

BREVI CENNI

SUI SISTEMI DI SICUREZZA

Corso per
L'Istituto Superiore Statale
Geymonat di Tradate



I SISTEMI DI SICUREZZA

Generalmente se sentiamo parlare di sistemi di sicurezza pensiamo all'antifurto, tuttavia questo è vero solo in parte.

Infatti, possiamo sicuramente includere in questa categoria gli impianti di videosorveglianza e anche quelli anti-incendio.

In questo breve corso ci dedicheremo a scoprire le potenzialità di un sistemi di sicurezza inteso proprio come antifurto e scopriremo come ciò porti a considerare anche tematiche di videosorveglianza, di anti-incendio e persino di pronto soccorso a persone anziane o disabili.

LE COMPONENTI DI UN SISTEMA DI SICUREZZA

- la centrale di gestione (la scheda elettronica che controlla e comanda le altre unità)
- gli organi di comando (tastiera, lettori di prossimità)
- le periferiche di rilevazione (sensori, contatti di vario genere, barriere)
- le periferiche di comunicazione (dispositivo GSM/GPRS, modulo IP per la connessione alla rete, modulo vocale per collegamento alla rete PSTN)
- dispositivi di segnalazione (sirene esterne ed interne, lampeggianti, leds)
- le interfacce espansione (espansioni di zone, ricevitori radio)
- il gruppo di alimentazione
- i cavi di collegamento
- l'installatore

In ognuna di queste componenti, nel corso degli anni, l'elettronica ha contribuito a migliorarne caratteristiche e prestazioni.

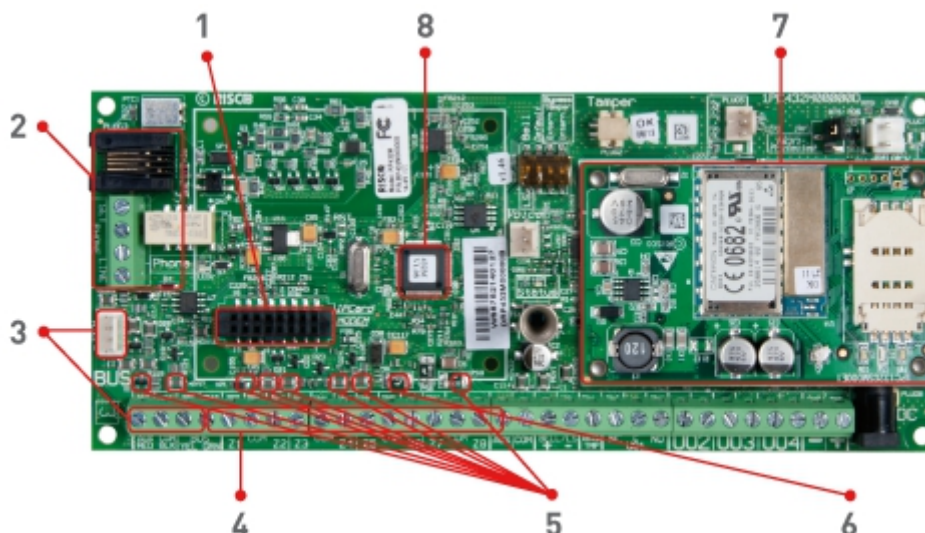
L'apparecchiatura che ha beneficiato in più larga misura di questa evoluzione è senza dubbio la centrale di gestione, mentre la componente che non si può aggiornare in modo semplice è, purtroppo, l'installatore

LA CENTRALE DI CONTROLLO

La centrale di controllo è la componente fondamentale per i sistemi di sicurezza, perchè in essa risiedono gli ingressi di controllo e le uscite di comando, oltre a vari connettori ad innesto per espansioni di vario tipo. Tutte le informazioni in ingresso ed in uscita sono gestite dal **MICROPROCESSORE.**

I microprocessori sono dei componenti elettronici nel quale il progettista scrive il programma che controllerà le varie funzioni e potrà decidere come operare in base ai dati rilevati. E' fondamentale realizzare un programma che non abbia "buchi", ovvero salti di programma e/o combinazioni di eventi non previsti.

Segue l'immagine di una scheda della centrale LightSYS di produzione RISCO



1. Connettore per modulo di rete
2. connettore per la rete telefonica PSTN
3. Connettore per collegare dispositivi su bus (usato da quelli installati nel contenitore)
4. Morsetti
5. Protezioni
6. e filtri sugli ingressi
7. Modulo GSM/GPRS ad innesto
8. **microprocessore**

All'interno del microprocessore il programma appositamente realizzato dai softweristi sarà in grado di determinare i vari stati del sistema (allarme, inserimento, disinserimento, ecc.) e di stabilire l'azione da svolgere (chiamata telefonica, SMS, email, o altro). Oltretutto questi componenti hanno un orologio interno che può attivare funzioni autonomamente.

Questo *algoritmo*, realizzato “ad hoc” per quel micro installato su quella scheda specifica si chiama **FIRMWARE**. Va da sè che firmware diversi non sono intercambiabili.

La centrale RISCO ha un firmware aggiornabile, quindi riscrivibile, per consentire ai progettisti di correggere e migliorare le prestazioni della apparecchiatura con il passare del tempo semplicemente riscrivendone il firmware.

Le comunicazioni tra la scheda centrale e le periferiche possono avvenire tramite un **BUS dati**., oppure tramite opportuni collegamenti di tipo analogico (definibili NC, EOL, DEOL, TEOL).

Quando il collegamento è di tipo BUS, il passaggio dei dati avviene con 2 soli fili, uno di clock ed uno di dati, secondo lo standard **RS485**.

Va sottolineato che per aggiornare il firmware di una centrale si utilizza lo standard **RS232**, passando magari per la porta USB tramite un convertitore.

Il motivo per cui si utilizza lo standard RS485 per collegare tra loro le periferiche della centrale è che consente alle informazioni di percorrere senza problemi distanze superiori ai 300 metri (le distanze sono strettamente legate alle sezioni dei cavi conduttori). Oltretutto esistono delle schede di interfaccia che prolungano ulteriormente la lunghezza del bus.

A questo punto vediamo l'interazione tra sensori e centrale.

La premessa generale è che un sensore può informare la centrale del suo stato o tramite il bus o tramite un collegamento "tradizionale".

Con il bus è sufficiente collegare i sensori tramite quattro conduttori e identificarli per averne il completo controllo. Ben diverso è il collegamento tradizionale.

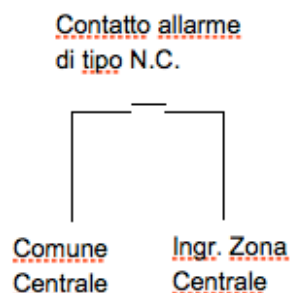
In questo caso lavoriamo solo su **contatti chiusi a riposo ed aperti in stato di allarme**. In realtà ogni sensore ha almeno **due tipi di segnalazione: allarme intrusione e allarme per manomissione** (detto TC=taglio cavi, linea 24H= linea 24 ore oppure linea di guardia). Questa linea di protezione è importantissima perchè impedisce l'apertura del sensore anche ad impianto disinserito.

