La gestione da remoto dei sistemi di sicurezza anticrimine

di Emanuele Azzola

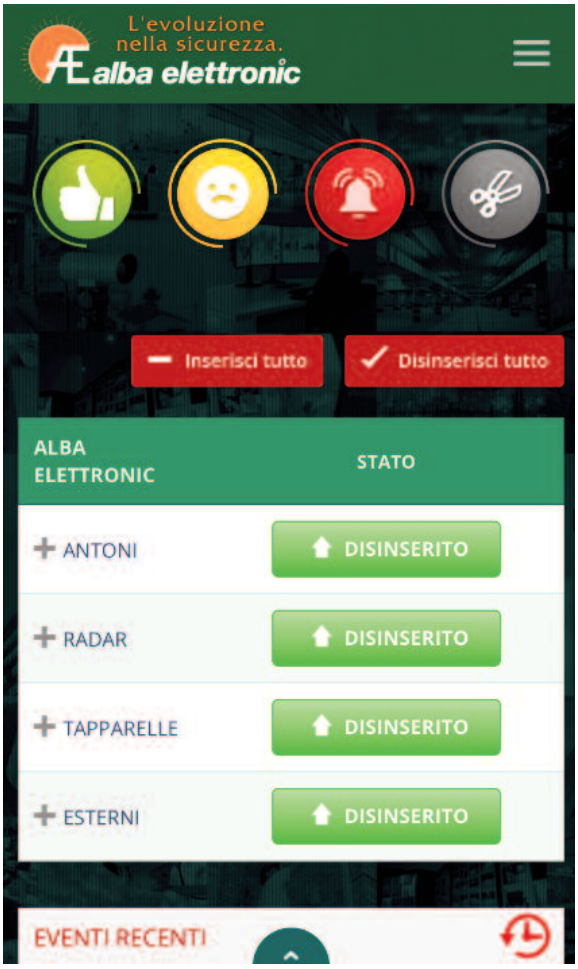

Fig. 1 - *Interfaccia utente comando impianto allarme per i-Phone.*

Possibilità di gestire gli impianti da smartphone: opportunità o minaccia?

L'evoluzione tecnologica e quella socioeconomica, che ne è al contempo causa e conseguenza, hanno imposto anche nel settore della sicurezza l'introduzione di importanti cambiamenti, che riguardano soprattutto le modalità di funzionamento degli impianti e di impiego degli stessi da parte degli utenti.

Ecco dunque che la possibilità di visualizzare le immagini della propria abitazione o azienda quando ci si trova all'estero o la necessità di abilitare e disabilitare "l'antifurto" senza bisogno di avere con sè chiavi o doversi ricordare complessi codici, diventano richieste all'ordine del giorno per gli installatori di sistemi di sicurezza di oggi. Il bisogno di soluzioni immediate per l'utente si traduce quindi in applicazioni che permettono ad esempio di visualizzare le registrazioni di un sistema di videosorveglianza o ancora di gestire il proprio impianto d'allarme utilizzando *PC, Smartphone e Tablet;* tutto questo grazie a interfacce e icone intuitive, tasti di comando, mappe grafiche, notifiche push in *real time*, ecc.

La parola d'ordine è più che mai integrazione: avere un APP che permette di gestire il proprio sistema di sicurezza vuol dire integrare su un unico dispositivo *mobile* la *security* con l'automazione, la climatizzazione, l'illuminazione, ecc.

Fig. 2 - *Visualizzazione mappa grafica impianto allarme su i-Phone.*

La gestione da remoto dei sistemi di sicurezza anticrimine

Fig. 3 - *Visualizzatore immagini live e registrate da impianto Tvcc su i-Pad.*

È così che l'utente può, ad esempio, attivare l'apertura del cancello pedonale di casa, escludere il sensore esterno alla porta d'ingresso, controllare in diretta che il corriere di Amazon lasci il proprio pacco fuori dalla porta e se ne vada, prima di riattivare il sensore e richiudere il cancello; tutto questo senza nemmeno doversi alzare dalla propria scrivania o mentre si trova in vacanza all'altro capo del mondo.

La sicurezza derivante dall'integrazione di impianti di rivelazione incendio, sistemi di controllo, accessi che dialogano con impianti di allarme antintrusione e di videosorveglianza, con funzioni avanzate quali video analisi e video verifica, nell'era del cosiddetto *"Internet Of Things"*, da un lato permette una gestione veloce ed intuitiva mentre dall'altro consente di estrarre e di disporre di una serie di informazioni e dati utili.

