L’AUTORE:

Marco Saporiti nato nel lontano 1959 a Verona, ma di fatto milanese sin da bambino era attratto da tutto quello che in qualche modo era legato all’elettronica, l’informatica la scienza. L’esperienza maturata negli anni nel settore dell’impiantistica ed in particolare quella relativa alla sicurezza lo ha portato ad avere una cultura specifica, tanto che proprio per il fatto di essere nato nella fase di passaggio tra la vecchia tecnologia cosiddetta “a valvole”, poi quella “a transistor” ed infine quella “digitale” , gli ha fornito quell’esperienza che ben pochi possono vantare. I problemi dati dalle prime centraline antifurto, fonte di falsi allarmi continui, gli anni di piombo, le rapine del secolo, i sequestri degli anni ’80, le linee telefoniche tradizionali, i primi cellulari, il teledrin, i primi computer Commodore 64, Spectrum, Amiga , così come le prime centraline Coves Tervis, i primi sensori ad ultrasuoni e via dicendo, sino ad arrivare alla tecnologia attuale , impensabile allora, ecco tutto questo ha dato all’autore (sono io, ma preferisco parlarne dal punto di vista dell’amico che mi descrive ad un altro amico…), la professionalità e la possibilità di scrivere questo libro indirizzandolo a quel lettore che voglia avvicinarsi per necessità o semplice curiosità al mondo della sicurezza con una lettura scorrevole, leggera quasi romanzata, non trascurando chi, vuole avere anche una conoscenza più tecnica più specifica per intenderci: come?, perché?! In questo libro, per ovvi motivi, tutto è relativo alla normativa vigente in Italia, perché ogni Stato ha le sue diverse regole in materia sicurezza, ad esempio, in Russia è possibile dotare la protezione perimetrale di un impianto ad alta tensione che dia la << scossa >> , spesso anche la morte a chi volesse tentare un intrusione non autorizzata, in Italia questo è vietato. Gli argomenti trattati sono molti, ma in particolare essendo questo libro, rivolto alla generalità della popolazione,

saranno trattati con maggiore enfasi e farciti di particolari i temi della protezione domestica . L'autore non ha mai subito un sequestro, una rapina, uno scippo e tantomeno un furto, quindi forse non ha una base psicologica per allietare chi invece lo ha subito, ma ha certamente impedito che questi eventi avvenissero dove con la sua esperienza e la sua consulenza ha indirizzato intere famiglie, facoltosi imprenditori, grandi magazzini, persino stalle e celle frigorifere a dotarsi delle opportune tecnologie atte a prevenire, reprimere e scoraggiare piuttosto che correggere, rimediare e a salvare il salvabile.
Questo è il punto! L'autore cercherà di far capire che anziché aspettare che avvenga un furto, e poi dotarsi di un impianto che ne impedisca il successivo, è meglio dotarsi di tutto il necessario perché questo non avvenga mai, i tempi di Arsenio Lupin , Robin Hood sono finiti, adesso anche per rubare un autoradio ci si munisce di un arma, non si esita a minacciare, ferire uccidere.
N.B.: Generalmente in questa pagina la foto ritrae l'autore, ma poiché la mia immagine potrebbe distogliere dai temi reali trattati, ho preferito dare un immagine " in tema " precisando che ovviamente, con l'autore non ha alcun legame…

Marco Saporiti

•PREMESSA*:*

Il presente volume è frutto di decenni di esperienza, e si propone di fornire un valido sussidio all'apprendimento delle specifiche tecniche che determinano la scelta di un tipo di antifurto anziché un altro, il posizionamento ideale per proteggere al meglio l'ambiente e le tattiche utilizzate dai malintenzionati, così da fornire un valido aiuto contro tentativi di furto, rapina, sequestro.
Il lettore anche se privo di dimestichezza, dispone di un elevato numero di indicazioni correlate da suggerimenti che consentiranno di scegliere il tipo di impianto da installare. Sono illustrate tutte le tipologie, da quella più semplice a quella di ultima generazione evidenziandone i pro e i contro di ognuna.

INTRODUZIONE:

Gli antifurto sono per definizione, i dispositivi che impediscono i furti, ma così erroneamente sono chiamati anche i dispositivi antieffrazione e antitaccheggio. E' bene, invece, distinguere accuratamente le diverse definizioni perché è evidente che anche le protezioni saranno diverse, e così i risultati ottenuti.
Gli antifurto, generalmente intervengono, quando il furto è già stato commesso, gli antieffrazione al contrario, intervengono prima che questo avvenga. Gli antitaccheggio , che come vedremo, sono facilmente neutralizzabili, vengono utilizzati all'interno dei grandi magazzini, ed intervengono quando l'oggetto protetto viene fatto passare attraverso percorsi obbligati atti a rilevare (e rivelare) il mancato pagamento dell'oggetto stesso.
Nella presente edizione parlerò ampliamente anche di antirapina, antisequestro sempre differenziando le due diverse ubicazioni dell'installazione, la casa, la proprietà privata, l'auto, e l'azienda, il negozio, lo stabilimento, il parcheggio ecc.. E' infatti evidente che laddove vivano solamente persone del nucleo familiare difficilmente ci si pone il problema di impedire che qualcuno dall'interno possa "preparare" l'impianto affinché non intervenga nelle ore successive, nottetempo, cosa invece da non sottovalutare in ambienti frequentati da numerose persone, come le aziende, i negozi.

Nello scegliere i dispositivi da utilizzare bisogna innanzitutto pensare alla cosa da proteggere – il valore della "cosa" non deve determinare il valore dell'impianto o della protezione utilizzata, bisogna invece pensare sempre ad impedire l'accesso alla "cosa" dovendo valutare i costi di un'eventuale intrusione, che determina danni materiali (porte, finestre, mobili), oltre al rischio di incontri non desiderati con possibili reazioni anche a danno della propria vita. Infatti, ad esempio, per proteggere qualche gioiello di famiglia, si pensa sia sufficiente dotarsi di una cassaforte, ma se inserita in un ambiente non protetto, non si può escludere l'intrusione, il danneggiamento e non si può nemmeno escludere che la cassaforte stessa sia asportata, o comunque aperta da persone con esperienza.

E' bene iniziare a pensare che ogni oggetto (come una cassaforte) che dispone di un sistema di apertura di emergenza –nel caso di batterie scariche, combinazione dimenticata ecc-permette facilmente l'utilizzo di questi sistemi anche agli estranei che conoscono i particolari di ogni cassaforte, così come la chiave che serve ad aprirla nel caso non funzionasse il sistema elettronico.

Raramente chi la possiede porta con sé la chiave, tende a nasconderla in casa, dove c'è la cassaforte. La cassaforte in un appartamento deve avere come unico scopo, quello di ritardare, di rendere difficoltoso il "lavoro" del malintenzionato, perché è ovvio, che lasciare oggetti di valore a portata di mano, può non impedire all'impianto di rilevare l'ingresso del ladro, ma non impedire allo stesso di appropriarsene e di darsi alla fuga. Tenere presente che la sirena non sempre è un deterrente, perché ormai non ci si fa' caso. Quindi i mezzi di segnalazione sonora devono servire come prima cosa ad infastidire e mettere in fuga il ladro – prima che riesca ad appropriarsi della cosa, e dopo, a richiamare l'attenzione.

Riassumendo: Un sistema di sicurezza, per la protezione di un luogo e le persone che vi dimorano dovrebbe consentire:

AZIONE DETERRENTE: Fare in modo che eventuali malintenzionati decidano di non iniziare l'intrusione in quanto hanno la consapevolezza che il luogo è adeguatamente protetto.

AZIONE DISSUASIVA: Far sì che l'intrusione sebbene iniziata, si interrompa in quanto è individuata e segnalata.
AZIONE DIFENSIVA: Consentire agli occupanti il sito protetto, un adeguato tempo per organizzare anche sotto il profilo psicologico, la reazione nonché dare un congruo tempo alle forze dell'ordine per l'intervento.
Premesso questo, iniziamo a definire e illustrare i diversi sistemi di rivelamento e quindi il loro utilizzo più appropriato:

♦**SISTEMI DI RILEVAZIONE PERIMETRALI:**

Si tratta di apparecchiature in grado di rilevare un tentativo di intrusione ancor prima che esso avvenga, sorprendendo quindi il ladro fuori della zona protetta e permettendoci di rimanere all'interno senza alcun problema. Esistono una vasta gamma di prodotti atti a questo tipo di protezione che vanno dalle barriere a microonde, barriere a infrarossi, sensori interrati nei giardini o integrati nella pavimentazione, rilevatori di taglio vetri o di recinzione, fino ai semplici contatti magnetici su porte e finestre.

♦**SISTEMI DI RILEVAZIONE VOLUMETRICI:**

Sono quelli che si conoscono comunemente come sensori a infrarossi, anche se il termine è restrittivo, visto che ormai quasi sempre la tecnologia dell'infrarosso è utilizzata in combinazione con quella delle microonde. Comunque sia, qualsiasi tecnologia andiamo ad utilizzare, il fine è sempre lo stesso, ossia proteggere l'interno di un ambiente in modo che nella zona controllata sia impossibile effettuare movimenti senza che questi determinino l'avvio delle segnalazioni di allarme.

♦**SISTEMA DI CENTRALIZZAZIONE:**

Stiamo parlando del cervello di ogni impianto d'allarme, la centrale, cioè il dispositivo elettronico che riceve i nostri comandi, riceve i segnali da tutti i rilevatori, aziona i dispositivi di segnalazione e molto altro ancora. Molto spesso le principali caratteristiche di un sistema d'allarme, dipendono per la maggior parte dalla centrale, infatti, sul mercato sono disponibili prodotti che permettono oltre alla sorveglianza elettronica di un ambiente, anche le più disperate funzioni come ad esempio l'ascolto ambientale dal vostro cellulare, l'accensione di un dispositivo elettrico a distanza, la gestione di tutto il sistema di allarme dal computer o dal cellulare, così come l'invio di messaggi specifici (furto, rapina ecc) e molto altro..

♦**DISPOSITIVI DI SEGNALAZIONE:**

Sono quelle apparecchiature elettroniche che hanno il compito di comunicare un tentativo di effrazione, cioè sirene, lampeggiatori, combinatori telefonici, ponti radio e così via..

In pratica oggigiorno non abbiamo più a disposizione solo le sirene per avvertire qualcuno di un tentativo di furto, ma possiamo contare sull'affidabilità dei combinatori telefonici, apparecchi che attraverso la linea telefonica o rete cellulare, ci comunicano con messaggi registrati o con degli sms che qualcuno vuole violare l'ambiente da noi protetto. Tutto questo aumenta l'efficacia dell'impianto d'allarme e riduce di molto i tempi di intervento, sia per noi che per le forze dell'ordine.

♦**DISPOSITIVI ANTIRAPINA:**

Sono costituiti da pedane-tappeti o pulsanti nascosti o celati in modo da non destare sospetti, e si attivano con procedure atte ad evitare false segnalazioni o errate attivazioni. I dispositivi antirapina NON devono attivare i dispositivi di segnalazione sonora, ma solo inviare un apposito segnale a chi si deve attivare per intervenire. Questo perché, generalmente, il rapinatore all'avvio di una sirena potrebbe reagire sparando, prendendo ostaggi ecc (la stessa ragione per la quale agli addetti lo sportello viene detto di non reagire); raramente, si da' alla fuga. Quindi al contrario, è bene cercare di ritardare la fuga del rapinatore, trattenendolo il più a lungo all'interno in modo che la segnalazione di tentata rapina, o rapina in corso abbia il tempo di attivare tutte le procedure d'intervento delle forze dell'ordine, che possono attendere all'esterno l'incauto malvivente senza mettere a rischio le persone che in quel momento si trovano all'interno. In alcuni casi si attivano procedure elettroniche, che, quando ricevono un allarme antirapina, permettono alle porte blindate di ingresso / uscita di bloccare chi tenta la fuga, quando si appresta ad uscire.

I dispositivi antirapina sono generalmente di tipo autobloccante, cioè una volta attivati, per disabilitarli o per ripristinare la condizione iniziale, richiedono una chiave, senza la

quale mantengono il dispositivo in allarme anche se questo non è più premuto. Il motivo di questa scelta è presto detto: Intanto posso sapere chi o da dove è stato attivato, poi una volta attivato, anche sotto la minaccia delle armi non potrò disattivarlo.

♦**PUNTI DEBOLI:**

Entriamo ora nel dettaglio di ogni singola tipologia :

Innanzitutto al di là dei dispositivi utilizzati, dalla complessità o meno dell'impianto anti intrusione, si deve ben valutare il punto debole di tutta la struttura. Quello cioè che permette al legittimo proprietario la possibilità di inserire o escludere l'impianto d'allarme.

È chiaro che avere a disposizione un impianto tale da scoraggiare chiunque anche solo a pensare di tentare l'effrazione, e poi dotare l'ingresso di un cartello con scritto: << Per disattivare l'allarme, premere il pulsante giallo…>> vanificherebbe tutto. Quindi come prima cosa va' pensato il tipo di "chiave" da utilizzare, e subito dopo, il suo posizionamento.

Esistono molti sistemi, le chiavi elettroniche, quelle meccaniche, i sistemi a combinazione, i lettori di impronte digitali, fino ad arrivare a riconoscitori vocali, dell'iride o misti, che utilizzano cioè più sistemi tra quelli indicati. Sono da eliminare senza dubbio le chiavi di tipo meccanico. Possono facilmente essere disattivate e per questo motivo vengono utilizzate unicamente all'interno di ambienti già protetti, dove si presuppone che per utilizzare la chiave meccanica , si sia già stati abilitati a raggiungerla passando alcuni dispositivi più qualificati.

Le chiavi elettroniche sono le più utilizzate; La tecnologia ha ormai raggiunto livelli tali da garantirne il funzionamento ed impedirne la manomissione o la duplicazione. In base al tipo di impianto una stessa chiave può inserire completamente l'area da proteggere, oppure parzialmente (impianto a zone) , permette di inserire l'impianto anche in presenza di persone all'interno (protezione perimetrale) o permette di accedere solo ad alcune aree, di percorrere corridoi prestabiliti, di aprire solo alcune porte ecc..(protezione settoriale).