Se la linea manomissione non fosse attivata sarebbe possibile aprire il sensore ad impianto spento, cortocircuitare il contatto di allarme e richiuderlo, così **si potrebbe violare la zona anche ad impianto inserito**. Questo è contrario ad ogni normativa, che nel caso dei dispositivi di sicurezza richiede la cosiddetta SICUREZZA ATTIVA.

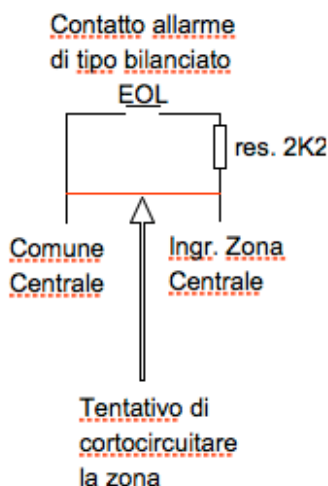
Il principio di sicurezza attiva prevede che i contatti di allarme siano a mancare (proprio per prevenire i tentativi di taglio cavi) mentre i comandi di stop allarme siano a dare.

Per garantire la migliore sicurezza nel collegamento tra sensori e centrale si utilizzano delle resistenze, i cui valori variano da produttore a produttore.

In questo breve corso consideriamo alcuni possibili bilanciamenti previsti da RISCO.



Nel caso di un contatto di tipo Normalmente Chiuso, l'allarme avviene alla apertura dello stesso generata dalla rilevazione di un intruso da parte del sensore. Se questo contatto fosse cortocircuitato non avremmo l'allarme.



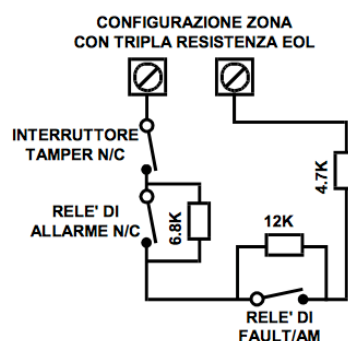
Nel caso di un contatto di tipo BILANCIATO, l'allarme avviene alla apertura dello stesso generata dalla rilevazione di un intruso da parte del sensore. Ma se i cavi di questo contatto fossero cortocircuitati avremmo un allarme, perchè non accetta la condizione NC. Infatti a riposo la centrale legge il valore di 2K2 e in allarme non legge nulla.



Nel caso di un contatto di tipo DOPPIAMENTE BILANCIATO, il controllo è attivo contemporaneamente sia sul contatto di allarme che sul contatto di manomissione. Infatti con il sensore a riposo la centrale legge la resistenza di 2K2 tra il contatto allarme e il contatto manomissione, in allarme legge il valore di 4K4 perchè il contatto di allarme diventa NO. Nel caso di cortocircuito la centrale non accetta la condizione NC e ovviamente in caso di taglio cavi avremmo comunque allarme.

Il vantaggio di un collegamento DEOL è che riconosciamo sia l'allarme che la manomissione con due soli conduttori, mentre nel caso di contatti NC è necessario portare in centrale due conduttori di manomissione per ogni sensore e realizzare una serie tra di loro, utilizzando una zona (ingresso) programmata come linea di guardia.

Nel caso si desideri che la zona 24h sia bilanciata a sua volta, si collega una sola resistenza in serie sul dispositivo più lontano dalla centrale.

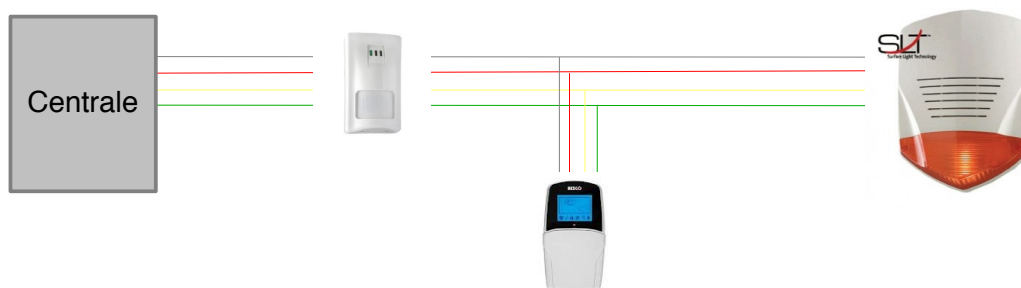


Un altro possibilità da contemplare è quello del triplo bilanciamento, detto TEOL. Collegando opportunamente le resistenze di bilanciamento, con due soli conduttori riconosciamo sullo stesso ingresso di centrale gli stati di allarme, manomissione e mascheramento del sensore (questo solo se il dispositivo prevede questa funzione). L'anti mascheramento si può attuare con una microonda o con un infrarosso attivo e sono ovviamente sensori con elevato grado di sicurezza,

Ovviamente i costi di queste apparecchiature variano sensibilmente tra loro ed è responsabilità dell'installatore consigliare il prodotto più appropriato per garantire la sicurezza del cliente.

Il collegamento delle apparecchiature sul bus, come già detto, consente di utilizzare solo 4 conduttori e soprattutto di mescolare collegamenti a stella a collegamenti lineari, in ogni caso si tratta di collegamenti **in parallelo**. Il **riconoscimento delle periferiche** è realizzato impostando opportunamente dei dip-switch (generalmente **seguendo il codice binario**).

La programmazione di ogni parametro avviene da software così come pure il monitoraggio e il test del dispositivo (alimentazione, disturbi, bontà del collegamento e altro ancora).



LA GESTIONE REMOTA DELLE APPARECCHIATURE

Finora abbiamo visto che la tecnologia semplifica il collegamento tra le apparecchiature e la programmazione, nonché la supervisione, delle stesse tramite software. Ma possiamo realizzare tutto questo semplicemente con un collegamento remoto.

In precedenza era necessario un modem dal lato installatore, con problemi di costi, di lentezza e compatibilità.