La messa in rete di prodotti quali centrali d'allarme antintrusione o antincendio, di sistemi di controllo dei varchi, di videoregistratori digitali, ecc., facilita il compito di installatori e impiantisti che possono eseguire sempre più operazioni come verifiche, diagnosi, configurazioni e tarature senza dover fisicamente intervenire in campo. La connessione *on-line* dei dispositivi permette infatti una più facile personalizzazione degli impianti, una migliore supervisione degli stessi e una manutenzione più efficiente. Nello specifico le connessioni internet e *LAN*, abbinate a un elevato contenuto tecnologico proprio dei migliori prodotti, permettono una moltitudine di funzionalità tra cui la modifica di programmazioni delle centrali d'allarme, la taratura di soglie dei "rilevatori di movimento" o, ancora, l'inquadratura e la messa a fuoco delle telecamere, comodamente dall'ufficio, da casa propria o da qualsiasi luogo dove vi siano un accesso a internet e un PC.

Queste innovazioni hanno come naturale conseguenza una riduzione e ottimizzazione delle tempistiche d'intervento con ovvi e considerevoli risparmi di tempo (e denaro) sia per l'installatore che per l'utente.

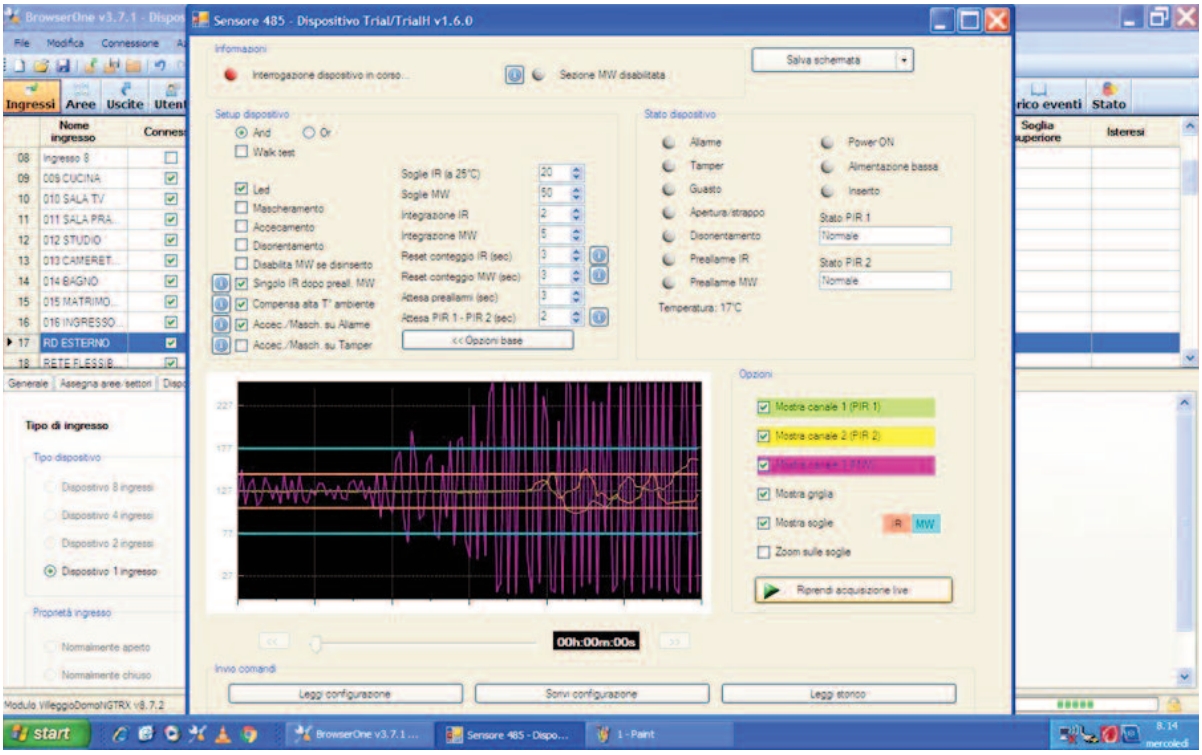

Fig. 4 - *Pagina di configurazione da remoto (tramite PC) di un sensore antintrusione.*

Attenzione però! Tutte queste novità potrebbero minare il livello di sicurezza di un impianto: le richieste del cliente non devono mai indurre a rendere il sistema potenzialmente "cieco" riducendone efficacia ed efficienza, mentre l'installatore deve sempre utilizzare *password* e codici che impediscano la possibilità ad un estraneo di accedere al sistema e manometterlo *(hackeraggio)*; un po' come avviene per il *remote-banking.* La sicurezza informatica è un aspetto essenziale per la protezione di dati sensibili: strumenti quali filtri, *firewall*, protocolli di comunicazione, ecc., rischiano di diventare inutili se non vi sono poi delle personalizzazioni a livello di *username* e di *password* associate: queste devono essere complesse, uniche, protette e se necessario modificate periodicamente. Negligenze in questi aspetti potrebbero in ultima analisi portare al fallimento del sistema di sicurezza nel suo complesso.

La conclusione è pertanto molto semplice ed ovvia: sfruttare appieno le opportunità offerte dall'evoluzione delle *smart-tecnologies* e del mondo connesso, senza dimenticare che il fine ultimo di un sistema di sicurezza rimane pur sempre quello di garantire… sicurezza!

Fig. 5 - *Pagina di gestione degli impianti d'allarme connessi.*