Come tutte le chiavi, anche quella elettronica può andare perduta, essere dimenticata e più difficilmente duplicata. Per questo motivo, gli apparati antintrusione dispongono della possibilità di inserire o disattivare l'impianto anche utilizzando una seconda opzione, che spesso è quella di una tastiera numerica posta sulla centrale. Insisto nello ripetermi, ma rifiutate quegli impianti che utilizzano come chiave di emergenza la chiave di tipo meccanico!
Le chiavi elettroniche non hanno dispositivi di segnalazione, che invece –devono- essere presenti sulla sua analoga serratura. Sono dei led colorati rossi, verdi e gialli, indispensabili perché spesso non si sa se l'impianto è attivo, oppure avere la conferma di un avvenuto inserimento, o ancora sapere che l'impianto è stato disattivato perché qualcuno si trova già all'interno. Un'altra utile indicazione è data dal lampeggiamento di uno dei led, che indica l'avvenuto allarme durante l'assenza, oppure l'impossibilità di inserire l'impianto perché uno o più dispositivi sono in allarme. Ad esempio, se dimentico una finestra aperta, e se questa è protetta, non potrò inserire l'impianto (a meno che non sia previsto il contrario) fino a quando non avrò chiuso quella finestra. La norma prevede che il colore rosso indichi allarme inserito, il verde via libera, il giallo indica un inserimento parziale. Qui è opportuno valutare se è meglio far sapere all'eventuale malvivente che l'impianto è inserito o meno. Spesso si preferisce invertire le segnalazioni, così da far credere che l'impianto sia disattivato, quando invece non lo è. Personalmente lo sconsiglio, è sempre meglio disincentivare e prevenire, poiché nel caso contrario, potrei sì salvare l'appartamento, ma probabilmente non la porta di ingresso, forzata senza tante delicatezze da chi, credeva di introdursi in un ambiente non protetto, così come la possibile confusione che si genera con il dubbio sarà inserito o no?; Meglio lasciare le cose come previste anche se tecnicamente, invertire le segnalazioni è semplicissimo.
Tutti i dispositivi di antintrusione prevedono la possibilità di inserimento immediato o ritardato dell'impianto. Quello ritardato si utilizza, quando la "chiave" è posta all'interno dell'area protetta, e quindi è necessario aprire la porta (viene attivato un pre-allarme silenzioso), entrare e disattivare l'impianto entro il

tempo stabilito. Lo stesso avviene nel percorso inverso – attivo l'allarme e devo uscire dall'area protetta prima che sia passato il tempo stabilito(sempre programmabile a piacere). Anche in questo caso, se non è assolutamente possibile agire diversamente, sconsiglio di utilizzare i sistemi ritardati, perché permettono l'ingresso del malintenzionato per un tempo sufficiente a fare danni, rubare e persino minacciare i presenti costringendoli a disattivare l'impianto.
I dispositivi ritardati sono indicati – come vedremo- nelle protezioni perimetrali, nei giardini, nei box dove spesso l'impianto viene attivato prima di abbandonare l'area protetta. In questo caso l'abitazione rimane chiusa, la chiave è esterna e il tempo necessario è quello di percorrenza del vialetto, del giardino, della rampa del box ecc.. Tra le chiavi elettroniche vi sono anche quelle che utilizzano la tecnologia "trasponder" quella cioè che permette all'utilizzatore di tenere la chiave in tasca, o comunque di attivare o disattivare l'impianto senza la necessità di utilizzare le mani, quindi anche con il semplice passaggio nella zona prevista, senza che occhi indiscreti possano accorgersi di nulla.
Abbiamo detto quindi che la chiave deve essere posta all'esterno dell'area da proteggere. Ma spesso si predilige un impianto di livello superiore, quindi una doppia protezione: perimetrale (porte, finestre, giardino,box ecc..) e volumetrica (gli interni) .Utilizzando questo sistema posso inserire l'impianto anche quando sono in casa, di notte posso dormire tranquillo senza correre il rischio di trovarmi nel letto estranei…Dovendo poter inserire la protezione perimetrale, ma non quella volumetrica, che mi impedirebbe inevitabilmente il movimento nella mia stessa casa, ecco che diventa necessario installare due chiavi: una all'esterno per l'inserimento totale dell'impianto e una all'interno per l'inserimento perimetrale,lasciandomi libero di muovermi. Per non generare confusione, è bene prevedere in fase di configurazione che la stessa chiave se inserita all'interno, attivi e disattivi la protezione perimetrale, e dall'esterno tutto l'impianto. Ci sono anche sistemi che in base al numero di volte che la chiave viene inserita e tolta, o in base al tempo che viene lasciata inserita

nella sua serratura (inseritore) in modo ciclico si inserisce nell'ordine: -spento – perimetro – volumetrico – totale – spento . Questo permette maggiore libertà d'azione, poiché posso eseguire tutte le operazioni sia all'interno che all'esterno, ma richiede molta pratica per evitare di inserire l'area sbagliata. I led sugli inseritori indicano la condizione attuale ma, più sono le funzioni, maggiore è la possibilità di fare confusione. Se ci si orienta per un impianto a zone, dove cioè alcune aree possono rimanere sotto protezione, mentre altre sono libere, è bene prevedere di installare gli inseritori parziali all'ingresso delle singole aree, lasciando un eventuale controllo generale alla centrale, così che se decido di entrare in un'area posso attivarla e disattivarla secondo necessità, e se invece devo abbandonare l'intero complesso, posso inserire l'intero impianto senza dovermi preoccupare di passare da un'area e l'altra . Alcuni impianti prevedono la possibilità di segnalare i tentativi di utilizzo di chiavi diverse da quelle memorizzate, denominati " chiave falsa" e può inviare un allarme specifico, oppure limitarsi a segnalare (facendo lampeggiare un led sull'inseritore) il tentativo di manomissione. Poiché un tentativo di disattivare l'impianto utilizzando una chiave diversa non disattiva le protezioni, l'allarme di chiave falsa generalmente non attiva avvisatori acustici o combinatori telefonici, anche perché lo stesso proprietario potrebbe per errore utilizzare una chiave utilizzata per altro impianto(ufficio). Diverso il discorso di un eventuale taglio dei cavi, o tentativi di ponticellare i contatti su porte o finestre (**antimanomissione** – tamper) , oscurare i sensori volumetrici (**antioscuramento**), deviare i raggi utilizzando specchi o altri mezzi riflettenti (**antiaccecamento**), riempire di schiumogeni le sirene (**antischiuma**), o rimuovere i dispositivi (**antirimozione**). In questi casi l'allarme deve attivarsi immediatamente, ed è sempre in funzione sia che l'impianto è stato inserito o no. Per questo nei casi di intervento tecnico, o quando è necessario aprire la custodia di un sensore, la centrale o le sirene, si può inibire il controllo di antimanomissione solo utilizzando procedure particolari, come una combinazione numerica diversa da quella utilizzata per l'utilizzo normale, oppure con una chiave apposita, o negli impianti meno recenti,

lasciando suonare l'impianto per il tempo necessario a bypassare la protezione utilizzando una procedura non semplice, che richiede la conoscenza dell'impianto e i valori dei componenti elettronici da utilizzare allo scopo (circuiti bilanciati, resistenze di precisione). Un altro punto debole potrebbe essere costituito dalla sirena esterna, che se neutralizzata permette agli intrusi di lavorare con maggiore tranquillità.

♦**LE SIRENE:**

Le sirene sono posizionate ad altezze tali che per raggiungerle è necessaria come minimo una scala, che ovviamente sarà tenuta all'interno dell'area protetta dal proprietario. Poiché questo non costituisce un certo impedimento, le sirene sono dotate di tre tipologie di protezione:

ANTI RIMOZIONE : Si attiva se viene staccata dalla parete dove è fissata.

ANTI APERTURA : Rileva un apertura regolare, anche senza utilizzare attrezzi da scasso, apertura comunque difficoltosa dato che i coperchi sono sempre due – entrambi protetti - .

ANTI SCHIUMA: Questa protezione si è resa necessaria dopo che ci si è resi conto di una prassi utilizzata per rendere inoffensiva la sirena; Riempivano di schiuma utilizzando bombolette spray o altri materiali simili la sirena utilizzando le fessure che permettono il passaggio dell'aria e di conseguenza il suono, riuscendo così a ridurre, se non a reprimere completamente ogni emissione sonora, pur mantenendo la sirena in funzione.

Come tutti i dispositivi di segnalazione, anche la sirena deve essere autoalimentata, cioè in grado di funzionare in modo autonomo, quindi disporre di una batteria ricaricabile al suo interno. Un'eventuale anomalia di funzionamento della batteria deve generare un pre-allarme o una segnalazione dalla centrale al fine di evitare che quando necessario, la sirena non sia perfettamente in grado di fare il suo dovere.

È bene precisare che le attuali normative circa l'inquinamento acustico e le disposizioni in materia di segnalazioni acustiche, stabiliscono i tempi di allarme compatibili con la Legge e cioè: La sirena deve inviare un allarme sonoro per un tempo massimo di tre minuti continui, una pausa di un minuto, e per un massimo di tre volte il ripetersi di queste condizioni. Escludendo quindi un'eventuale rimozione o manomissione, l'allarme generato da un tentativo di effrazione o furto, attiva la sirena che non potrà suonare all'infinito, ma rispettando le normative smettere di suonare completamente dopo dodici minuti, indipendentemente dallo stato di allarme che la ha attivata. L'abbinamento con un

lampeggiante è necessario per individuare l'origine dell'allarme . In impianti particolari il lampeggiatore della sirena è utilizzato per inviare appositi segnali, atti ad indicare al proprietario, prima che questi entri nella sua proprietà, se all'interno c'è qualcuno, se durante la sua assenza l'allarme ha suonato e così via. Per permetterne l'installazione, la sirena dispone di un particolare circuito che attiva le protezioni interne solamente quando, una volta inserita la batteria, ed effettuati tutti i collegamenti, viene chiusa completamente e quindi alimentata dalla centrale. Da quel momento se ci si accorge , ad esempio, di avere dimenticato qualche collegamento o comunque se devo riaprirla, dovrò munirmi di cuffie protettive, aprire la sirena e farla suonare senza alcuna possibilità (se non quella di scollegare tutto di nuovo,batterie comprese) di tacitarla. Quando avrò completato il lavoro, e richiusa completamente dalla centrale con le funzioni appropriate potrò finalmente ripristinare lo stato di quiete.
Segnalo anche l'esistenza di sirene particolari, sicuramente molto efficaci, che diversamente dalle altre richiamano senz'altro l'attenzione e che inducono il malintenzionato alla fuga: sono quelle che utilizzano un sintetizzatore vocale, un messaggio parlato al posto del suono tipico. Immaginate di sentire un messaggio di questo tipo: < Attenzione, è in atto un tentativo di furto presso l'abitazione… in via…ecc..> Lo stesso messaggio può essere inviato attraverso un combinatore telefonico alle forze dell'ordine e può essere differenziato in base al tipo di allarme intervenuto, quindi furto, rapina, manomissione e se abbinato ad altri servizi anche: incendio, allagamento, fuga di gas e così via.

♦**COMBINATORE TELEFONICO:**

Il combinatore telefonico è un dispositivo in grado di inviare alcuni messaggi pre-registrati attraverso la linea telefonica tradizionale o utilizzando un cellulare interno. L'utilizzo del cellulare garantisce contro la possibilità che il malintenzionato tagli i fili della linea telefonica dall'esterno, anche se alcuni combinatori telefonici prevedono questa possibilità ed attivano un allarme nel caso in cui venga a mancare la linea, che è sempre monitorata dai circuiti elettronici interni. Diverso il caso in cui, anziché tagliare la linea, ci si limiti ad "occuparla" alzando ad esempio la cornetta del telefono, e lasciandola sollevata per il tempo necessario. In questo caso, il problema non si pone se si utilizza una linea dedicata, mentre non sarà possibile utilizzare un sistema di controllo (**presenza linea – linea occupata**) se il combinatore è collegato ad un'unica linea telefonica, utilizzata anche per le normali attività nel luogo da proteggere. In questo caso, la linea deve essere collegata in ingresso al combinatore telefonico, ed in uscita ai telefoni di casa, così che, il combinatore avrà sempre la priorità e sarà lui stesso a prendersi la linea, disconnettendo i telefoni, quando dovrà inviare allarmi. L'utilizzo di un cellulare, invece, da' maggiori garanzie, ed è situato all'interno della centrale o nel combinatore, ha una sua scheda sim, un suo numero di telefono, molto spesso adibito allo scopo, quindi con un contratto particolare, una tariffa adeguata e abilitato alla sola trasmissione dati, quindi non utilizzabile come normale "telefonino". Nel combinatore telefonico si possono programmare i numeri telefonici da chiamare, l'ordine con il quale questo avviene, e il numero di volte che il numero deve essere richiamato se trovato occupato, così come il tipo di messaggio (furto-rapina sms ecc..). I messaggi da inviare possono essere registrati direttamente dall'utente, oppure essere già pronti, pre-registrati o programmati. Nell'ultimo decennio si è abbandonato il sistema di registrazione che utilizzava un nastro magnetico, preferendo quello che della registrazione digitale. Come ogni dispositivo di segnalazione, anche il combinatore deve avere all'interno una batteria tampone ricaricabile, e le protezioni contro l'apertura , la manomissione e la rimozione forzata. Generalmente i messaggi

sono inviati ad amici, parenti, vicini di casa o ai proprietari dell'appartamento stesso, mentre l'invio di messaggi ai numeri 112 o 113 richiede una preventiva autorizzazione, non sempre concessa, dato che un falso allarme attiverebbe comunque l'intervento delle forze dell'ordine, già occupate in altre operazioni, con costi elevati e rischio di denuncia per procurato allarme; meglio allora rivolgersi ad istituti di vigilanza che con un abbonamento annuale accettano volentieri il servizio, non limitandosi ad attendere una richiesta d'intervento, ma tenendo sotto controllo costante l'impianto, attivandolo a distanza, utilizzando parole chiave di riconoscimento per un eventuale errore di utilizzo dell'impianto e cosi via. Spesso in questo caso in particolare negli esercizi commerciali o industriali, al posto del combinatore telefonico è utilizzato un ponte radio collegato direttamente con l'istituto di vigilanza ed è in grado di svolgere tutte le funzioni del combinatore telefonico con l'aggiunta di tutte quelle possibili eseguire dalla centrale(comandi a distanza). È bene precisare che le centrali mantengono nella loro memoria interna lo storico delle operazioni eseguite, quindi è sempre possibile sapere se e quando è stato attivato l'impianto, da quale zona è provenuto un allarme e quando e negli impianti più evoluti anche quali persone si trovano all'interno dell'area protetta, nonché tutti i dati relativi agli orari di ingresso e uscita delle persone abilitate ad accedere in aree controllate. Le centrali possono essere abbinate a stampanti, che nei casi appena citati riporteranno su carta tutti i dati memorizzati sino a quel momento, in mancanza della stampante i dati potranno essere letti su un display posto quasi sempre sulla centrale stessa.
Quando parliamo di dispositivi di segnalazione abbinati ad impianti antintrusione o furto, dobbiamo sempre tenere presente che tutti, quindi anche le stampanti appena descritte, devono poter segnalare un'assenza di tensione, un tentativo di manomissione ecc.., quindi se qualcuno eventualmente dovesse distruggere la stampante per eliminare i dati che porterebbero alla sua identificazione, questi dati devono poter venire recuperati e quindi mantenuti in memoria sino alla loro rimozione attraverso

procedure tali da impedirne una cancellazione involontaria o forzata.

♦DISPOSITIVI PERIMETRALI:

Si definiscono dispositivi perimetrali tutti quelli che proteggono il perimetro e gli accessi. Sono perimetrali quei dispositivi che proteggono porte, finestre, persiane, tapparelle, i dispositivi a barriera, quelli interrati o posti sulle recinzioni. Sono costituiti principalmente da contatti magnetici, serpentine, a corda, a pressione e da barriere a fasci infrarossi o microonde.