Oggi, invece, si sta diffondendo tra queste apparecchiature la possibilità di connetterle ad internet tramite il router di casa nostra. Questo generalmente richiede:

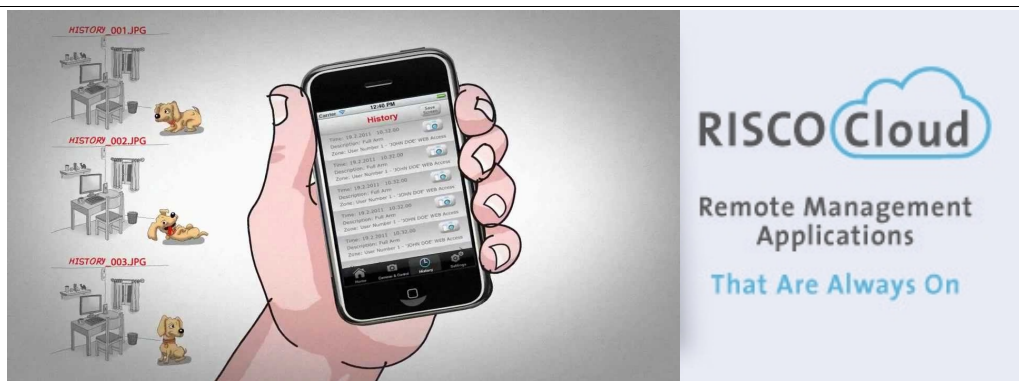
- a) un indirizzo IP pubblico che sia fisso
- b) configurare i parametri di rete correttamente (sub-net mask, gateway, ecc.)
- c) aprire le porte TCP e UDP come specificato dal produttore

Nel caso di tratti di un collegamento ADSL privato, l'indirizzo IP è dinamico, quindi cambia ad ogni riaccensione del modem e la centrale di allarme non è più rintracciabile dall'esterno. Esistono dei siti che forniscono il servizio di Re-directoring, ovvero si preoccupano di tenere traccia di questi cambiamenti, ma non sono sempre affidabili e spesso sono a pagamento.

Per questo motivo i produttori si sono attrezzati per fornire loro stessi questo servizio.

Attenzione, però, nel caso di servizi di redirectoring, se il router si guastasse, l'intera operazione andrebbe ripetuta. **Nel caso di RISCO, non si deve più operare sul router.**

Prima nel settore, da alcuni anni, per gestire completamente e comodamente il proprio sistema di sicurezza, **RISCO utilizza la tecnologia CLOUD**, sul quale un utente può registrarsi fornendo la propria email, scegliendo una user, una password e indicando il numero di serie della sua centrale antifurto.



Confermata la registrazione del dispositivo l'accesso potrà avvenire tramite app, web-browser o software di configurazione, da qualunque parte del mondo.

E' possibile utilizzare sensori ad infrarossi via radio con telecamera a bordo, che, in caso di allarme o su richiesta, inviano al proprietario dell'impianto fino ad 8 fotogrammi per sensore.

Da remoto potremo visualizzare e modificare lo stato del nostro impianto, lo stato di ogni singola zona, attivare delle uscite, leggere gli eventi in memoria, visualizzare immagini.

La facilità con cui queste operazioni sono attuabili garantiscono il successo del prodotto e, di conseguenza, dell'installatore.

Non dimentichiamoci, difatti, che solo una installazione eseguita a regola d'arte sarà veramente affidabile e soddisfacente per l'utente finale (e redditizia per l'esecutore dell'impianto).

GLI ORGANI DI COMANDO

Per organi di comando si intendono le tastiere e i lettori di prossimità. Sono collegati alla centrale tramite i 4 conduttori del bus.

Le tastiere possono avere un display LCD (generalmente 16 caratteri x 2 righe), e/o dei leds di segnalazione. In alcune versioni le tastiere hanno un display touch risultando graficamente accattivanti e molto pratiche.

I lettori di prossimità riconoscono i tag che vengono memorizzati ed associati ad un utente piuttosto che ad un altro. Va detto che sia il lettore quanto il tag possono abbinarsi ad un gruppo di zone (partizioni) l'uno indipendente dall'altro, così da creare combinazioni differenti di attivazioni.

Esempio1: Abitazione bi-familiare. Piano terra genitori, piano superiore figlio/a. **Un lettore all'esterno dell'ingresso comune.** Se l'impianto viene disattivato dal padre con il suo tag, disinserirà l'impianto del piano terra, al contrario se a disattivarlo è il figlio/a con il proprio tag si disattiverà l'impianto del primo piano (per brevità di ragionamento non consideriamo la gestione della zona comune). In questo caso è il tag a diversificare l'operazione.

Esempio2: Abitazione bi-familiare. Piano terra genitori, piano superiore figlio/a. **Due lettori all'esterno di ogni singolo ingresso.** I tag di prossimità sono programmati per accedere liberamente a tutto l'impianto. Se avvicino il tag al lettore del piano terra disinserisco solo il piano terra, se avvicino il tag al lettore del piano superiore disinserisco il primo piano. In questo caso è il lettore (non il tag) a diversificare l'operazione.

Ogni operazione viene registrata nella memoria eventi della centrale con data, ora, codice che ha operato sull'impianto e tipo di attivazione.

Se programmata opportunamente, la centrale può inviare un messaggio di avviso ad operazione avvenuta.

LE PERIFERICHE DI RILEVAZIONE

Esistono diversi tipi di tecnologie adatte al riconoscimento di una intrusione, le più usate sono quelle che utilizzano gli infrarossi passivi e/o quella che impiega le microonde. A questo tipo di rilevazioni si aggiungono i contatti magnetici, a filo, a vibrazione, ad asta.

Sensori ad infrarossi passivi

Si tratta di **sensori passivi (non hanno emissioni di alcun tipo)**, che sfruttano il calore emesso dal corpo umano per effettuare la rilevazione di una intrusione. Per questo scopo sono impiegati speciali componenti elettronici, chiamati piroelementi (o **sensore piroelettrico**). Questo elemento è opportunamente collocato in un circuito elettronico e il tutto è collocato in un contenitore dotato di una lente plastica (**lente di Fresnel**). Tale lente concentra i campi di rilevazione esattamente nel fuoco del piroelemento. Il contenitore plastico generalmente può essere dotato di uno snodo per ottenere la migliore collocazione. Occorre tenere presente che **per sua natura un sensore ad infrarossi passivi ha una migliore rilevazione se l'intruso è costretto ad attraversarne l'ottica**. Un buon sensore ad infrarossi passivi deve avere un doppio elemento sensibile, con regolazione della portata (12/15 metri mediamente) e della sensibilità, lente intercambiabile per cambiare l'area di rilevazione a proprio piacimento secondo le necessità, protezione dalla apertura e dalla rimozione. Modelli più sofisticati possiedono un sistema di antiaccecamento che impedisce di mascherare il sensore anche a impianto spento, infatti in tal caso si avrebbe un allarme dell'impianto; inoltre esistono versioni in grado di riconoscere il movimento di piccoli animali (cani e gatti per esempio) evitando falsi allarmi.

