AP)
www.satel-italia.it - info@satel-italia.it

HIKVISION

TOTAL SOLUTION PROVIDER

CCTV | Intrusion | Intercom | Access Control

www.hikvision.com

LA CONVERGENZA SECONDO HIKVISION

Dopo aver conquistato in soli 15 anni la leadership mondiale nella videosorveglianza con la sua gamma di soluzioni end-to-end convergente sul software iVMS, Hikvision allarga oggi i propri orizzonti per abbracciare una nuova identità: quella di **Total Solution Provider** per l'intero mercato della sicurezza.

Il primo passo, nel 2016, è stato l'ingresso nel mercato antintrusione con l'acquisizione di Pyronix, nota realtà britannica produttrice di sistemi d'allarme. Ma Hikvision punta a sviluppare una gamma ben più ampia di soluzioni convergenti su un'unica piattaforma di gestione e programmazione e capace di abbracciare videosorveglianza e intrusione, come pure intercom, controllo accessi e in futuro probabilmente safety.

Hikvision dispone infatti di uomini, knowhow e risorse per raggiungere a breve termine una convergenza tecnologica completa. Sono i suoi numeri a parlare: oltre 18.500 dipendenti in tutto il mondo, dei quali 7.000 ingegneri dedicati a ricerca e sviluppo; un investimento annuo in R&D che va dal 7 all'8% del fatturato; estrema attenzione alla qualità dei prodotti - controllata, testata e assoggettata a severi processi certificativi nei suoi due moderni siti produttivi in Cina. Con 21 filiali disseminate nel mondo, +33% di fatturato nel 2016 nella sola Italia e una previsione di circa 5 miliardi di dollari per il fatturato globale 2016, Hikvision si conferma una realtà focalizzata e dedita al risultato, con estrema capacità di innovazione, solidità finanziaria e soluzioni verticali per rispondere a qualunque esigenza.

CCTV

Gamma completa di soluzioni end to end convergenti sul software iVMS per coprire qualunque esigenza e servire ogni tipologia di mercato: entry level, professional, mercati verticali.

Intrusion

Rivelatori per interno ed esterno, una centrale wireless ibrida che presenta innumerevoli vantaggi e il Pyronix Cloud Home Control+ che trasforma lo smartphone in una tastiera portatile touch.

Intercom

Sistemi video Intercom IP per residenziale che comunicano video/audio, archiviano immagini e messaggi vocali e diventano una soluzione completa integrando il video nei sistemi di registrazione.

Access Control

Due linee: la gamma Solution (controllori e lettori di card) e la gamma Professional (terminali), il tutto comprensivo di relativi accessori. Nuovo valore aggiunto per i clienti hi-end.

HIKVISION

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

Filiale Milano
Viale Fulvio Testi 113
20092 Cinisello Balsamo, MI
T +39 02 92886311
F +39 02 92886399

Filiale Roma
Via Pontina 573
00128 Roma
T +39 06 94538790
F +39 06 94538791

Filiale Bologna
Via G. Fattori 4
40033 Casalecchio di Reno, BO
T +39 051 0393670
F +39 051 0393671

www.hikvision.com
info.it@hikvision.com