Contatto Basculante

Lo scopo è quello evidente di segnalare con la dovuta tempestività ogni tentativo di entrare all'interno dell'area protetta anche quando al suo interno sono presenti persone, in modo che queste possano intervenire tempestivamente ed evitando sgradite sorprese tipiche in questi casi. Ogni tipologia d'accesso ha la sua analoga protezione; Nel caso delle tapparelle le scelte sono due, un contatto basculante che inserito all'interno dei cassoni, e posto in modo da rilevare un aumento del diametro dell'albero avvolgitore, così che sollevandola, attivi il dispositivo. L'altro è costituito da una cordicella collegata ad un apposito sensore di movimento, anch'esso posto all'interno del cassone, con la corda fissata al centro della tapparella . In questo caso la protezione offerta è maggiore, poiché ogni movimento verso l'alto o il basso di circa un centimetro invia una segnalazione di allarme.

Contatto Tapparelle

Contatto Magnetico

Questo permette di tenere la tapparella abbassata quanto basta per evitare un ingresso indesiderato, con le finestre aperte, in pratica l'apparato memorizza la posizione della tapparella e ne segnala ogni minima variazione. Per il contatto basculante questo non è possibile. In questo caso invece, il taglio della corda genera un allarme e un tentativo di tagliare o forare la tapparella anche. Con un contatto basculante il taglio o la foratura di una saracinesca non garantisce che questi saranno rilevati. Nel dover proteggere una saracinesca a maglie, quindi aperta, il contatto basculante è l'unico possibile, oppure sarà necessario utilizzare contatti di tipo magnetico. I contatti magnetici sono costituiti da due parti una il magnete, che a sua volta può essere polarizzato per evitare che una qualsiasi calamita possa "imbrogliare" l'altra parte, ovvero un contatto che si attiva in presenza di un campo magnetico . A loro volta i contatti magnetici possono assumere differenze nell'aspetto e nel loro utilizzo, sono in altre parole posti (il magnete sulla parte mobile, e il contatto su quella fissa) all'esterno fissati a parete, con viti poi protette contro la rimozione da tappi appositamente studiati, oppure all'interno di fori di diametro opportuno, tali da renderli completamente invisibili. Tutti i contatti magnetici utilizzano una linea antimanomissione o anti taglio cavi, non distinguibile una volta terminato il collegamento, perché tutti i fili hanno lo stesso colore e diametro. Per poterli riconoscere in fase di installazione, vengono pre-spelati i due fili del contatto, mentre gli altri due dell'anello antimanomissione sono lasciati coperti, e generalmente sono tutti di colore bianco. Esiste una regola dettata dalla logica più che da una Legge, ed è quella che stabilisce che ogni contatto sia esso riferito ad un dispositivo perimetrale che volumetrico, debba essere chiuso (quindi permettere il passaggio del segnale, o meglio della corrente) in posizione di riposo cioè quando si trova nello stato di attivato, pronto a rilevare la sua apertura, il taglio dei cavi, la mancanza di alimentazione elettrica ecc.. Quindi quando il magnete si trova nella posizione di porta chiusa, ad esempio, il circuito elettrico sarà chiuso. Per questo motivo nel caso vogliate collegare due o più contatti sulla medesima struttura, questi andranno collegati in serie tra loro,

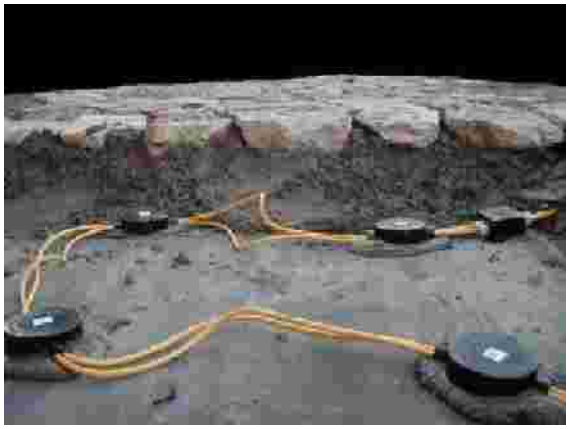
MAI in parallelo ! I contatti da incasso sono molto utilizzati nella protezione di persiane, infissi e porte, quelli da esterno su porte basculanti, box auto, serrande in genere . Vi sono poi contatti per utilizzi particolari, come quelli per rilevare il taglio del vetro, quelli che invece si attivano se cambiano inclinazione e quelli che utilizzati nell'epopea del Far West (si fa' per dire…) utilizzavano una striscia metallica o di carta stagnola incollata alle finestre, che se rotte, interrompevano il contatto e generavano l'allarme. Per fortuna sono state abbandonate data la facilità con la quale venivano bypassate se non addirittura scollate e lasciate integre ben in vista…È bene precisare che per rilevare la rottura vetri, i modelli a disposizione sono due, uno chiamato inerziale (nella foto) sente il colpo dato al vetro o la successiva caduta, l'altro più sofisticato sente le frequenze generate quando si passa un diamante sul vetro nel tentativo di tagliarlo ed è costituito da un microfono collegato ad un circuito apposito; A volte le due funzioni (inerziale e rumore) sono integrate in un unico dispositivo e a differenza dei contatti normali, questi dispositivi necessitano oltre che dei fili del contatto e antimanomissione, anche di quelli per alimentare i circuiti elettronici interni. Come già detto nel paragrafo riferito ai rilevatori ad ultrasuoni, quando si vogliono rilevare rumori, frequenze, suoni ecc… si deve prestare particolare attenzione ai dispositivi utilizzati e alla qualità degli stessi. Un prodotto economico spesso, rileva anche suoni che non dovrebbe, come il passaggio di un camion, il fischio del vigile, un temporale e così via.

Sensore rottura vetro

Contatti da incasso

Fin qui siamo rimasti incollati alle pareti domestiche, ma se vogliamo anticipare il malintenzionato e fermarlo prima che arrivi vicino alla nostra porta, ecco che la tecnologia offre moltissime opportunità, tutte molto efficaci . Parliamo delle cosiddette barriere, di tubi interrati nel giardino, di controllo sulle recinzioni, e sistemi contro il furto dei veicoli nei parcheggi.

Impianto antintrusione di tipo invisibile realizzato con rivelatori GEOSISMICI interrati nel sottosuolo in grado di percepire le onde sismiche che si propagano nel terreno,al passaggio di una persona in superficie. Questo impianto può essere posato sotto superfici a prato,ghiaia,asfalto e autobloccanti. I segnali rilevati vengono poi inviati a una potente scheda di elaborazione che in base alla necessità può discriminare o allarmare la CPU dell'impianto di allarme. Questo sistema permette di dividere il perimetrale esterno in più tratte quindi sapere e monitorare dove l'intruso ha tentato l'avvicinamento all'abitazione.



Impianto antintrusione di tipo invisibile per qualsiasi tipo di pavimentazione. Il sistema e costituito da sensori di PRESSIONE integrati nel cemento tra la soletta e il massetto. I sensori grazie alla costruzione monolitica dell'involucro percepiscono anche il più lieve dei passi e inviano alla scheda di elaborazione dei segnali che verranno discriminati o trasformati in allarme a seconda della condizione. I sensori in allarme manderanno inoltre un segnale al web server di videosorveglianza il quale sposterà le telecamere motorizzate nella zona interessata per monitorare e registrare tutti i movimenti esterni

Nella foto un impianto antintrusione su recinzioni a maglie interlacciate o elettrosaldate. Questo sistema permette di essere sempre protetti poiché l'impianto può essere inserito 24/24 h. La tecnologia piezodinamica insieme ad una potente scheda di elaborazione permette a questo sistema di allarmare l'impianto per scavalcamento,taglio e sfondamento della rete

{ PAGE **}**

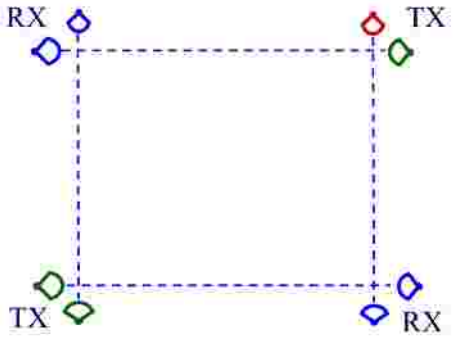
Un sistema antintrusione su recinzioni rigide (grigliati). Sistema simile a quello sopraindicato ci permette di essere sempre protetti poiché l'impianto è sempre inserito. I sensori utilizzati per questo impianto grazie ad una scheda di elaborazione dati sentono tutte le minime flessioni e torsioni dei pali di sostegno della cinta allarmando l'impianto per scavalcamento e sfondamento.

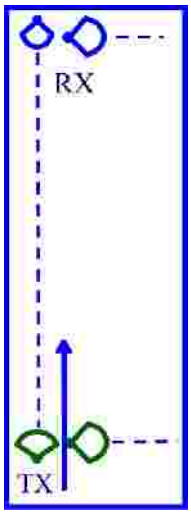
Negli anni ’70 i primi sistemi utilizzavano un tubo riempito d’olio, posto intorno all’intera area da proteggere e con un sensore di pressione (un vero e proprio pressostato) veniva misurata la differenza di pressione che veniva esercitata dal passaggio di una persona sopra di esso. Quello che mi stupì è che un simile impianto lo avevo realizzato in un piazzale di una ditta di trasporti, dove si voleva impedire il furto dei TIR, una volta piazzato il tubo, tutto veniva coperto da cemento armato, e con grande stupore (era la prima volta che lo utilizzavo, ed era il primo impianto del genere in Italia), notavo come anche solo il passaggio di un cane determinava la segnalazione in centrale. Questo per farvi notare come anche camminando su cemento armato , comunque la Terra si muove, ogni vostro passo muove enormi quantità di energia e di terreno compensate – per fortuna- dall’elasticità del nostro Globo. Evidentemente le tecnologie attuali possono discriminare le segnalazioni inviate dai sensori, così da permettere la protezione con sistemi interrati anche in

quelle ville dove oltre al cartello “ Attenti al cane”, il cane è anche presente e libero di circolare senza far entrare in funzione allarmi ingiustificati. Poiché è risaputo che mentre i cani possono venire avvelenati o comunque neutralizzati, i Nani da circo o bambini spesso utilizzati come apripista al contrario potrebbero cercare di eludere questi sistemi. Quindi dato che il cane non necessariamente per fare il suo lavoro deve essere di grossa taglia, è bene evitare di avere un vitellone, meglio restare sotto i 15 Kg. così che tarando l’impianto per rilevare pesi a partire dai 20 chili potete stare tranquilli che anche nani e bambini avranno una certa difficoltà ad eludere il sistema. Se poi volete eccedere (mai nella sicurezza è troppo!) potete integrare il sistema interrato con le barriere da esterno e/o con sistemi di videosorveglianza. A questo proposito segnalo che anche una telecamera è in grado di segnalare in modo automatico il passaggio di una persona, semplicemente utilizzando una tecnica che confronta le immagini, e se queste variano allora significa che qualcuno o qualcosa è entrato nell’area dell’obiettivo. Ma di questo argomento vi rimando alla sezione dedicata.

♦BARRIERE DA ESTERNO:

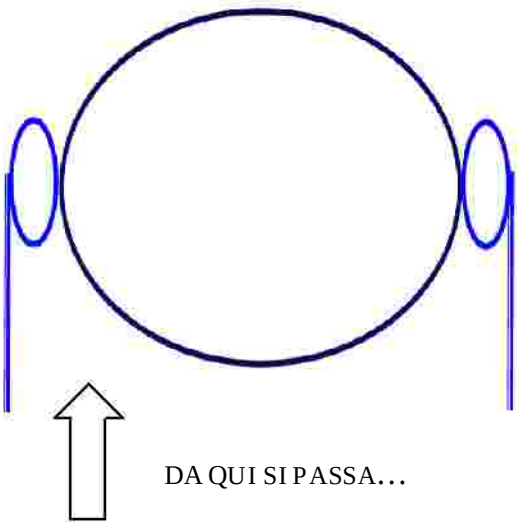
Veniamo ora alla protezione perimetrale che utilizza le cosiddette barriere. Possono essere ad infrarossi o microonde oppure miste. Intanto precisiamo che nel posizionarle devono essere rispettate alcune regole che eviteranno falsi allarmi, e "buchi" che ne permettano la penetrazione. Nel disegno qui a fianco, potete vedere che le barriere vanno posizionate incrociate, in modo che nessuno possa attraversarle senza venire rilevato, inoltre i trasmettitori (TX) vanno vicini così come i ricevitori (RX), per evitare che la ricezione di uno interferisca con la ricezione di un altro o viceversa che un trasmettitore possa interferire con un ricevitore posto nelle vicinanze. Disponendo le barriere come nel disegno in basso, si può notare che tra i due trasmettitori, e anche tra i ricevitori rimane un passaggio, segnalato dalla freccia, che permette di superare la barriera senza che questa possa intervenire. Nelle barriere esistono poi due tipologie di copertura: una formata da raggi lineari l'altra da fasci impenetrabili, ma che come è possibile veder nel disegno lasciano una zona scoperta nelle vicinanze del trasmettitore e del ricevitore, che se anche è vero che sono invisibili, non garantiscono la certezza di inviolabilità.