Sensori a microonde

Sono **costituiti da un trasmettitore ed un ricevitore a microonde**, contenuti nello stesso involucro, con frequenza di lavoro intorno a 10 GHz, il cui principio di funzionamento è basato sull'**effetto Doppler**. Il segnale a microonde è irradiato dal trasmettitore e quando incontra un ostacolo viene riflesso e raccolto dal ricevitore; se l'ostacolo è fermo, la frequenza del segnale di ritorno rimane invariata, se l'ostacolo si muove, la frequenza cambia: aumenta o diminuisce secondo il senso di movimento dell'ostacolo. I circuiti del ricevitore sono in grado di valutare la differenza di frequenza fra il segnale trasmesso e quello ricevuto, possono quindi, elaborando questa differenza, generare lo stato di allarme. In sostanza rileva i movimenti che avvengono nel suo raggio di azione che è variabile a seconda dei modelli, passando dai 15 mt. fino a 40 mt. Al fine di evitare falsi allarmi sono previste nei sensori la regolazione della portata e della sensibilità. Va infatti tenuto conto che a differenza dei raggi infrarossi, **le microonde attraversano superfici isolanti**, per cui l'azione del sensore si manifesta anche oltre pareti, porte di legno, vetrate, pannelli di plastica ecc., pertanto nel scegliere l'ubicazione del sensore si dovrà tener conto di queste possibilità, sia per prevenire possibili falsi allarmi dovuti a movimenti di cose o persone in zone attigue a quelle da proteggere, sia per estendere la zona di controllo ad aree separate da quella dove è installato il sensore.

Una eccezione è costituita dalla microonda di Risco in banda K (frequenza 24GHz), che ha una copertura più uniforme della zona e una minore penetrazione delle pareti o delle recinzioni.

Alcuni accorgimenti da tenere presente nell'installazione sono:

- Fissare il rivelatore a superfici stabili, esenti da vibrazioni o possibili movimenti.
- Non orientarlo verso oggetti metallici che possono oscillare, vibrare o comunque entrare in movimento. L'acqua che scorre nei tubi di scarico o nei pluviali, entrambi in plastica, può essere causa di falsi allarmi.

Attualmente nei casi con forte rischio di falsi allarmi è frequente l'impiego di sensori che combinano la tecnologia ad infrarossi passivi con la tecnologia a microonde, allo scopo di avere un allarme solo quando entrambe le tecnologie rilevano una intrusione (i cosiddetti sensori a doppia tecnologia). Esistono anche altri tipi di sensori, in gergo detti intelligenti, che effettuano il conteggio degli allarmi per tecnologia e solo raggiunto un certo rapporto di rilevazione tra le due tecnologie, rilasciano il segnale di allarme (se per esempio la sezione ad infrarossi non ha rilevazioni, mentre ne ha la sezione a microonde si ha comunque un allarme).

I sensori a singola tecnologia con microonda sono attualmente soppiantati in pratica da modelli a doppia tecnologia, che vediamo ora.

Sensori a doppia tecnologia

Si tratta di sensori che uniscono nella rivelazione entrambe le tecnologie esaminate precedentemente: gli infrarossi e le microonde. Questi rivelatori effettuano il conteggio degli allarmi per tecnologia e solo raggiunto un certo rapporto di rilevazione tra le due tecnologie entro un certo lasso di tempo, rilasciano il segnale di allarme (se per esempio la sezione ad infrarossi non ha rilevazioni, mentre ne ha la sezione a microonde si ha comunque un allarme). A tale proposito sono stati fatti molti passi avanti rispetto ai primi sensori a doppia tecnologia.

Ogni azienda produttrice sviluppa propri sistemi sempre più avanzati.

Possiamo utilizzare sensori che permettono la commutazione automatica del rivelatore da doppia a singola tecnologia. Questo previene la neutralizzazione del sistema di allarme quando il canale infrarosso dei normali sensori a doppia tecnologia viene messo in condizione di non poter rilevare un intruso (vedi mascheramento da superfici in legno, cartone, o similari).

Altre tecnologie riescono a distinguere una pianta mossa dal vento da un intruso (si tratta di brevetti RISCO). Altri rivelatori integrano un motion analyzer, ovvero un sistema che analizza la quantità e la densità della "disturbo" per decidere se si tratta di un allarme.

Sensori da esterno

L'impiego di sensori all'esterno delle proprietà è sempre più richiesto, tuttavia una rilevazione sicura, esente da allarmi impropri è molto difficile.

Tali ambienti sono di per sé a rischio elevato di falsi allarmi: vento che muove arbusti e rami, animali - sia domestici che estranei -, colpi di luce solare o dei fari delle automobili sono solo alcuni esempi. Lo sviluppo tecnologico e l'impiego di tecniche intelligenti di rilevazione ha consentito di realizzare un sensore particolarmente adatto per la protezione perimetrale esterna.

Il sensore **Watchout**, in contenitore **IP65** (unico nel suo genere), vanta queste caratteristiche:

- doppio canale a microonde (per discriminare i movimenti di arbusti e rami)
- doppio canale ad infrarossi passivi (per ottenere un piano di rilevazione tri-dimensionale)
- doppio canale ad infrarossi attivi, per riconoscere tentativi di mascheramento
- doppio canale ad infrarossi attivi, dedicato alla segnalazione di lente sporca
- **sistema anti-collisione tra le microonde**, per non avere problemi di posizionamento dei sensori
- installazione da 1 metro a 2,7 metri di altezza
- riconoscimento di animali fino a 70 di altezza

a questo va aggiunta tutta una serie di regolazioni, accessori, algoritmi proprietari che ne qualificano ulteriormente le prestazioni.

Sensore WatchOUT Risco



Sensore Beyond Risco



Sempre Risco ha introdotto sul mercato un sensore da esterno con la microonda in banda K.

I rilevatori in banda K emettono le microonde con una frequenza pari a 24 GHz, proprio per le sue caratteristiche fisiche, ha una minor forza di penetrazione degli oggetti, limitando la sua azione all'interno dell'ambiente da proteggere, infatti non è in grado di attraversare porte, muri e finestre evitando quindi possibili falsi allarmi dovuti a movimenti nei locali adiacenti.

Protezioni per finestre e porte

Oltre ai sensori di cui ho parlato sopra, ne esiste una tipologia indirizzata alla protezione perimetrale (finestre, tapparelle, persiane, porte).

Microfoni selettivi

In realtà non si tratta di contatti, ma di veri e propri sensori, costituiti da un **microfono piezoelettrico**, usati per la protezione di vetrate, cassaforti, muri, pavimenti e soffitti di camere blindate. Attivano i circuiti di allarme non appena viene tentata un'effrazione con mezzi meccanici o termici. L'attacco su materiali come vetro, cemento o metalli, produce vibrazioni in tutta la massa; il sensore raccoglie le vibrazioni e le converte in segnali elettrici che vengono poi amplificati ed elaborati in ampiezza, frequenza e durata.

Bisogna tenere presente però una sostanziale differenza tra questi sensori: quelli per la protezione di vetrate non vengono installati sulla vetrata stessa ma su di una parete adiacente o di fronte e sono sensibili alla frequenza di taglio e rottura del vetro; quelli per la protezione di muri e cassaforti vengono installati sul muro o sulla cassaforte stessa.