È meglio quindi preferire le barriere a raggi lineari (tipicamente quelle ad infrarossi), mentre quelle a fascio come le microonde e (non sia mai!) quelle ad infrasuoni sono adatte quando lo scopo non è quello di impedire un ingresso, ma l'uscita. Un esempio è quello di un area dove impedire il furto di automezzi o

l'asportazione di beni. Quando invece, è necessario impedire l'accesso a persone da porte, finestre, balconi, ponteggi (vedi apposito capitolo) ecco che le barriere ad infrarossi, che utilizzano i raggi lineari sono gli unici possibili. I raggi possono variare da due fino ad arrivare a 20 e più. Per evitare falsi allarmi dovuti al passaggio di un animale, viene fatto in modo che il raggio posto più in basso , se interrotto da solo, non generi un allarme, e questo ovviamente vale per i giardini e non per le finestre o i balconi. Lo stesso principio si utilizza per gli altri raggi; quando uno solo viene interrotto non viene generato un allarme, perché potrebbe trattarsi di un volatile , difficilmente una persona riuscirebbe nell'intento. A tal proposito vorrei sottolineare che nonostante la fantasia (e la fantascienza) di alcuni registi cinematografici, la possibilità di visualizzare i raggi (infrarossi) non è così remota, ma anzi con gli opportuni mezzi



possibile! Quindi rimanendo a quanto esposto prima, circa il valore del bene da proteggere e la possibilità che questo induca alcuni ad investire in costose apparecchiature e mezzi, si deve tenere ben presente non tanto il numero dei raggi o la distanza tra di loro, in quanto questo è più che sicuro e dà ottime garanzie, quanto all'altezza coperta dal raggio posto più in alto, in sostanza, l'altezza che deve avere la barriera per impedire che possa venire scavalcata con una sorta di ponte mobile, o dal solito circense campione di salto con l'asta…Tralasciando quella che potrebbe essere la sceneggiatura di un film, si può pensare di unire le diverse tecnologie per assicurarsi che nessuna falla permetta l'accesso, quindi non è da escludere che oltre alle barriere si possa dotare l'intero sistema anche della protezione interrata, così che per il malintenzionato diventi una corsa agli ostacoli dove il traguardo non deve mai essere raggiunto!
Terminata la divulgazione teorica, passiamo a quella pratica: Tutte le barriere da esterno sono costruite per resistere agli agenti atmosferici, alle alte e basse temperature e posseggono protezioni proprie contro l'apertura, la rimozione e il taglio dei cavi. Quello che invece non tutte hanno sono i cosiddetti dispositivi a prova di esperto..quelli cioè che impediscano di deviare i raggi con gli specchi (anti accecamento) e quelli che impediscano ad un trasmettitore portatile di accorciare la barriera sino a ridurla a pochi metri (anti offuscamento). Quest'ultimo sistema è nuovo ma sappiamo tutti quanto sia veloce l'ingegno e consiste nel presentarsi sul posto protetto dopo averlo accuratamente studiato, con un trasmettitore ad infrarossi identico a quello installato, che viene posto tra il trasmettitore originale e l'analogo ricevitore solo che la distanza tra loro viene accorciata, così che rimanga scoperta la parte rimanente. Per impedire questo, gli apparati sono dotati di un dispositivo che utilizza diversi canali di trasmissione, diverse frequenze, e nei casi più "alti" un segnale digitale codificato che associ TX e RX in modo univoco, impedendo falsi allarmi e soprattutto che altri apparati possano sostituirsi all'originale. Per questo motivo sia i trasmettitori che i ricevitori visti esternamente sono identici, così da rendere difficoltosa l'individuazione di uno o dell'altro, ma si possono

individuare solamente aprendo una scatola di derivazione, un pozzetto ecc, dove si possono contare i fili (o i cavi) che nel trasmettitore sono sempre in numero inferiore! Sembrerò ripetitivo, ma tutto quello che concerne un impianto atto a proteggere beni di varia natura, deve trovarsi sempre all'interno dell'area protetta. Inoltre tutte le barriere sono prive di qualsiasi segnalazione ottica, presente invece su tutti i rivelatori volumetrici, anche questo per evitare appunto possibili aiuti a chi vuole introdursi senza essere stato invitato.


Piccola barriera a fascio

Qui a lato una fotografia di una barriera a microonde che rende evidente quanto appena detto; Le dimensioni inducono a pensare che utilizzi un solo fascio, e l'altezza dal suolo oltre a permettere il passaggio raso muro di chiunque mi porta ad indicarla come un pessimo esempio di installazione. Probabilmente lo scopo di questa barriera sarà quello di proteggere il perimetro da un ingresso di automezzi e in ogni caso non da persone. Per impedire , o meglio per segnalare il tentativo d'ingresso da balconi o finestre si utilizzano barriere a infrarossi con un numero di raggi che vanno da tre a otto e vengono disposte fissate a muro sui due lati verticali. La distanza che intercorre tra il balcone e l'ingresso in abitazione, è quasi sempre irrisoria, quindi l'allarme deve scattare immediatamente e fare più rumore possibile, per spingere alla fuga l'acrobata del furto. In questo caso la barriera deve assolutamente essere di ottima qualità, perché un falso allarme sarebbe bene evitarlo per voi e per i vostri vicini..Spesso si adotta una piccola ma efficace accortezza: si fissa una telecamera finta (identica all'originale, impossibile distinguere la differenza, solo che dentro è vuota!) posta ben in vista rivolta verso il balcone o la finestra protetta, e

questo spesso induce a evitare un tentativo, passando al balcone successivo .

A lato un esempio di barriere per interni poste a protezione degli ingressi e delle finestre. A differenza delle barriere esterne, quelle per gli interni possono essere provviste di segnalazioni ottiche, oltre che avere dimensioni minori, e un design che ben si adatta all'arredamento. Chi deve acquistare una nuova casa, o che intende restaurarne una, farebbe bene a prevedere un impianto anti intrusione predisponendo sotto traccia tubazioni e canaline atte a contenere i cavi che andranno a collegare tutti i dispositivi, quindi anche all'interno dei cassoni di tapparelle, persiane, così come a ridosso delle porte e finestre cercando di NON utilizzare le tubazioni esistenti che contengono i fili dell'impianto elettrico. In via eccezionale possono essere utilizzate solo quelle che contengono i cavi coassiali TV, poiché questi non interferiscono in alcun modo con i segnali dei rivelatori, mentre questo non è garantito per i collegamenti telefonici ed elettrici. Per concludere consiglio di abbinare l'impianto ad un dispositivo UPS, una sorta di gruppo elettrogeno casalingo, molto utilizzato in abbinamento con i computer domestici, che svolge due funzioni molto utili: quella di proteggere l'impianto da sovratensioni, fulmini ecc, e l'altra quella di mantenere alimentato l'impianto anche in mancanza della tensione di rete, per un tempo breve, ma utile poiché aggiunge tempo al tempo, allungando la vita delle batterie .

PONTEGGI E IMPALCATURE:

L'utilizzo di impalcature o ponteggi utilizzati per il rifacimento di facciate o manutenzione nei condomini, comporta inevitabilmente il rischi di un intrusione "riservata ai primi piani" anche sui piani più alti, ovvero all'intero condominio. Nel proteggere un ponteggio si devono impedire due cose: la possibilità che si possa salire esternamente fino a raggiungere un qualsiasi appartamento, e la possibilità di utilizzare un appartamento posto all'interno del perimetro costituito dal ponteggio, per raggiungere altri appartamenti dello stesso complesso. Si dovranno installare barriere esterne e rilevatori interni che dovranno intercettare il camminamento, e nello stesso tempo non impedire agli inquilini di muoversi liberamente anche sui propri balconi o finestre.

Qui a lato un immagine di una barriera ad infrarossi posta all'esterno del ponteggio per impedire la risalita verticale.

Le barriere utilizzate hanno una portata media di 25/30 metri. Ma per proteggere lunghi tratti vengono utilizzate anche quelle con portate superiori e che si servono dell'ausilio di specchi che permettono ai raggi di seguire e superare gli angoli e nella pratica

devono impedire che rimangano scoperti in particolare il primo piano raggiungibile dalla strada, quindi la possibilità di arrampicarsi, e subito dopo con barriere anche ogni piano all'interno per rivelarne il camminamento. Vengono utilizzati anche dispositivi a infrarossi o microonde non a barriera ma a fascio, per coprire zone interne, poco raggiungibili dalla linea virtuale della barriera, balconi o terrazzi che non si riescono a proteggere con il sistema formato di barriere. In questo caso si deve prestare molta attenzione, poiché utilizzare rivelatori di quel tipo all'esterno, potrebbero generare falsi allarmi dovuti alla presenza di volatili, vento ecc… In genere escludendo le barriere, tutti gli altri rilevatori vengono collegati ad una scheda discriminante, in grado di contare gli impulsi, e la loro durata. Se è un volatile, l'allarme non scatta, negli altri casi sì. Riassumendo deve essere protetto il perimetro orizzontale più basso e più alto (salita dalla strada e discesa dai tetti), si devono proteggere tutti i piani dal possibile passaggio all'interno dei ponteggi stessi, anche per evitare che qualcuno possa uscire dalla propria abitazione per andare a "visitarne " un'altra. Gli antifurto per ponteggi, generalmente vengono noleggiati e dispongono di una centrale munita di orologio che provvede ad attivare e disattivare l'impianto automaticamente. Oltre ad essere munito della sirena, spesso viene munito di combinatore telefonico, soprattutto nei casi in cui, anziché un condominio, il ponteggio sia montato intorno ad un museo, o comunque un luogo non abitato. Non ho molto altro da aggiungere, se non che nei ponteggi molte volte si tende a coprirli contro la polvere da vere e proprie tende, che con il vento creano parecchi problemi alle barriere, e che trovandosi all'esterno queste sono sottoposte ad ogni più impensabile tipologia di falso allarme. Per questo l'unica raccomandazione è quella di eseguire l'impianto come si suol dire: a regola d'arte!

DISPOSITIVI VOLUMETRICI:

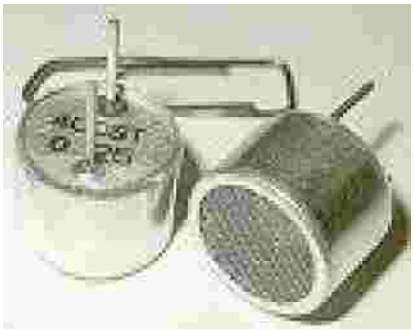
♦**SENSORI AD ULTRASUONI:**

Negli anni ’70 gli antifurto iniziavano lentamente ad invadere il mercato, erano ingombranti, facili da manomettere e davano numerosissimi falsi allarmi, dovuti principalmente all’instabilità dei sensori e alla tipologia utilizzata per il rilevamento.

Primi tra tutti i dispositivi che utilizzavano gli ultrasuoni. Gli ultrasuoni sono adatti in ambienti perfettamente chiusi, sigillati, che non hanno al loro interno oggetti o pareti di piccolo spessore, privi di vetri finestre, e non ultimo, che non “contengano” animali domestici.

Questo perché gli ultrasuoni per funzionare egregiamente devono poter saturare l’ambiente, le frequenze utilizzate inducono spesso oggetti di piccole dimensioni ad entrare in “risonanza” (effetto diapason), a vibrare, inoltre gli ultrasuoni sono generati in modo casuale anche da elettrodomestici, autovetture, temporali, fischi ecc.. Per questo motivo sono stati abbandonati e sostituiti con rilevatori ad infrarossi o microonde. Il sistema funzionava in questo modo, un trasmettitore irradiava gli ultrasuoni, un ricevitore leggeva la frequenza e soprattutto il tempo che questi impiegavano rimbalzando sulle pareti a tornare indietro. Qualsiasi movimento, anche minimo all’interno di quell’area, determinava un ritardo, o una variazione delle frequenze e di conseguenza intervenire l’allarme. Le uniche utilizzazioni ancora, anzi a volte uniche, possibili dove utilizzare gli ultrasuoni sono gli interni di casseforti, caveau, celle frigorifere (gli ultrasuoni sono insensibili ai cambi di temperatura) oppure anche se a mio giudizio erroneamente, all’interno delle automobili. Infatti, le auto non sono a < chiusura stagna >, hanno finestrini sottili, sono esposte a rumori ambientali, sentono i tuoni e gli ultrasuoni provenienti da fonti esterne, possono far vibrare i finestrini inducendo un effetto tale da far scattare un falso allarme. Si deve solo all’alta tecnologia di oggi il limitato intervento di falsi allarmi, utilizzando un sistema che filtra gli ultrasuoni che annulla i piccoli movimenti o che non abbiano la stessa identica frequenza di quella trasmessa dall’apparato in questione. La tecnologia

ultrasonica però è utilizzata egregiamente per rilevare il taglio o la rottura di vetri, finestre, dato che questa operazione genera ultrasuoni. In questo caso è utilizzato un microfono atto a rilevare le frequenze generate da un oggetto che taglia il vetro, sono sensibilissimi, ma non possono comunque garantire il risultato, poiché se una finestra viene aperta completamente agendo sulle guarnizioni o sulle cerniere che la tengono fissata, oppure se anziché utilizzare un diamante per il taglio, utilizzo una fiamma ossidrica per fondere il vetro, ecco che il microfono ultrasonico non percepirà alcuna frequenza sospetta. In ultimo se consideriamo che un trasmettitore ad ultrasuoni, anche se di debole potenza e che lavora su frequenze lontane anche per gli animali dalla soglia d'udibilità, col procedere può danneggiare l'udito, elevare le temperature di liquidi ecc.. Per tutti questi motivi, personalmente non utilizzerei gli ultrasuoni in nessun caso, e forse, è proprio per questo che ormai simili antifurto si trovano solo nei musei della tecnica.



♦**SENSORI AD INFRAROSSI:**

Questi apparati rilevano variazioni brusche di temperatura all'interno di ambienti non molto grandi, meglio evitare di superare gli 8 10 metri di lato, perché pur esistendo apparati che giungono fino a 30 metri di rilevazione, nel caso degli infrarossi il rischio di falsi allarmi diventa possibile.

Gli infrarossi non sono sensibili ai movimenti di piccoli insetti, ai movimenti al di fuori del campo di lettura anche di persone, alle lente variazioni di temperatura dovute al normale riscaldamento ambientale, e non sono disturbati da interferenze radio o magnetiche. Sono quindi indicati a proteggere piccoli locali, anche con finestre aperte, corridoi ingressi ecc. .Il principio di funzionamento è quello di inviare alcuni raggi infrarossi, che in parole povere hanno una temperatura[1], e di leggere il raggio che viene riflesso e ritorna. Se la temperatura ricevuta è uguale a quella trasmessa non ci sono allarmi, altrimenti si avvia la segnalazione.

Per questo motivo, un dispositivo ad infrarossi non rileva il movimento di una tenda mossa dal vento, mentre potrebbe rilevare la diversa temperatura della corrente d'aria rispetto a quella interna.

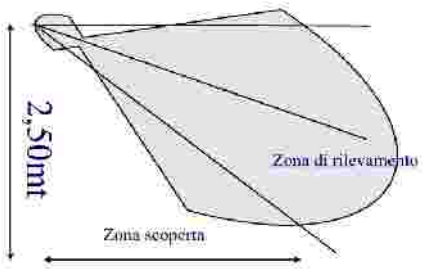
Come vedremo nessun dispositivo va' indirizzato verso finestre, termosifoni o elettrodomestici che potrebbero attivarsi in maniera autonoma (frigoriferi, scaldabagni). Esistono diversi tipi di rilevatori ad infrarossi, quelli **passivi** quelli **attivi** e quelli a **barriera** . Quelli a barriera sono descritti nel capitolo dedicato alle protezioni perimetrali.