Contatti meccanici a vibrazione

Sono dotati di un contatto che viene fatto oscillare dalle vibrazioni che, in caso di effrazione, si producono su una vetrata: l'apertura del contatto normalmente chiuso (NC) determina l'allarme.

Contatti inerziali:

Sono un'alternativa più affidabile del rivelatore a vibrazione e permettono inoltre di proteggere superfici di vetro più ampie. Il principio di funzionamento è il medesimo: una massa metallica tende a spostarsi per inerzia sotto l'azione delle vibrazioni e apre un contatto NC. Al rivelatore è abbinato un circuito per l'elaborazione dei segnali e la regolazione della sensibilità.

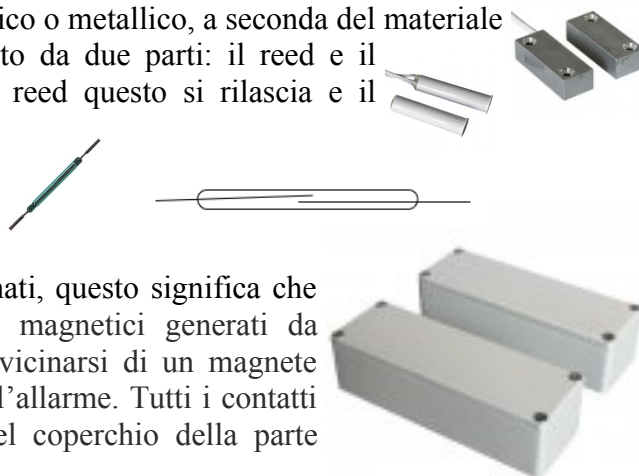
Contatti a filo

Servono per la protezione di tapparelle. L'estremità di un filo, avvolto su rocchetto, è fissata alla base della tapparella: il movimento in salita o in discesa fa ruotare il rocchetto che, a sua volta provoca l'apertura ciclica di un contatto. Come per l'inerziale, questo rivelatore necessita di un circuito per elaborare gli impulsi generati e inviati alla centrale. In alternativa al filo, un'astina metallica posta nel cassoncino "sente" l'avvolgimento o lo svolgimento della tapparella senza impiegare alcuna scheda di elaborazione dei segnali.

Contatti magnetici

Si tratta di contatti realizzati in contenitore plastico o metallico, a seconda del materiale su cui verrà installato. Tipicamente è composto da due parti: il reed e il magnete. Quando si allontana il magnete dal reed questo si rilascia e il contatto si apre.

Possono essere da incasso o da superficie.



Molte versioni sono realizzate a flussi contatenati, questo significa che diverse ampole reed s'agganciano ai campi magnetici generati da batterie di magneti, vengono sbilanciati all'avvicinarsi di un magnete esterno di effrazione attivando di conseguenza l'allarme. Tutti i contatti dispongono di protezione contro l'apertura del coperchio della parte reed.

Alcuni modelli sono dotati anche di protezione contro lo strappo della parte reed e l'apertura e lo strappo della parte magnetica e dispongono di collegamento per test remoto di funzionamento. Ovvero, richiesto si possono utilizzare anche contatti con un sensore termico tarato a 60°C (per rilevare effrazioni con fiamma ossidrica) e ad un sensore inerziale incorporato che andrà collegato ad opportuna scheda di analisi.

Sensori accelerometrici

Cominciano ad apparire in commercio dei sensori con accelerometro 3D che misura continuamente la sua posizione rispetto al suolo.

Questo rivelatore è ottimo per la protezione di oggetti di valore, come TV al plasma, dipinti, opere d'arte, sportelli bancomat, o di qualsiasi oggetto che non deve essere spostato. Le regolazioni previste evitano gli allarmi impropri.

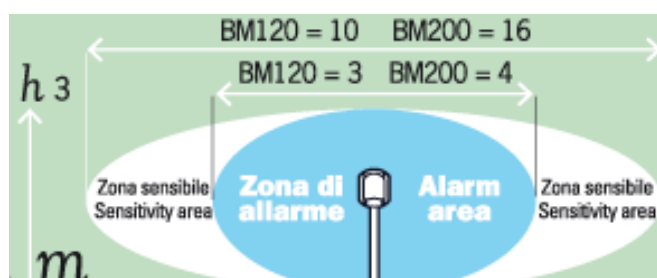
Barriere ad infrarossi attivi

Si tratta di profili in alluminio con un coperchio in plexiglas, contenenti dei trasmettitori e dei ricevitori ad infrarossi attivi. Ad ogni trasmettitore nella colonna opposta si trova un ricevitore. Queste trasmissioni sono codificate, o con lo stesso raggio trasmettente o con un cavo cosiddetto di sincronismo che corre tra la barriera trasmettente e quella ricevente. Le altezze (da 0,5 a 3 metri), le portate (da 15 a 200 metri) e le dimensioni (da un profilo di 3 x 3 cm a un cilindro del diametro di 15 cm.) possono variare. E' fondamentale che la comunicazione sia del tipo codificato e sincronizzato, per evitare possibili sabotaggi.

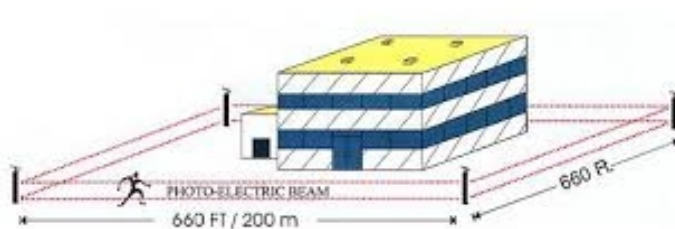


Barriere a microonde

Le barriere a microonde sono formate da un trasmettitore e da un ricevitore. Creano nello spazio che proteggono un lobo che può variare dai 3 ai 16 metri ed avere portate di 200 metri. Metà del lobo è dedicato a preallarme, mentre la metà più interna causerà l'allarme vero e proprio.



Nel caso delle barriere, per proteggere un perimetro è necessario incrociare tra di loro 4 coppie ed è fondamentale che non ci siano ad interpersi tra i fasci avvallamenti del terreno o arbusti.



LE PERIFERICHE DI COMUNICAZIONE

Questi dispositivi mettono in comunicazione la centrale con il mondo esterno. Il termine comunicazione è quanto mai proprio, infatti in questa categoria comprendiamo comunicatori vocali (noti anche come combinatori telefonici), combinatori GSM, moduli di rete.

Ogni apparecchiatura può funzionare indipendentemente dall'altra, anzi i vettori possono comunicare contemporaneamente.

Specificando meglio diciamo che il modulo vocale trasmette messaggi in fonia, quindi il ricevente sentirà un avviso di questo genere: "attenzione attenzione, tentativo di furto presso abitazione sig. X, protezioni esterne, sensore portico". Esiste a bordo della centrale una foltissima libreria di messaggi pre-registrati, ma è prevista anche la personalizzazione degli stessi (utile se ci colleghiamo con le forze dell'ordine).

Il modulo GSM invierà SMS riportanti data, ora, nome impianto, partizione, sensore e n° di zona allarmata.

La scheda di rete trasmetterà messaggi e-mail e notifiche alla app di gestione.

È evidente che posso scegliere “a chi inviare cosa”.

Se gli utenti sono stati autorizzati in fase di programmazione, possono interagire con la centrale, per spegnere l'impianto, escludere eventualmente le zone, terminare le chiamate, re-inserire l'impianto, controllare gli eventi.

DISPOSITIVI DI SEGNALAZIONE

I dispositivi di segnalazione sono le sirene, i lampeggianti e i leds.

Quindi abbiamo due tipologie di segnalazioni: ottiche, acustiche, vocali.

La normativa prevede una certa potenza sonora, un tempo massimo oltre il quale la sirena deve smettere di suonare, salvo poi riprendere in caso di altro allarme, il numero dei lampeggi e il colore della segnalazione luminosa.

Tutto questo per distinguere, per esempio, la sirena di una ambulanza da quella di un antifurto.

Vale la pena di evidenziare il collegamento di una sirena.

1° caso : sirena collagata sul bus. Con solo 4 conduttori si può eseguire una diagnostica completa, quindi sapere la tensione della batteria a vuoto, a pieno carico, la tensione di ricarica, la tensione che arriva alla scheda della sirena, lo stato del cono magnetodinamico. In programmazione determino il tempo di allarme, la frequenza dei lampeggio, abilito il suono e assegno la sirena a tutto l'impianto o solo ad una parte. Tutto molto semplice, operando da software o dalla tastiera della centrale.

2° caso : sirena con collegamento tradizionale. Occorrono due conduttori per alimentare la sirena, due conduttori per rilevare la manomissione e/o apertura del contenitore, un cavo di comando (a positivo o negativo presente). Mancando questo comando (**principio di sicurezza attiva**) la sirena suonerà per il tempo impostato in centrale. Se la centrale si guastasse la sirena attiverrebbe il proprio timer e smetterebbe di suonare.

In ognuno di questi casi, la sirena ha una batteria ermetica al piombo in tampone (tipicamente 12V 2,1Ah).

Attualmente esistono in commercio anche versioni di sirene che emettono messaggi vocali.

LE ESPANSIONI

Ogni centrale è predisposta per gestire le proprie periferiche fino al massimo delle capacità, ma in realtà spesso non è richiesto l'impiego di tutte le periferiche possibili. Per questo motivo gli impianti sono modulari ed espandibili aggiungendo schede elettroniche che svolgono compiti specifici. Queste periferiche sono collegate alla centrale tramite il bus a 4 conduttori.

Per esemplificare, se ho una abitazione su tre piani, non porterò i cavi di ogni sensore fino in centrale, ma ad ogni piano installerò una scheda ingressi a cui collegherò i sensori di quel piano. Se devo effettuare in un locale tecnico delle attivazioni tramite relè, porterò in quel locale una scheda uscite che, collegata tramite bus alla centrale, seguirà le logiche di attivazione programmate in centrale.

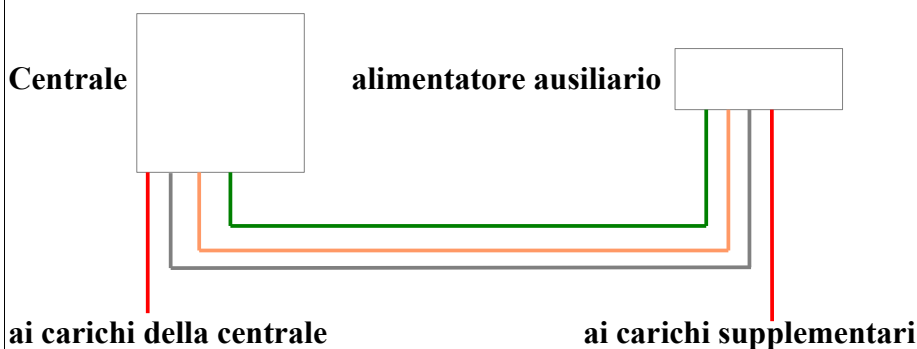
Quindi, un sistema scalabile permette di impiegare solo quelle espansioni utili a soddisfare le esigenze del cliente, aumentando la complessità e il costo dell'impianto a poco a poco.

IL GRUPPO DI ALIMENTAZIONE

I sistemi di sicurezza hanno sempre una batteria ermetica al piombo in tampone. In caso di mancanza della tensione di rete subentrerà istantaneamente per alimentare l'impianto. La capacità della batteria dipende dalla estensione dell'impianto. E' verosimile pensare che in un impianto base di un appartamento non servono alimentatori ausiliari in campo, in quanto la centrale è in grado di erogare sufficiente corrente alle apparecchiature.

Qualora l'assorbimento totale dell'impianto superasse la capacità dell'alimentatore si installeranno in campo uno o più alimentatori ausiliari.

Il collegamento tra alimentatori e centrale avviene tramite bus, ma i positivi non dovranno mai essere in cortocircuito tra di loro. È invece necessario che i negativi siano in comune.



Il negativo DEVE essere in comune affinché il riferimento a 0V sia uguale per tutte le apparecchiature.

Sul bus gli alimentatori sono supervisionati, quindi ogni anomalia verrà immediatamente segnalata, diversamente se gli alimentatori sono di tipo tradizionale non ci sarà il collegamento seriale, ma resta valido il concetto dei negativi in comune e dei positivi separati. Questi alimentatori riportano su di un morsetto la segnalazione "trouble" tramite una uscita di tipo open collector.

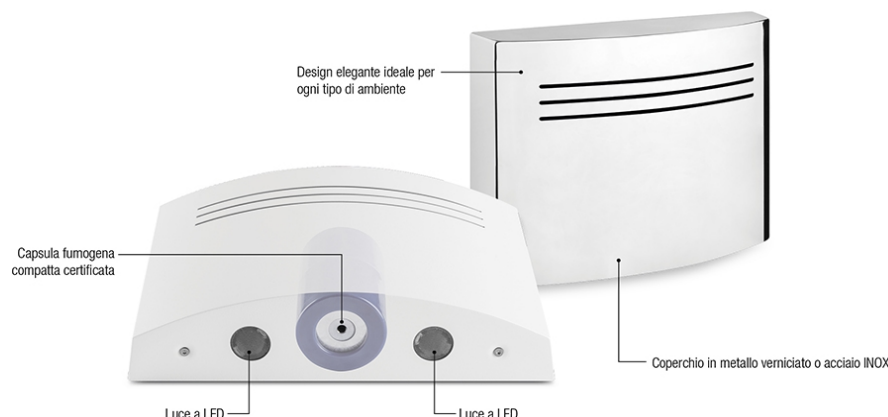
I CAVI DI COLLEGAMENTO

I cavi utilizzati nei sistemi di sicurezza sono multiconduttore, isolati in guaine di pvc non propagandi la fiamma, in coesistenza con cavi di energia in conformità alla norma CEI UNEL 36762. Generalmente si distinguono i conduttori di alimentazione (rosso e nero) perchè hanno una sezione maggiore (0,5 o 0,75 mmq) rispetto ai conduttori di segnale (tipicamente da 0,22mmq).