INFRAROSSO

Attivi sono quelli che inviano un segnale, un raggio infrarosso (per la verità i raggi sono molti di più, ma il principio non cambia) e rileva quindi la differenza di temperatura tra raggio trasmesso e ricevuto. Alla presenza di movimenti si determina una variazione di temperatura, ma anche una variazione del tempo necessario al raggio trasmesso a tornare ed essere ricevuto. Tutti i dispositivi una volta alimentati iniziano a funzionare dopo un tempo di "riscaldamento" che permette all'apparato di saturare l'ambiente e adattarsi alle caratteristiche che da quel momento, se

variate, ne determinano l'entrata in funzione e quindi l'invio di un segnale d'allarme.
Passivi sono quei dispositivi che si "limitano" a misurare la temperatura ambientale e le sue variazioni nel tempo ,quindi sono atti a rilevare il movimento di un qualsiasi corpo che emetta infrarossi in quantità superiore all'ambiente in cui è inserito . La scelta tra le due tipologie di sensori infrarosso non deve essere puramente di tipo economico, poiché quelli attivi costano leggermente di più, ma valutando le seguenti considerazioni: La prima risponde alla seguente domanda: L'ambiente che devo proteggere contiene valori tali da invogliare professionisti a tentare il furto pur consapevoli dei rischi dovuti alla presenza di impianto adeguato?
La seconda, potrebbe il professionista (del crimine) ricorrere a mezzi quali ad esempio tute che rendono la temperatura corporea uguale a quelle ambientali, fiamme ossidriche, dispositivi elettronici tipici del mestiere ecc..? Se le due risposte sono entrambe positive, allora l'utilizzo dei rilevatori attivi è d'obbligo, altrimenti entrambi i dispositivi andranno bene e risolveranno in ogni caso lo scopo per il quale sono stati concepiti. Questo perché quelli attivi oltre a misurare la temperatura, misurano anche il tempo dei raggi che tornano al dispositivo che li ha inviati, determinano la differenza di angolazione di ogni singolo raggio (in questo caso anche una tenda mossa dal vento, può determinare un allarme), quindi una persona che pur indossando una tuta in grado di mantenere la temperatura del corpo rilevata uguale a quella dell'ambiente, non riuscirebbe ad impedire un ritardo o una variazione di angolatura del raggio trasmesso e poi ricevuto dal sensore. Il ricevitore passivo, invece misura solo variazioni di temperatura in ogni caso più che sufficiente allo scopo. Non è un caso che solo nei film di James Bond esistono tute del genere e che quelle a disposizione della NASA oltre a costare probabilmente più dei valori che volete proteggere, siano di difficile reperibilità. Nella fase di installazione dei dispositivi ad infrarossi si deve tenere conto di diversi fattori. Innanzitutto devono essere montati ad un'altezza compresa tra i due e tre metri dal suolo, meglio se non raggiungibili facilmente per evitare che

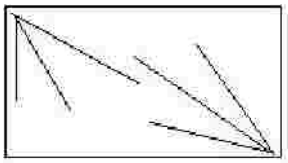
qualcuno li possa girare verso zone sicuramente non raggiungibili dal passaggio dell'intruso, poi devono essere orientati verso la direzione più probabile di provenienza, generalmente porte o finestre ed infine avere il collegamento antimanomissione sempre attivato. Alcuni dispositivi hanno anche la possibilità di inibirne il funzionamento in modo tale che il dispositivo non lavori inutilmente durante il periodo di inattività, cioè, quando l'impianto d'allarme è spento o disattivato. Generalmente a questo provvede la centralina, purché il dispositivo abbia l'apposito comando previsto allo scopo. Questo comando è separato, e negli impianti di un certo livello è gestibile direttamente dalla centralina con apposite funzioni, perché così è possibile abilitare il dispositivo anche a impianto disattivato, e valendosi delle spie Led sempre presenti sui sensori, è possibile verificare l'area di copertura dello stesso, muovendosi in più direzioni e verificando l'effettiva rilevazione del dispositivo.



Esistono varianti, sinceramente poco interessanti quale ad esempio la possibilità di inibire la funzione dei Led del dispositivo anche ad impianto inserito, per non mettere il malintenzionato in allarme, e forse, poterlo catturare in flagranza… giudicate Voi se sia il caso di utilizzarlo o meno, tenendo presente che non funzionando la segnalazione non potete sapere se funziona il dispositivo e con il tempo si tende ad entrare in uno stato d'ansia che vi spingerà ad inserire l'impianto e provarlo facendo scattare l'allarme, con tutto quello che ne consegue.
(Ricordate la favola …al lupo, al lupo…?) I cavi che alimentano i dispositivi devono essere nascosti, non raggiungibili primo per una questione estetica, poi perché pur essendo autonomamente

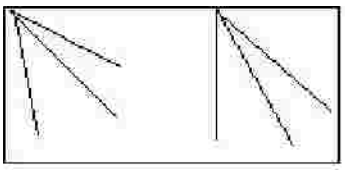
protetti (un taglio dei cavi, un ponticello ecc.. determina l'allarme immediato, anche ad impianto spento)è sempre meglio evitare di invogliare qualcuno a tentare di provarci. Tutto è relativo, nel senso che se i valori da proteggere sono tali da determinare un alto rischio di tentato furto, ogni facilitazione per il malintenzionato aumenta il rischio che questi , ad esempio un esperto di impianti antifurto, forse lo stesso installatore, conosca le procedure per rendere inoffensivo l'impianto. Ed è per questo motivo che negli impianti di un certo livello si predilige affidare la posa dei cavi ad una Ditta, mentre le apparecchiature e gli impianti sono fatti eseguire ad un'altra impresa, in modo da evitare che un solo soggetto conosca tutto l'impianto. Questo vale per grossi valori da proteggere, per le abitazioni una sola Ditta installatrice è più che sicura, in ogni caso è lo stesso impianto che si protegge da solo, dandovi la possibilità di cambiare password, distinguendo l'intervento tecnico da quello normale e via dicendo. Tutto questo per ribadire un concetto basilare: in un impianto che deve proteggere la vostra vita e i vostri beni scegliete una ditta installatrice che offra garanzie, non improvvisate, non affidatevi ad amici o parenti, non risparmiate più del dovuto. Un impianto eseguito a regola d'arte, si installa una volta sola e vi protegge per sempre.

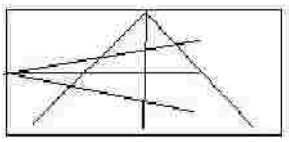
Nell'immagine qui a sinistra è illustrata la disposizione tipica di un sensore posto a due metri e 50 dal suolo, con le zone coperte e scoperte dal sistema di rilevazione. L'inclinazione verso il basso copre l'area più vicina, ma diminuisce la distanza e quindi la portata del dispositivo. Tutti gli apparati contengono al loro interno le indicazioni utili al montaggio, con le distanze di copertura, l'inclinazione e l'altezza ottimale.
I sensori vanno sempre installati nella direzione opposta a quella di un possibile ingresso, diretto verso l'ingresso stesso,e mai invece, verso l'area da proteggere (una cassaforte ad esempio), questo per rilevare immediatamente l'intrusione. Nei locali di certe dimensioni si possono prevedere più sensori, ma questi devono essere disposti in modo tale da non rilevarsi a vicenda, mai uno di fronte all'altro, piuttosto incrociati o disposti a cascata.



Non disporre i sensori come indicato qui a sinistra, potrebbero rilevarsi a vicenda innescando una catena infinita di falsi allarmi.

A destra è indicato un esempio di cascata, sensori disposti a rilevarsi a coprono l'area senza sotto a vicenda , oppure più disposti sinistra vengono incrociati ottenendo lo stesso effetto della disposizione a cascata.





In questo modo è possibile aumentare l'area di copertura utilizzando più dispositivi, oppure utilizzandone uno solo ma di portata maggiore evitando però di utilizzare dispositivi ad infrarossi per distanze superiori ai 20-25 metri. Per coprire distanze maggiori meglio ricorrere ai rilevatori a microonde.

[1] Leggere apposito capitolo.

♦**SENSORI A MICROONDE:**

L'utilizzo di sensori a microonde si rende necessario, quando è richiesta una maggiore velocità e sensibilità nel rilevamento, quando le distanze da coprire sono maggiori e sono meglio indicati in tutti quei casi in cui gli spazi sono ristretti, come nei corridoi, nei locali dove sono possibili variazioni brusche di temperatura (locali caldaia), o dove al contrario la temperatura è bassa, come ad esempio in una cella frigorifera. Come tutti i dispositivi elettronici le temperature di esercizio hanno restrizioni e trovare dispositivi che possono lavorare a 30 gradi sotto zero non è facile, l'esempio era puramente indicativo. Nei casi limite esistono naturalmente apparati in grado di funzionare in tali condizioni, ma devono essere richiesti espressamente. Per proteggere una cella frigorifera è più semplice ed economico proteggere l'ingresso con dispositivi perimetrali(vedi) oppure con sensori posti all'esterno della cella puntati in modo da rilevare il tentativo di aprire la porta della cella . Se, esiste la possibilità che qualcuno possa entrare in quella cella perforando pareti, pavimenti meglio ricorrere ai dispositivi descritti in seguito relativi alle protezioni dei caveau e alle casseforti. Come nei dispositivi ad infrarossi, gli apparati a microonde utilizzano la medesima tipologia di rilevamento, inviano onde radio e ne misurano la frequenza, il tempo e ogni altra variazione tra quella inviata e quella ricevuta. Sono molto più soggetti a falsi allarmi, poiché qualsiasi movimento, anche impercettibile, all'interno dell'area coperta viene sicuramente intercettato. Tutti i sensori hanno quindi, la possibilità di regolarne la sensibilità, la portata e in casi particolari, dispongono di selettori che consentono di programmare il numero dei rilevamenti minimo necessario prima di considerarli allarme ed inviare l'apposito comando alla centrale per gestirlo. Non si deve erroneamente pensare che il termine microonde sia per analogia associato ai forni che utilizzano la stessa tecnologia. Questi non

scaldano, non cuociono, non fanno scintille sui metalli, meglio associarli più semplicemente alle microonde utilizzate dai radar negli aeroporti; Quando sono accesi (o meglio abilitati dalla centrale), impiegano circa un minuto prima di rendersi operativi, tempo necessario a misurare il luogo che coprono con i loro raggi . Saturano l'ambiente ed è poi in pratica impossibile introdurre un oggetto o muoversi nell'area senza venire sorpresi dall'affidabile dispositivo. Dovendo evitare che qualche malaugurata mosca o zanzara muovendosi nell'area protetta, inneschi un allarme, i dispositivi a microonde sono tarati in modo tale che per considerare un allarme devono essere stati deviati almeno tre raggi contemporaneamente. In pratica l'apparato inizia ad allarmarsi quando rileva il passaggio di un criceto, mentre non segnala scarafaggi, formiche e simili. L'installazione è del tutto simile a quella appena vista per i dispositivi ad infrarossi, ma spesso trattando distanze maggiori le regolazioni di posizionamento, inclinazione e sensibilità andranno eseguite sul posto con prove di movimento, avvalendosi dei Led di segnalazione, posti come già detto, su tutti i dispositivi di rilevamento. Negli apparati a microonde è possibile trovare più indicatori, oppure uno solo ma multicolore che segnalerà un rilevamento di movimento intercettato ma non considerato allarme (interrotti solo uno o due raggi anziché i tre previsti), un rilevamento intercettato considerato allarme, ma non inviato alla centrale (fase di test), una segnalazione di avvenuto allarme non rilevato dall'utilizzatore[2] (l'apparato è andato in allarme durante la vostra assenza, e dalla centrale non è arrivato il comando di allarme ricevuto) e naturalmente la segnalazione di allarme con relativa funzione di segnalazione acustica.

.

DISPOSITIVI ANTI TACCHEGGIO:

Vengono definiti dispositivi antitaccheggio tutti quei mezzi elettronici, meccanici e di sorveglianza atti ad impedire furti all'interno degli esercizi commerciali , segnalando l'uscita della merce non pagata. I sistemi più utilizzati sono principalmente due: Elettronici : inseriti all'interno di supporti plastici o celati sotto etichette di vario tipo – Meccanici : costituiti da più tradizionali catene, lucchetti o ingombranti contenitori la cui apertura richiede l'utilizzo di chiavi meccaniche particolari o dispositivi magnetici.

I dispositivi elettronici sono facilmente neutralizzabili, non solo rimuovendo l'etichetta o il supporto che li contiene, ma anche "coprendoli" con monete metalliche (andavano bene le vecchie 100 Lire), poiché il sistema utilizzato era (ed è) costituito da una bobina (un approfondimento tecnico è descritto nella sezione dedicata) che attraversando l'area di controllo genera uno sbilanciamento dei circuiti radio e la conseguente segnalazione visivo - sonora.

Proprio il fatto di essere costituito da una bobina passiva (non c'è alcuna batteria, o circuito elettronico) ed il sistema tipico dei circuiti radio utilizzato, che rende facilmente neutralizzabile l'intero sistema. Per questi motivi si tende ad inserire la parte "elettronica" in una parte meccanica aumentando così la difficoltà del malintenzionato, oppure utilizzando più etichette, ad esempio una visibile e facilmente asportabile, un'altra celata all'interno o in parti meno accessibili. È altresì ovvio che la

possibilità di inserire l'oggetto da asportare all'interno di un contenitore metallico ne inibisce ogni possibile rilevazione, e per evitare questo, gli oggetti più piccoli vengono messi all'interno di contenitori plastici di dimensioni difficilmente occultabili o, cosa ormai entrata nell'uso comune, vengono esposti oggetti inutilizzabili, finti, del tutto uguali all'oggetto da rappresentare ma privi di ogni parte funzionante che quindi permettono la visione e la possibile scelta nell'acquisto, ma l'inutile asportazione. Una volta deciso l'acquisto sarà il commesso a fornire l'acquirente di una ricevuta, questi si recherà alla cassa per il pagamento e una volta eseguito,torna dal commesso per il ritiro dell'oggetto. Nelle immagini qui a lato sono visibili a destra una piastra contenente la bobina e rimuovibile con un forte magnete polarizzato utilizzata principalmente nel settore abbigliamento, sotto, delle etichette contenenti la bobina generalmente fissate con adesivo e a sinistra, una etichetta adesiva dove viene evidenziata la "bobina" posta sotto l'etichetta stessa e che dimostra come anche solamente tagliando con una lametta l'etichetta senza asportarla sia sufficiente interrompere il circuito e rendere così inutile il tipo di protezione. La tecnologia utilizzata viene indicata con il nome RFID (che tradotto significa: Identificazione attraverso la Radio Frequenza) e quando utilizzata nelle versioni avanzate, permette l'invio in automatico di tutte le informazioni come il prezzo, il prodotto ecc..con l'intenzione di sostituire l'utilizzo dei codici a barre. Per il dettaglio tecnico si rimanda alla sezione dedicata.

DISPOSITIVI ANTI SEQUESTRO:

Anche se l'argomento potrebbe interessare pochi, e anche se questi pochi generalmente possiedono i mezzi economici che gli permettono una adeguata protezione, si deve poter prevedere che non sempre un sequestro è finalizzato alla richiesta di un riscatto, ma potrebbe generarsi da una tentata rapina andata male, da un tentativo di furto e non ultimo un errore di persona. Vi sono poi quei sequestri anomali, ad esempio quelli scaturiti in seguito ad un tentativo di stupro oppure quelli involontari, tipico l'esempio di un ladro che ruba un auto, non accorgendosi che all'interno si trovava un neonato addormentato (attenzione mamme! Potrebbe configurarsi il reato di abbandono di minore…). Il termine sequestro in realtà è un sinonimo di **rapimento**, infatti rapimento significa: Portare via con sé qualcuno o con inganno, mentre sequestro di persona significa: **rapire** una persona privandola della libertà a scopo di estorsione o riscatto. La sottile differenza determina una diversità notevole sia nella pena che subirà chi commette quel reato, sia nella sostanza in un caso non viene richiesto un riscatto, nell'altro sì. Nei casi di stupro, ben poco può fare la tecnologia, se non fornendo spray al peperoncino o corsi di difesa personale, ma non sempre i tempi di reazione si adeguano all'evento, poi c'è anche la possibilità di utilizzare una sorta di sirena tascabile molto potente, ma anche in questo caso si deve avere il tempo di azionarla; Chi invece pensa di essere soggetto ad un tentativo di rapimento, può dotarsi di numerosi apparati, li cito in ordine sparso: Conoscete quella sorta di trasmettitore radio che utilizzano gli sciatori, e che viene azionato in caso di valanga? Ecco quello potrebbe andare bene, ma ha una sola limitazione, quella che per poter essere localizzato deve trovarsi in un raggio di azione di 80 metri , si chiama ARVA e francamente non penso possa essere utile in questo caso. Molto più semplice l'utilizzo di trasmettitori GPS che inviano costantemente la propria posizione, anche loro con una

limitazione, il segnale satellitare non attraversa ostacoli come le grotte, le cantine, gli interni di qualsiasi abitazione, quindi potrebbe solamente rivelarsi utile per segnalare l'ultima posizione raggiunta prima di perdere il segnale. I telefoni cellulari (meglio se dispongono di GPS integrato) sono una manna dal cielo per le forze dell'ordine, che possono localizzarlo anche se vi trovate in ambienti chiusi, peccato però che spesso, o meglio sempre, chi vi sequestra la prima cosa che tende a fare, è proprio quella di privarvi del cellulare. Se non è persona esperta, lo fa' unicamente per impedirvi di usarlo per fare chiamate, quindi se lo lascia acceso e lo porta con sé la possibilità di rintracciarlo rimane inalterata, mentre se lo spegne….Per fortuna qualcuno a questo ha pensato, e quindi un analogo dispositivo molto più piccolo può agevolmente essere nascosto – di solito all'interno della cintura o legato ai polpacci - . In entrambi i casi il problema rimane quello delle batterie che devono costantemente essere caricate e scaricate per poter durare a lungo, e dato che un sequestro non è prevedibile spesso, si tende ad utilizzare questi apparati solo nei casi cosiddetti a rischio, lasciandoli nei cassetti per mesi. Con una richiesta di riscatto si preferisce munire di apparati elettronici il denaro stesso utilizzando delle banconote civetta, che contengono un trasmettitore interno, oppure utilizzando inchiostri invisibili (infrarossi o ultravioletti) che macchiano tutte le banconote e le mani di chi le utilizza, ma questo è più utile al dopo. Il pagamento del riscatto non sempre garantisce la liberazione dell'ostaggio, quindi più mezzi si utilizzano nella prevenzione e localizzazione più sarà veloce l'intervento delle forze dell'ordine. Il consiglio che posso dare è quello di utilizzare due telefoni cellulari, uno quello che utilizzate comunemente perfettamente funzionante, l'altro rigorosamente configurato su "silenzioso" cioè senza suoneria e vibrazione, meglio se piccolo così da essere facilmente occultabile. Il primo è quello che il sequestratore si aspetta di trovare (guai a nasconderlo, lo cercherebbe ovunque – denudandovi – trovando così anche l'altro), ed è quello che consegnerete. Se il trucco funziona l'altro potrà essere utilizzato per rintracciarvi e anche per fornire un ascolto ambientale di quello che accade intorno a voi. A tal proposito ricordatevi di

configurarlo in modo che accetti la risposta automatica, così che risponda al vostro posto e rimanga attivo sino a quando le batterie lo permetteranno. Quindi riassumendo, il telefono che utilizzerete come spia non deve avere: trasferimenti di chiamata – segreteria telefonica attiva – dispositivi bluetooth o wireless che potrebbero interfacciare un collegamento con i telefoni dei sequestratori e determinare un consumo maggiore della batteria – inoltre il numero telefonico deve essere a conoscenza solo delle persone vicinissime e fidatissime, in quanto la conoscenza di un secondo cellulare può arrivare anche ai sequestratori, che spesso sono molto vicini ai famigliari . Deve invece rispondere ai seguenti requisiti: Configurato per la risposta automatica dopo il primo squillo – meglio se dispone di GPS integrato – suoneria e vibrazione disabilitati – luminosità display a zero (pensate al buio vedere una calza illuminarsi…) ed in particolare trattatelo come se fosse il vostro normale odierno cellulare, la batteria sempre carica e non dimenticatelo sul comodino, sempre con sé ! Per finire segnalo alcuni dispositivi alla portata di pochi, veramente pochi, ma che è giusto sapere che esistono: Sono il massimo raggiunto dalla tecnologia, e sono celati all'interno di orologi o di cinture, così come nei tacchi delle scarpe e così via… Sono completi di tutto, dispositivo GPS, microfono per l'ascolto ambientale, alcuni anche di webcam davvero millimetriche, e sono quelli che danno maggiore libertà ai figli dei "ricchi", lasciandoli circolare senza la necessità di una guardia del corpo sempre con il fiato sulle spalle, e che comunque poco potrebbe fare davanti a una decina di uomini armati.

FURTO DELLE AUTOMOBILI :

Tralasciando il furto degli oggetti che si trovano all'interno di autoveicoli, già trattato, vediamo come prevenire quello del furto del veicolo; Le auto di piccola cilindrata spesso vengono rubate con il solo scopo di utilizzarle per commettere reati come le rapine e poi abbandonate, a volte anche solo per farsi un giro, non disponendo del biglietto per prendere la metropolitana, quelle di cilindrata più elevata invece, vengono rubate per essere rivendute o utilizzate all'estero. Il cosiddetto antifurto *IMMOBILIZER* quello cioè che ormai viene fornito di serie con l'auto e consiste nel bloccare la pompa di benzina ed i circuiti elettrici se non viene disattivato dalla sua chiave, garantisce quanto basta dal delinquentello di passaggio ma non da un professionista . Basti pensare che in alcuni casi si utilizza un carro attrezzi, si porta via l'auto e poi all'interno di un officina "amica" si provvede a disattivarlo. Per disattivarlo ci sono due semplici sistemi, il primo utilizza la tecnica della sostituzione della chiave con un'altra cambiando il ricevitore con uno "pulito", l'altra smontando completamente il dispositivo e ricollegando il tutto come se l'auto fosse uscita dalla fabbrica senza antifurto. Quindi rimane l'antifurto satellitare che se abbinato ad un cellulare provvede a fare tutto quello che è necessario, inviare l'allarme via sms, fornire la posizione dell'auto ecc..Peccato però che l'utilizzo di segnali provenienti da satelliti richieda la visibilità tra l'antenna e il satellite. Ecco che il ladro astuto provvede a coprire l'antenna ricevitrice GPS e via…L'unico sistema per ovviare a questo è quello di munire l'auto di un antenna civetta, quella che il ladro si aspetta di trovare, fissata all'interno sul cruscotto ma collegata al nulla. Quando il ladro taglierà il cavo penserà di aver risolto il problema, mentre non sa che voi avete messo la vera antenna dentro lo specchietto retrovisore (quelli esterni), oppure in un posto difficilmente individuabile, ma comunque sempre a portata ottica con il satellite. Lo stesso vale per la scheda che gestisce il tutto, e che è provvista anche della sim del telefono cellulare. Fatela montare in una posizione assurda, scomoda, irraggiungibile, in modo che il tempo necessario a scovarla sia

sufficiente a permettere al dispositivo di inviare quanti più dati riesce a dare. Non dimenticate di dotarlo di batteria tampone ricaricabile, così che – e spesso accade – se il ladro dovesse scollegare la batteria dell'auto, l'invio dei dati possa proseguire.

SCIPPI E BORSEGGI:

Una attività dura a morire è quella che svolgono impavidi delinquenti da strada: scippare quasi sempre persone anziane con il classico sistema che consiste nell'affiancare con un motorino la vittima prescelta, afferrare la borsetta e via, uno strattone e poi la fuga. Quasi sempre finisce con il ferimento della persona scippata, a volte le ferite riportate nella caduta possono portare alla morte. Il borseggio, invece, se da un punto di vista, non genera ferimenti, e quindi è meno violento (purtroppo anche per il codice penale), dall'altra crea enormi difficoltà a chi lo subisce, perché non se ne accorge immediatamente, rischia di perdere documenti con tutte

le conseguenze del caso, non ha la possibilità di reagire e quindi (tentare) fermare il borseggiatore. La tecnica utilizzata in questi casi si avvale spesso di più persone ognuna delle quali ha un compito ben preciso: distrarre la vittima, fare da palo, eseguire materialmente il furto. I luoghi di "lavoro" sono quasi sempre quelli più affollati, mezzi pubblici, manifestazioni, concerti, fiere, ma non si deve sottovalutare anche il singolo, autodidatta, così come l'utilizzo di bambini che vi seguono ed eseguono il furto mentre camminate, incuranti della probabilità di essere visti o scoperti. Per proteggersi dal borseggio esistono dispositivi molto efficaci e si dividono in due categorie: quelli contro l'apertura e quelli contro lo strappo. Contro l'apertura (di borse, portafogli, valigie), sono costituiti da una sirena tascabile potentissima, che si attiva appena si tenta di aprire l'oggetto protetto e possono essere formati da una catenella collegata al sensore (la più sicura), oppure da un sensore che vede la variazione di luce (più indicata all'interno di

valigie). La catenella può essere fissata sulla parte apribile della borsetta, o direttamente al portafoglio. Appena si tenta di “tirarlo” o di aprire la borsetta interviene la sirena, che sicuramente mette in fuga il ladro, ed impedisce che riesca ad appropriarsi delle vostre cose. I dispositivi a strappo, invece si adattano oltre che alla protezione dei borseggi, anche a quella dello scippo; In questo caso la catenella è fissata all’esterno del bene da proteggere, generalmente alla cintura , e in caso di strappo dovute allo scippo o al borseggio, impedisce la caduta, perché la catena si sgancia automaticamente, ma genera un allarme sonoro che segue l’oggetto sottratto, sino a quando – nel caso di una borsetta – lo scippatore non riesca ad aprirla, trovare il dispositivo, cercare di gettarlo (molto difficile se è stato fissato), e quindi proseguire la sua fuga. Pur non impedendo quindi lo scippo, si può prevedere che nella difficoltà di eliminare l’allarme, il ladruncolo si appropri in tutta fretta dei soldi, e abbandoni la borsetta al più presto. A tal proposito, sarebbe bene prendere l’abitudine di portarsi dietro le fotocopie dei documenti, tenendo gli originali in casa. È preferibile rischiare una multa o una richiesta di presentarsi in questura con un documento valido, piuttosto che dover rifare tutti i documenti. Nella fotocopia potrebbero rimanere evidenziati solo i dati sensibili o utili in caso di fermo, e cioè il numero del documento, la data di rilascio, il codice fiscale e NON inserire dati come nome e cognome (che potete fornire a voce), soprattutto l’indirizzo o dati che possano fornire al ladruncolo il modo di identificarvi, e poi con le chiavi che vi ha appena rubato entrare nel vostro appartamento o localizzare la vostra auto. I documenti ve li porterete quando ritenete siano necessari, tenendo presente che l’unico documento strettamente necessario è la patente auto che dovete avere durante la guida. Una fotocopia generalmente non è accettata, ma presentando l’originale entro le 24 ore si evita la contestazione di “guida senza patente”. Giudicate voi come è meglio comportarsi, in ogni caso le fotocopie dei documenti sono utili anche nel caso si dovessero smarrire o venissero rubati gli originali.

VIDEO SORVEGLIANZA:

Gli impianti anti intrusione dotati dei sistemi di videosorveglianza si rivelano molto utili ai fini di identificare gli autori dell'effrazione. Per questo motivo, dotarsi di una semplice telecamera che si limiti a far visualizzare su un monitor quanto viene inquadrato, equivale ad installare un video-citofono! Se abbinata invece, ad un sistema di video-registrazione, il risultato sarà proprio quello desiderato. Nel posizionare le telecamere, si deve prevedere che queste possano essere oscurate, rimosse, o semplicemente girate, in modo da riprendere tutto tranne le immagini necessarie; Quando è possibile è meglio prevedere di installarne due, una di fronte all'altra, così da coprirsi a vicenda. Se anche qualcuno tentasse di oscurarle entrambe, e nello stesso momento, difficilmente eviterebbe di essere inquadrato da una delle due telecamere. Un'altra accortezza, è quella di utilizzare telecamere del tipo A che nascondono l'orientamento dell'obiettivo, anzi alcune dispongono di lenti con visuale a 360 gradi, in grado di coprire una vastissima area. Le telecamere di tipo B hanno invece il vantaggio (se montate su appositi brandeggi) di poter essere orientate in modo automatico (ad inseguimento) e manuale, quindi indirizzate dove si svolge l'azione che in quel momento interessa riprendere.

TIPO A

TIPO B

Nell'epopea appena trascorsa, si utilizzavano videoregistratori VHS a nastri che a loro volta dovevano essere sostituiti o riportati all'inizio per iniziare una nuova registrazione. Con opportuni accorgimenti elettronici, questi nastri giravano lentamente, tanto da durare fino a 8 ore, e mai più di 24. Con la tecnologia digitale si è arrivati ad utilizzare

videoregistratori che utilizzano un hard disk, con capacità di registrazione in grado di coprire ininterrottamente come minimo una settimana, e al massimo (per il momento) tre mesi! La tecnica digitale permette di avere su un'unica pista di registrazione fino ad 8 segnali video, che diventano 16 e più utilizzando la tecnica molto conosciuta nelle regie televisive, che consiste nel suddividere lo schermo in più immagini, ognuna proveniente da una fonte diversa. Le immagini sono accompagnate da informazioni tra le più disparate, come l'ora, il giorno, l'area e così a seguire…Naturalmente sarebbe bene nascondere l'impianto di videoregistrazione o inserirlo all'interno di una camera blindata, al fine di evitare che chi si introduce possa in seguito asportarlo con tutte le sue preziose informazioni. Tutte le telecamere devono essere dotate di illuminatori ad infrarossi, così che possano riprendere anche di notte senza alcun problema. L'utilizzo di fari o lampade è sconsigliato, perché innesca un automatismo di protezione che porta l'obiettivo a chiudersi per potersi adattare alla luce (che non deve mai essere rivolta verso l'obiettivo), e a lungo andare provoca una sorta di buco nero al centro dell'immagine, e anche perché, rompere una lampada è molto semplice . A tal proposito mi spiace dover segnalare che l'unico modo per accecare una telecamera è proprio quello di indirizzargli una forte fonte luminosa contro, non esiste alcun modo di ovviare a questo, se non con un apposito circuito che attiva un allarme di accecamento, ed è proprio per questo motivo che consiglio di installare sempre due telecamere. Vi è poi la possibilità di montare particolari filtri antiriflesso e anti abbagliamento (come quelli utilizzati in fotografia per riprendere il sole), si perde un po' nella qualità dell'immagine, ma almeno si salva l'obiettivo. Segnalo anche la possibilità di dotarsi di telecamere finte, costano poco, e spesso fanno la differenza. Per rendere credibile la cosa, dotatevi anche del cartello che segnala la zona video sorvegliata, collegate fili e cavetti e utilizzate quelle telecamere munite di un piccolo Led sempre acceso, così da rendere il tutto più verosimile. Se qualcuno "non la beve", beh, in questo caso spero abbiate seguito sino a qui i miei consigli e vi siate dotati di un impianto antintrusione.