Intorno ai conduttori corre una treccia in rame e all'interno della guaina i conduttori sono avvolti in una lamina di alluminio. **La treccia in rame va collegata a titolo di schermo su un negativo comune in centrale: NON si deve collegare anche dal lato dell'utilizzatore, per evitare dannosi "giri di massa".**



IL FUMOGENO : COME INTEGRARE UN SISTEMA DISSUASIVO LOCALE



Attualmente si stanno diffondendo dei sistemi per impedire al malintenzionato, che non demorde dalla sua intenzione di rubare nemmeno a rischio di essere arrestato, di accedere ai beni protetti. La soluzione che i progettisti hanno adottato è quella di invadere un locale, al momento della

intrusione, con una cortina fumogena e in alcuni casi si abbinano luci strobo per aumentare lo stato di disorientamento. Il sistema in figura è prodotto dalla azienda Venitem, la quale ha realizzato il fumogeno all'interno di una applique che normalmente serve per illuminare il locale, ma in caso di allarme satura di fumo un ambiente di 100 mc. Per attivare il fumogeno occorre un segnale di preallarme e un segnale di allarme.

INTEGRAZIONE CON SISTEMI TVCC E ANTIINCENDIO E CONTROLLO ACCESSI

Le centrali moderne possono facilmente controllare rilevatori di fumo, di gas, termovelocimetrici e pulsanti anti-incendio. In alcuni casi sono costruiti dalle stesse aziende produttrici degli antifurti, in altri si utilizzano apparecchiature con uscite di allarme a relè, quindi interfacciabili facilmente con qualsiasi centrale.

Per quanto riguarda la video sorveglianza, alcuni produttori hanno realizzato sensori con PIR-CAM a bordo e utilizzando le connessioni della rete WEB, o della rete cellulare, le riprese vengono visualizzate dall'utente finale grazie a smartphone e/o tablet.

Non dimentichiamo che ogni centrale ammette decine di utenti, ognuno con un proprio codice o con un attivatore personalizzato e che ogni operazione effettuata viene registrata nella memoria del sistema e potrà essere consultata al momento opportuno. Questo permette di realizzare anche dei sistemi di controllo accesso, ancorchè non sofisticati, che il più delle volte soddisfano le necessità di una piccola azienda.

In questo modo l'installatore offre una soluzione globale, che chiude le porte ad altri concorrenti.

L'INSTALLATORE

L'esecutore dell'impianto (il cosiddetto installatore) è la "componente" più importante di un sistema di sicurezza.

I produttori migliorano continuamente i prodotti, anche perchè la tecnologia è in continua evoluzione e senza innovazione si perderebbero rilevanti fette di mercato.

L'attenzione nella realizzazione evita molto spesso gli allarmi impropri, che sono quanto di peggio possa accadere: un sistema di sicurezza deve diventare trasparente per l'utilizzatore, lo deve rassicurare e soprattutto non generare dubbi o ansie sulla sua funzionalità.

Nella valutazione del prezzo di vendita dell'impianto non bisogna sottovalutare il costo della

manod'opera strettamente legato alle difficoltà installative. Anche l'immagine che si dà di sé, durante il lavoro, deve essere qualificante. La migliore pubblicità è la soddisfazione del cliente.

Statistiche attente hanno dimostrato che una cattiva referenza ha diffusione 1:10, mentre una buona rereferenza ha diffusione 1:4.

Ciò detto, mi permetto di fornire alcuni consigli utili:

- eseguire un sopralluogo per rendersi conto delle necessità del cliente e capire le problematiche installative
- presentare un preventivo personalizzato e possibilmente corredato di informazioni sui prodotti utilizzati (se inviato per email il preventivo potrebbe essere interattivo, con foto e video esplicativi)
- conoscere le istruzioni tecniche dei prodotti utilizzati
- utilizzare apparecchiature affidabili e di alte prestazioni, non le più economiche
- lavorare operando per il “meglio” e non per il “presto”
- al momento di eseguire il lavoro presentarsi puntuale, con un tappeto su cui posare i propri attrezzi e prestare attenzione a mobilia e suppellettili

Vorrei terminare con una considerazione di carattere economico: *nel calcolo del prezzo di installazione, oltre al costo del materiale, sono da considerare le imposte, le tasse, il costo dei materiali di consumo, le spese generali e amministrative. Può sembrare superfluo un simile promemoria, ma per inesperienza molti giovani installatori alle prime armi sottovalutano questi costi e presto si trovano in difficoltà economiche. Quindi è meglio computare ogni costo a breve, medio e lungo termine (per esempio eventuale prestito per l'acquisto di un nuovo mezzo) per valutare al meglio i margini di guadagno.*

Nota finale

Questa breve guida non può e non vuole essere esaustiva, ma vuole essere lo sgabello che ci aiuta a prendere quei libri che ci “intimoriscono” e che abbiamo disposto sui ripiani in alto della libreria, libri con i quali poi approfondire l'argomento. In questa ottica spero di essere stato d'aiuto.

Grazie per la pazienza e per l'attenzione.

Giuseppe Castignani

(www.castignani.it - micro@castignani.it)

APPENDICE AL CORSO SUI SISTEMI DI SICUREZZA RISCO C/O ISTITUTO GEYMONAT



RISCO Cloud è la soluzione basata sulla tecnologia Cloud che permette la totale gestione ed il facile controllo dei Sistemi di Sicurezza RISCO come la centrale Radio Agility™3, i sistemi ibridi LightSYS™2 e ProSYS™Plus.

sulla tecnologia Cloud che permette la totale gestione ed il facile controllo dei Sistemi di Sicurezza RISCO come la centrale Radio Agility™3, i sistemi ibridi LightSYS™2 e ProSYS™Plus.

Grazie al Cloud:

- Gli Utenti possono usare le **Applicazioni Web** e **Smartphone** per controllare e monitorare le proprie abitazioni e/o uffici (inserimenti, disinserimenti, esclusione zone, attivazione relè, videoverifica, attivazioni luci via radio, controllo automatico delle tapparelle, controllo della temperatura, ecc.)
- Gli Installatori possono usufruire delle funzioni di configurazione e di aggiornamento del sistema da remoto tramite Cloud e soprattutto riceveranno le segnalazioni di guasto in tempo reale, fornendo al cliente un servizio di assistenza e manutenzione a pagamento, ma che non grava sulla struttura aziendale
- Gli istituti di Vigilanza Privata possono beneficiare del Cloud per la verifica video degli allarmi.