E se fossi il ladro…?

Premesso che per evitare una denuncia per istigazione a delinquere tendo a precisare che lo scopo di questo paragrafo è unicamente quello di informare i commercianti, così che possano adattarsi e rimediare….

Il Taccheggio:
Per poter distaccare quelle grosse piastre plastiche attaccate agli abiti, è necessaria una grossa calamita, ad esempio presa da un grosso altoparlante, poi la si deve mettere sul lato opposto alla piastra, quindi sul retro ed esercitare con forza sino a separare la piastra dal suo fermo. Le cassiere hanno a disposizione una grossa base, molto pesante, e anche loro fanno una certa fatica, quindi non pensate sia così facile.
Per eliminare invece le etichette trappola, se è possibile è sufficiente appoggiare una moneta metallica al centro dell'etichetta, ma se avete un tronchesino, è molto meglio romperla, tranciarla in modo da interrompere la bobina che si trova all'interno. Tenete presente che spesso le etichette sono due, una esca facilmente individuabile, l'altra celata persino sotto le suole delle scarpe, spesso sono adesive quindi facilmente staccabili.

Le sirene:
Come abbiamo letto, è ormai inutile riempire le sirene di schiumogeni, è molto più semplice – una volta che siete riusciti a raggiungerle – coprire le fessure in modo da attenuare il suono, lasciandole suonare e lasciare credere ai vicini che in zona ci sia uno sciame di zanzare o che da qualche parte, lontano, stia suonando una sirena.

Combinatori telefonici:
Esistono due strade da percorrere: una è quella data dalla conoscenza del numero telefonico dell'appartamento da "violare", l'altra quella di non conoscerlo. In questo secondo caso, se si

tratta di una abitazione singola, una villetta si può individuare l'ingresso della linea telefonica aprendo eventualmente la scatoletta di derivazione, e ponendo tra i due fili bianco e rosso, una resistenza da 100 ohm, in grado di mantenere la linea funzionante per il combinatore, ma impedendo la formazione di numeri in chiamata sia essi formati utilizzando impulsi o suoni. Non dovete scollegare i fili, perché quasi tutti i combinatori dispongono del controllo di presenza linea. Se pensate che venga utilizzato un cellulare, l'unico modo per inibirlo è quello di utilizzare quegli strumenti che disturbano in un raggio di qualche centinaio di metri tutte le comunicazioni della rete.
Conoscendo invece il numero telefonico dell'utente è sufficiente effettuare una chiamata pochi secondi prima di far scattare l'allarme, così che il combinatore prendendosi la linea, altro non faccia che rispondere alla chiamata, e tutti i messaggi anziché andare a destinazione, vengono deviati sul telefono che avete appena utilizzato per chiamare.

Casseforti:
Quelle tradizionali, per intenderci, quelle con il pomello da girare sono facilmente violabili utilizzando uno stetoscopio. Si appoggia lo strumento vicino al pomello e si inizia a girare a destra; se dopo un giro completo non si sente nessun TAC, significa che la prima cifra è a sinistra, quindi si gira a sinistra, e quando si sente il TAC, si gira a destra e così via sino a combinare tutta la sequenza esatta. Fare attenzione che molto spesso superando la cifra esatta anche di poco, si azzera tutto, quindi eseguite le manovre molto lentamente. Con le tastiere elettroniche, invece se non avete trovato la chiave nascosta da qualche parte, dovete tentare con il numero dato dalla fabbrica (anche voi….un po' di ricerca suvvia!), perché quasi sempre pochi provvedono a modificarlo, lasciando la combinazione inalterata (come per il pin del cellulare) facilitandovi il lavoro. Comunque le casseforti che utilizzano la tastiera generalmente sono di piccole dimensioni, potete sradicarle dal muro e portarvele via così da poterle aprire con tutta calma. Per i CAVEAU delle banche, beh, dubito che chi voglia forzarli stia leggendo questo libro…

In generale:
Molto spesso, per chi ha pazienza, meglio togliere la tensione di rete elettrica, aspettare che si scarichino le batterie, e per velocizzare i tempi, meglio far suonare l'impianto a vuoto, e come per la favola "al lupo, al lupo" dopo continui e ripetuti falsi allarmi, è molto probabile che quando sarà giunto il momento buono, nessuno ci creda e vi lasci lavorare con tranquillità.

[2] I rilevatori hanno un Led utilizzato come memoria di avvenuto allarme. Quando l'apparato genera un allarme rimane acceso in modo fisso un Led di colore rosso. Perché si spenga sarà necessario che la centrale venga disattivata (impianto spento). Alla prima riattivazione della centrale il Led tornerà allo stato iniziale. Esistono dispositivi che sono invece azzerati dalla centrale con apposita funzione di ripristino. Lo scopo è quello di poter identificare l'area che ha generato l'allarme, o il dispositivo tra i tanti; Quando alla centrale ogni dispositivo è collegato singolarmente questa funzione non si rende necessaria, poiché è sempre possibile sapere quale dispositivo ha generato l'allarme

Conclusioni:

Spero di essere stato esaustivo, di avervi tolto ogni dubbio. Avrei potuto segnalare qualche marca considerandola migliore rispetto alle altre, avrei potuto indicare qualche azienda installatrice, ma non mi è sembrato corretto farlo. Primo perché ogni città, ogni regione ha le sue aziende, ed elencarne una su migliaia sarebbe stato illogico farlo, avrei potuto far sponsorizzare il libro da una nota azienda o una nota marca, ma anche questo ho ritenuto di evitarlo. Gli strumenti a disposizione oggi, come motori di ricerca, elenchi telefonici, pubblicità specialistica e non da ultimo il passa-parola possono aiutarvi nella scelta. Va da sé che se scegliete una buona ditta installatrice, sarà questa a dotarvi di una buona marca di apparati. Quello forse che potete tenere in considerazione è l'esperienza e l'anzianità dell'azienda che andrete a scegliere, non trascurando l'emergente, spesso con notevole esperienza come dipendente di ditte nel settore della sicurezza, e che ha deciso in seguito di provare a mettersi in proprio e che quindi per questo non deve rimanere escluso. La sicurezza propria , quella dei propri beni è un diritto sacrosanto, deve essere protetto. Se avete letto in ogni parte questo libro, avete senz'altro capito come in ogni mia frase, ogni mio consiglio abbia seguito un unico indirizzo, un unico filo conduttore: prevenire. Spesso si pensa di essere al di fuori delle categorie a rischio, semplicemente perché abitate al 5° piano, o perché avete un doberman in giardino, poi quando anche voi venite colpiti dagli eventi, sino ad allora impensabili, ecco che pensate di munirvi di una protezione che eviti il ripetersi del danno, intanto però, forse, avete perso le cose più care, lasciatevi dal bisnonno, oppure documenti fotografie irripetibili, avete subito danni rilevanti, e nel peggiore dei casi ora piangete un vostro caro, rimasto vittima di una reazione che fino a qualche anno fa' non sembrava potesse avvenire mai!
In coda a questo libro ho voluto inserire una sezione tecnica, un vero "mattone", dove vengono illustrate le varie tipologie fin qui trattate, unicamente da un punto strettamente tecnico. L'ho fatto per dovere di completezza, ma potete benissimo non leggerlo.

Un immagine dell'autore risalente ad un epoca definita dalle mie parti come quella della " Milano da bere…". Eravamo intorno agli anni '80. Con questa immagine insignificante ai fini della lettura di questo libro, lascio un indizio per chi la vuole immaginare nella serie *come sarà adesso*, mentre per me nostalgico rappresenta un piacevole ricordo, da lasciare ai posteri e gli eredi, in particolare a mia figlia Debora alla quale questo libro dedico. Ai lettori, invece, lascio i miei ringraziamenti nella speranza che se anche per poco, questo volume possa aver contribuito a migliorare la propria e altrui sicurezza. All'Editore, che pur considerando il tema della sicurezza – così come improntato – fosse quantomeno anomalo e insolito per giustificarne la pubblicazione, ha creduto in me rischiando di Suo, contribuendo alla riuscita nell'insieme di quest'opera. Ed infine a tutti i ladri, gli scippatori, i rapinatori, i sequestratori, insomma a tutti i numerosi iscritti della categoria, che forse, dopo avermi letto, se la siano presa un po' magari con l'intenzione di denunciarmi per concorrenza sleale, delusi per l'inevitabile calo della clientela che questo libro ha comportato. Che sia giunto il momento – per Voi – di cambiare mestiere?. O meglio che sia giunto il momento di guadagnarsi da vivere onestamente? Fatemi sapere!

Marco Saporiti

TECNICA:

La tecnologia RFID

INTRODUZIONE

La tecnologia RFID è una delle tecnologie più all'avanguardia e attualmente in rapido sviluppo tra quelle richieste dalle aziende. L'adozione della tecnologia di raccolta dati automatica (ADC) è stata recentemente favorita dalla determinazione degli standard chiave, dalle esigenze dei più grossi retailer e di enti governativi, da prestazioni tecnologiche potenziate e costi di implementazione sempre più bassi. L'RFID rappresenta un enorme valore aggiunto per numerosi settori e applicazioni. Tuttavia, ci sono fattori e mancanza di informazioni corrette riguardo alla natura e alle funzionalità dell'RFID che possono scoraggiare le aziende dall'adottare questa tecnologia.

Questo paragrafo offre una panoramica della tecnologia RFID e delle sue funzionalità, descrive le tecnologie e le frequenze utilizzate normalmente per applicazioni aziendali, identifica i principali standard e presenta modi per avvalersi al meglio dell'RFID e per aumentarne la comodità, la precisione e la sicurezza.

"RFID" indica un tipo di tecnologia in grado di scambiare dati in modalità wireless. I dati vengono registrati e letti da un chip fissato a un'antenna che riceve i segnali in radiofrequenza da un dispositivo di lettura/scrittura, chiamato comunemente lettore o codificatore. I dati vengono scambiati automaticamente, senza che sia necessario l'intervento di un operatore per avviare una lettura RFID.

L'RFID offre vari importanti vantaggi rispetto ad altri metodi di raccolta dati:

- L'RFID consente il monitoraggio e la raccolta dati in

ambienti non adatti agli operatori, dato che la lettura di tag non richiede l'intervento umano.

- È possibile realizzare oltre un migliaio di letture al secondo, garantendo un'elevata velocità ed estrema precisione.
- I dati registrati in un tag RFID possono essere modificati più volte.
- L'RFID non richiede prossimità tra il tag e il lettore, e perciò è adatto a numerose applicazioni in cui i codici a barre non sono utilizzabili.
- Migliaia di aziende in diversi settori hanno tratto vantaggio dall'RFID per sviluppare applicazioni in grado di controllare i processi, offrire precisione di dati in tempo reale, consentire la tracciabilità dei cespiti aziendali e degli inventari e ridurre i costi.
- La tecnologia RFID può essere utilizzata con sistemi di codici a barre e le reti Wi-Fi.

FUNZIONAMENTO DELLA TECNOLOGIA RFID

I sistemi RFID comprendono tag, lettori e software per l'elaborazione dei dati. I tag vengono applicati normalmente ai prodotti, spesso come parte di un'etichetta adesiva a codici a barre. I tag possono essere applicati inoltre a scatole di protezione più resistenti e a carte d'identità o cinturini. I lettori possono essere unità standalone senza sorveglianza (come quelle per il monitoraggio della porta di un dock o di un nastro trasportatore), integrati da un computer portatile per essere utilizzati come palmari o su carrelli elevatori o incorporati in stampanti di codici a barre.

Il lettore invia un segnale radio che viene ricevuto da tutti i tag presenti nel campo di radiofrequenze sintonizzati su quella frequenza. I tag ricevono il segnale mediante le loro antenne e rispondono trasmettendo i dati memorizzati. I tag possono contenere diversi tipi di dati, compresi numeri di serie, istruzioni di configurazione, cronologia delle attività (ad es. data dell'ultima manutenzione, ora del passaggio di un tag in un punto specifico, ecc.), o addirittura la temperatura e altri dati forniti dai sensori. Il dispositivo di lettura/scrittura riceve il segnale del tag mediante l'antenna, lo decodifica e trasferisce i dati al sistema del computer mediante un cavo o una connessione wireless.

Le seguenti sezioni descrivono più dettagliatamente tag, lettori,stampanti e prestazioni RFID.

Tag (transponder)

I tag RFID sono caratterizzati da due elementi fondamentali: un chip e un'antenna. Il chip e l'antenna sono montati in modo da costituire un inlay.

L'inlay viene racchiuso quindi da un altro materiale per costituire un tag o un'etichetta finita.

Tipi di tag diversi vengono utilizzati per diverse condizioni ambientali. Ad esempio, i tag adatti a scatole di cartone contenenti oggetti in plastica potrebbero non essere adatti a pallet in legno, contenitori in metallo o vetro. I tag possono avere le dimensioni di un chicco di riso, essere grandi come un mattone o essere così sottili e ?essibili da poter essere integrati in un' etichetta adesiva. I tag possono differire enormemente nelle prestazioni, compresa la capacità di lettura/scrittura, nonché nei requisiti di memoria e potenza

Le etichette con spessore di un foglio chiamate "etichette intelligenti" vengono utilizzate solitamente in applicazioni monouso, come quelle per l'identificazione di scatole e pallet. La stampante/codificatori creano etichette intelligenti on demand, codificano il tag e stampano al contempo del testo e/o un codice a barre sull'etichetta esterna. Le etichette intelligenti soddisfano la maggior parte dei requisiti di conformità di tag RFID per scatole e pallet.

I tag RFID si differenziano anche per quanto riguarda la resistenza, in base al tipo di applicazione e all'ambiente in cui vengono utilizzati. I tag per l'identificazione permanente possono essere protetti per resistere alle temperature estreme, all'umidità e ai solventi, a vernici, olio e ad altri elementi che possono deteriorare il testo, i codici a barre e altri metodi di identificazione a tecnologia ottica. I tag RFID possono essere riutilizzabili e adatti all'identificazione costante, offrendo quindi un vantaggio sul costo totale di gestione (TCO) rispetto alle etichette a codici a barre e altri metodi di identificazione temporanei.