Gli utenti e gli installatori non hanno alcun costo o canone per l'utilizzo del Cloud di proprietà di RISCO.

In pratica avviene questo:

Il tecnico, completata l'installazione, collega la rete internet al modulo IP della centrale.

Ogni centrale ha un proprio codice identificativo di 15 cifre (11 + 4).

Per aggiungere la centrale sulla propria lista dei dispositivi collegati è sufficiente che l'installatore acceda alla pagina Cloud tecnico di Risco (<https://www.riscocloud.com/ELAS/WAAPP/>) con le proprie credenziali fornite al momento della registrazione (la mail e la password) e aggiunge alla lista il codice ID della centrale.

The screenshot shows the RISCO Cloud web interface. At the top, there are navigation links: "Lista Utenti", "Lista Centrali", and "Logout". The RISCO logo is on the right. Below the navigation bar, there's a section titled "Centrali del gruppo" with a dropdown menu and "(Pagina 1/1)". There are buttons for "Esporta in Excel" and "Nuova Centrale (per utenti esperti)". Below this is a search bar "Trova Centrali con" followed by a dropdown "Qualsiasi Campo" and a text input "contiene". There is a "Trova" button and a checkbox "Visualizza informazioni supplementari". The main part of the screenshot is a table with the following columns: ID Centrale (seriale), ID Login Web, Nome, Cognome, Cellulare, Tipo centrale, Versione firmware, Zone disponibili, Periferiche Smart Home, Provider (1), Utente, Ultima Connessione, In linea, and Nr. Scheda SIM. The table contains three rows of data:

ID Centrale (seriale)	ID Login Web	Nome	Cognome	Cellulare	Tipo centrale	Versione firmware	Zone disponibili	Periferiche Smart Home	Provider (1)	Utente	Ultima Connessione	In linea	Nr. Scheda SIM
3000					LightSYS	02.59.01	36				13/09/2016 18:00:26	No	
300					LightSYS	03.17.01	50				22/03/2017 06:48:09	SI	
4000					ProSYS Plus	01.01.00.0011	64				22/03/2017 06:32:16	SI	

At the bottom of the table, there are two buttons: "Nuova Centrale (per utenti esperti)" and "Aggiungere Centrale Utilizzando l'ID (15 cifre) consigliato".

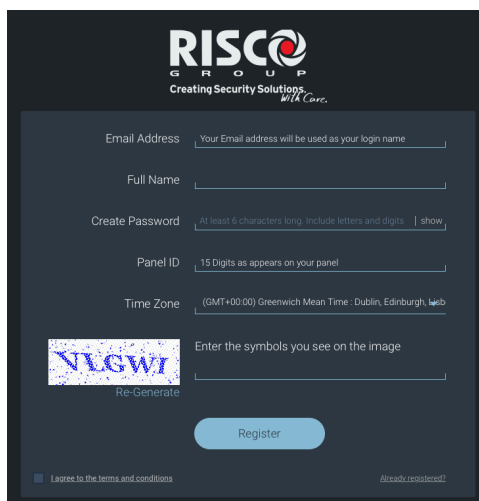
Nella schermata iniziale si vedranno i seriali, nome, cognome e cellulare del cliente proprietario dell'impianto, il tipo di centrale con la versione firmware, le zone della centrale, eventuali dispositivi smart home associati, l'ultima connessione avvenuta e se la centrale in questo momento è in linea.

Cliccando sul seriale si aprono dei menù che permettono di ottenere molte altre informazioni sull'impianto e sui dispositivi collegati.

I dispositivi collegati possono essere telecamere di RISCO o apparecchiature SMART HOME dedicate alla domotica.

A questo punto è il cliente finale, l'utilizzatore, che si collega al Cloud di RISCO , (www.riscocloud.com) si registra, riceve una mail di conferma, quindi può accedere al proprio

impianto da remoto tramite un qualsiasi PC, ovvero da smartphone scaricando l'applicazione iRisco e loggandosi utilizzando la mail fornita alla registrazione, la password e il codice di inserimento della centrale (lo stesso che utilizza in tastiera). In effetti la app sostituisce a tutti gli effetti la/e tastiera/e collegata/e alla centrale.



Il vantaggio risulta subito netto, perchè ho un quadro generale dell'impianto visualizzato in modo più chiaro ed esteso (zone aperte/chiusure, inserimenti/disinserimenti, comando delle uscite relè, controllo e gestione dei dispositivi domotici, visualizzazione immagini dalle telecamere collegate, eventi, allarmi, guasti).

Ovviamente si possono collegare più dispositivi.

La cosa interessante è che l'utente potrebbe farsi installare la centrale di comando nella casa di città e mettere online delle telecamere RISCO nella casa al mare, senza che qui vi sia una centrale installata. Lo stesso dicasi per i dispositivi domotici. Un esempio molto legato alla realtà è questo: il sig. Rossi ha un impianto di sicurezza nella propria abitazione, a casa dei genitori e a casa dei suoceri installa solo una telecamera Risco con audio bidirezionale. In questo modo potrà interagire in qualunque momento con i genitori/suoceri senza che da questi vi sia installata una centrale.

Tornando all'installatore i vantaggi non sono solo economici (più accessori installati, più alto il costo dell'impianto venduto, più alto l'utile), bensì tecnici.

Il software di configurazione (Configuration Software abbreviato in CS) permette di collegarsi al pannello di controllo (cioè la scheda elettronica della centrale di comando) con un PC, da locale la prima volta che si programma il sistema, in seguito sia da locale che da remoto via internet. Questo è importantissimo perchè si possono modificare tutte le programmazioni eseguite dal proprio ufficio, dalla propria auto, senza doversi recare sul posto, con evidente risparmio di tempo e denaro (consumo di carburante, gomma, autostrada, ecc.) Inoltre, sempre da remoto, si possono eseguire dei test dinamici per verificare il corretto funzionamento delle apparecchiature. Per esempio il test della sirena verifica in tempo reale, la tensione di ricarica, la tensione e l'assorbimento della batteria a vuoto e in allarme, il corretto funzionamento dello speaker). I test dinamici consentono su comando o in autotest, di sapere per tempo se un dispositivo si è guastato, se una batteria è da sostituire, e via dicendo.

L'installatore può farsi inviare, in automatico, delle mails da ogni impianto, per eventi tecnici. Ciò permette all'installatore di sapere che l'impianto del Sig. Verdi ha la pila del trasmettitore della sala scarica, il Sig. Bianchi ha il cono della sirena in cortocircuito, che la tastiera #2 del Sig. Rossi non comunica sul bus e via di seguito.

Queste sono assistenze da eseguire rapidamente ed è lo stesso installatore che informa l'utente finale, il quale è certamente soddisfatto di ricevere questo tipo servizio ed è sempre disposto a pagarlo, in alcuni casi richiede egli stesso un contratto di manutenzione. Il tutto, ovviamente si traduce in denaro e in buona pubblicità.