I tag RFID possono essere sia di sola lettura sia di sola scrittura (sebbene gli ultimi siano ora standard). I tag di sola lettura vengono programmati in fabbrica con un numero di serie o altri dati non modificabili. I dati memorizzati sui tag di lettura/scrittura possono essere modificati migliaia di volte. I tag di lettura/scrittura vengono spesso divisi in un'area di sola lettura definita dall'utente e protetta, che può contenere un numero di identificazione unico e una parte scrivibile di memoria che gli utenti possono programmare liberamente. Un utente può quindi codificare in modo permanente il numero di identificazione di un pallet in una memoria di sola lettura e quindi utilizzare la parte di lettura-scrittura per registrare gli articoli caricati sul pallet. Quando il pallet viene scaricato, la sezione registrabile può essere cancellata per essere riutilizzata.

I tag possono essere classificati anche come passivi, semipassivi o

attivi. I tag passivi, estremamente più diffusi, ricevono le trasmissioni dal lettore. Tutte le etichette RFID intelligenti sono passive. I tag attivi includono una batteria per permettere le operazioni di trasmissione e che consente inoltre di operare su distanze più elevate. Per tale motivo i tag attivi sono più grandi e più costosi dei tag passivi. I tag semipassivi comunicano come i tag passivi ma dispongono inoltre di una batteria. La loro portata si situa tra quella dei tag passivi e attivi e sebbene le loro batterie siano di lunga durata, le loro dimensioni sono simili a quelle dei tag passivi.

Opzioni

I dispositivi RFID consentono un'elevata ?essibilità di posizionamento perché, a differenza dei lettori di codici a barre, non è necessaria un prossimità diretta e le distanze di lettura possono essere elevate. Ad esempio, i lettori possono essere installati sotto pavimenti o montati su soffitti. La banda UHF (ultrahigh frequency) RFID può consentire un raggio di lettura di oltre 10 metri. I lettori portatili possono essere integrati in computer portatili o stampanti di etichette intelligenti o montati su veicoli (carrelli elevatori).

I sistemi RFID possono operare contemporaneamente con reti wireless, e spesso sono integrati con LAN wireless per scambiare dati con sistemi di computer host; le LAN Wi-Fi non creano interferenze con i sistemi RFID (le apparecchiature proprietarie anteriori di rete wireless a 915 MHz possono interferire con i sistemi RFID UHF, ma pochi di questi dispositivi sono ancora in uso).

PRESTAZIONI DELLA TECNOLOGIA RFID

Le caratteristiche fondamentali descritte qui sopra sono comuni a tutte le tecnologie RFID. I sistemi RFID si differenziano in base a gamma e frequenza utilizzate, memoria chip, protezione, tipo di dati raccolti e altri aspetti. Capire queste variabili è fondamentale per comprendere le prestazioni RFID e il modo in cui questa tecnologia può essere utilizzata. I seguenti paragrafi descrivono brevemente le caratteristiche RFID più importanti.

Frequenza

La frequenza è il fattore principale per stabilire il raggio d'azione, la resistenza alle interferenze e altre caratteristiche delle prestazioni dell'RFID. La maggior parte dei sistemi commerciali RFID funzionano sia sulla banda UHF, tra 859 e 960 MHz sia su banda HF (high frequency) a 13,56 MHz. Altre frequenze RFID diffuse includono i 125 KHz (una frequenza a corto raggio spesso utilizzata per l'identificazione

di veicoli), i 430 MHz e i 2,45 GHz, utilizzati entrambi per l'identificazione a largo raggio, spesso con tag costosi alimentati a batteria. La banda UHF è maggiormente utilizzata per le applicazioni della supply chain e di automazione industriale. Il diffuso standard Gen 2 di EPC global (che verrà illustrato in dettaglio in seguito) è una tecnologia UHF.

Raggio di lettura

Il raggio di lettura di un sistema RFID (la distanza dal tag in cui deve rientrare l'antenna del lettore per poter leggere le informazioni memorizzate nel chip del tag) va da pochi centimetri a decine di metri, in base alla frequenza utilizzata, alla potenza in uscita e alla sensibilità direzionale dell'antenna. La tecnologia HF viene utilizzata per applicazioni a corto raggio e può essere letta da una distanza che raggiunge i tre metri. La tecnologia UHF consente un raggio di lettura di oltre 20 metri. Il raggio di lettura dipende molto dall'ambiente fisico circostante, la presenza di metalli e liquidi può interferire, incidendo sulle prestazioni. Quindi i sistemi multipli all'interno dello stesso edificio possono funzionare su diversi raggi in base all'ambiente circostante e alla posizione dell'antenna. Per i tag di lettura/scrittura, il raggio di lettura supera normalmente il raggio di scrittura.

Protezione

I chip RFID vengono difficilmente contraffatti. Un hacker avrebbe bisogno di conoscenze specifiche di ingegneria wireless, codifica di algoritmi e tecniche di crittografia. Inoltre, è possibile applicare diversi livelli di protezione ai dati su un tag, e in tal modo le informazioni possono essere lette in certi punti della supply chain ma non in altri. Alcuni standard RFID comportano un'ulteriore protezione. Grazie a questa protezione insita, la FDA statunitense (Food and Drug Administration) ha incoraggiato l'uso dell'RFID come misura di sicurezza contro la contraffazione farmaceutica. I produttori di farmaci hanno iniziato ad avvalersi della relativa invulnerabilità della tecnologia RFID, assieme a produttori di apparecchiature elettroniche, di abbigliamento e altri produttori.

Standard

Nel primo periodo di utilizzo dell'RFID, era diffusa la falsa convinzione che l'RFID fosse una tecnologia proprietaria sprovvista di standard. Oggi, numerosi standard garantiscono diverse frequenze e applicazioni. Esistono ad esempio standard RFID per la gestione di prodotti, logistica dei container, biglietti di viaggio, identificazione di animali, identificazione di gomme e ruote e per numerosi altri usi. L'ISP (International Standards Organization) ed EPCglobal Inc. sono due delle più importanti associazioni per la determinazione di standard per la supply chain. Numerosi standard di settore e nazionali si basano sugli standard ISO o EPCglobal, come lo standard

statunitense ANSI MH10.8.4 per l'identificazione di contenitori riutilizzabili.
Per definizione, gli standard ISO possono essere utilizzati ovunque nel mondo e vengono adottati come standard nazionali in numerosi paesi. Lo standard UHF EPCglobal Generation 2 (EPC Gen 2) è stato presentato all'ISO e diventerà probabilmente parte della serie di standard ISO-18000.
Lo standard Gen 2 è stato creato per semplificare l'uso di numeri Electronic Product Code™ (EPC), che identificano in modo individuale oggetti quali pallet, scatole o singoli prodotti. Gli standard EPC forniscono sia specifiche tecniche RFID sia un sistema di numerazione per l'identificazione individuale e assolutamente chiara dei prodotti. Gli standard Gen 2 e EPC vengono amministrati da EPCglobal, una consociata di GS1 (la stessa organizzazione non-profit che rilascia i numeri UPC e gestisce il sistema EAN.UCC). Molti produttori, retailer, altre aziende, organismi del settore pubblico e associazioni industriali hanno adottato o sottoscritto gli standard EPC, in particolare lo Gen 2.

USO DELL'RFID

L'RFID offre soluzioni alternative quando è poco pratico o impossibile utilizzare altre tecnologie o operare in modo manuale per la raccolta dati. L'RFID è in grado di funzionare in ambienti in cui fattori quali ostacoli intermedi, requisiti di lettura ad alta velocità, temperature estreme ed esposizione a gas o ad agenti chimici impediscono l'uso di altri metodi di raccolta dati. L'RFID è estremamente pratico per un gran numero di operazioni comuni. I consumatori utilizzano normalmente l'RFID per aprire le porte della macchina in remoto, gestire rapidamente il prestito e la restituzione di libri nelle biblioteche e velocizzare le transazioni nelle stazioni di servizio passando una scheda di autenticazione alla pompa della benzina. Le aziende si affidano all'RFID per tracciare in sicurezza e registrare la posizione di migliaia di prodotti, invii e articoli di inventario.

L'RFID dispone ancora di moltissime potenzialità non utilizzate, specialmente se viene integrato con altre tecnologie e applicazioni software. Basta pensare a un sensore di temperatura o di urti integrato in un tag RFID che invia automaticamente un segnale di allerta sulle variazioni delle condizioni ambientali, che potrebbero danneggiare o rovinare i prodotti. I sistemi RFID e le reti wireless potrebbero essere integrati per garantire un monitoraggio continuo

su ampia scala. I movimenti di inventario da siti controllati possono dare l'input a una richiesta di rifornimento o avvertire il personale di sicurezza se il prodotto è stato spostato da personale non autorizzato. Queste applicazioni sono già operative, come altri sistemi all'avanguardia che offrono ulteriore praticità ed efficienza nelle transazioni con il consumatore, nel settore sanitario, di identificazione personale, della produzione, della logistica, della gestione delle risorse e in molte altre operazioni.

GLI INFRAROSSI :

La radiazione infrarossa (IR) è la radiazione elettromagnetica con una frequenza inferiore a quella della luce visibile, ma maggiore di quella delle onde radio. Il nome significa "sotto il rosso" (dal latino infra, "sotto"), perché il rosso è il colore visibile con la frequenza più bassa. La radiazione infrarossa ha una lunghezza d'onda (che è uguale alla velocità della luce al secondo divisa per la frequenza) compresa tra 700 nm e 1 mm. Viene spesso associata con i concetti di "calore" e "radiazione termica", poiché gli oggetti a temperatura ambiente o superiore emettono spontaneamente radiazione in questa banda (aumentando la temperatura, il picco si sposta sempre più verso il visibile finché l'oggetto non diviene incandescente).

Il limite inferiore dell'infrarosso veniva spesso definito come 1 mm poiché a questa lunghezza d'onda termina l'ultima delle bande radio classificate (EHF, 30-300 GHz). Ciò nonostante, la regione da circa 300 µm a 1000 µm era considerata una "terra di nessuno", difficilmente indagabile a causa della mancanza di sensori e soprattutto di sorgenti luminose adatte ad operare in questa banda. Recentemente queste limitazioni tecniche stanno cadendo, dando origine ad una intensa attività di ricerca su questa parte dello spettro elettromagnetico che si preferisce ormai definire regione della radiazione a terahertz o dei "raggi T".

Data la vastità dello spettro infrarosso e molteplicità di utilizzi delle radiazioni collocate in vari punti al suo interno, sono state sviluppate diverse classificazioni in ulteriori sottoregioni. Sfortunatamente non esiste un unico standard riconosciuto per queste bande, ma più convenzioni settoriali, nate in differenti campi di ricerca e dell'ingegneria per suddividere le regioni collegate a diverse classi di fenomeni nella branca di volta in volta interessata.

Nome banda Limite superiore Limite inferiore
Standard DIN/CIE
IR-A 700 nm 1400 nm

IR-B 1,4 µm 3 µm
IR-C 3 µm 1000 µm
Classificazione astronomica
vicino 700 - 1000 nm 5 µm
medio 5 µm 25-40 µm
lontano 25-40 µm 200-350 µm
Sistema ingegneristico
vicino (NIR) 750 nm 1400 nm
onda corta (SWIR) 1,4 µm 3 µm
onda media (MWIR) 3 µm 8 µm
onda lunga (LWIR) 8 µm 15 µm
lontano (FIR) 15 µm 1000 µm

Un ulteriore sistema pratico, sviluppato nell'ambito dell'industria delle telecomunicazioni, suddivide in bande molto strette la regione del vicino infrarosso interessante per la trasmissione a mezzo fibra ottica

Nome Intervallo
O (Original) 1,26 - 1,36 µm
E (Extended) 1,36 - 1,46 µm
S (Short) 1,46 - 1,53 µm
C (Conventional) 1,53 - 1,565 µm
L (Long) 1,565 - 1,625 µm
U (Ultra long) 1,625 - 1,675 µm

Nelle lunghezze d'onda adiacenti a quelle visibili fino ad un paio di micron, i fenomeni associati sono essenzialmente assimilabili a quelli della luce, anche se la risposta dei materiali alla luce visibile non è per nulla indicativa di quella alla luce infrarossa. Oltre i 2 µm ad esempio il normale vetro è opaco, così come molti gas, cosicché esistono finestre di assorbimento nelle quali l'aria è opaca e pertanto le frequenza che vi ricadono sono assenti dallo spettro solare osservato a terra. Una nuova finestra di trasmissione si apre tra 3 e 5 µm, corrispondente al picco di emissione di corpi molto caldi (la banda utilizzata, ad esempio, dai missili a ricerca termica).

Al contrario, molti materiali che ai nostri occhi appaiono

perfettamente opachi, sono più o meno trasparenti a queste lunghezza d'onda. Ad esempio silicio e germanio a queste lunghezze d'onda presentano opacità ridottissime, tanto che vengono usati per fabbricare lenti e fibre ottiche (attenuazioni nell'ordine di 0.2 dB/km per i 1550 nm). Pure molte materie plastiche sintetiche hanno una buona trasparenza a queste radiazioni.

A lunghezze d'onda maggiori si hanno fenomeni via via più simili alle onde radio.

Un rivelatore ad infrarossi è un rivelatore che reagisce alla radiazione infrarossa (IR). I rivelatori si dividono fra termici e fotonici.

Gli effetti termici della radiazione IR incidente possono essere rivelati attraverso fenomeni che dipendono dalla temperatura. Bolometri e microbolometeri sono basati su variazioni della resistenza. Termocoppie e termopile si basano sull'effetto termoelettrico. I Rivelatori di Golay sfruttano l'espansione termica. Per gli spettrometri IR i rivelatori piroelettrici sono i più comuni.

Il tempo di risposta e la sensibilità dei rivelatori per l'infrarosso possono essere più alti, ma di solito questi devono essere raffreddati per il abbattere il rumore termico. I materiali utilizzati sono semiconduttori con strette bande proibite. I fotoni incidenti possono causare l'eccitazione elettronica. In rivelatori fotoconduttivi, la resistività dell'elemento del rivelatore è monitorato. Rivelatori fotovoltaici contengono una giunzione p-n sulla quale un corrente fotoelettrica appare quando viene illuminata.

Alcuni materiali dei rivelatori:

Tipo Gamma spettrale (µm)
Arsniuro di Gallio Indio (InGaAs) fotodiodi 0.7-2.6
Germanio rivelatori fotodiodi 0.8-1.7
Solfuro di piombo (PbS) rivelatori fotoconduttivi 1-3.2
Clausthalite (PbSe) rivelatori fotoconduttivi 1.5-5.2

Arseniuro di Indio (InAs) rivelatori fotovoltaici 1-3.8
Siliciuro di Platino (PtSi) rivelatori fotovoltaici 1-5
Antimoniuro di Indio (InSb) rivelatori fotoconduttivi 1-6.7
Antimoniuro di Indio (InSb) rivelatore fotodiodi 1-5.5
Telluriuro di Cadmio Mercurio (MCT, HgCdTe) rivelatori fotovoltaici 2-25
Telluriuro di Cadmio Mercurio (MZT, HgZnTe) rivelatori fotovoltaici ?

Anidride vanadica è spesso usata come un materiale per rivelatori in un array microbolometero.

LE MICROONDE:

Le microonde sono radiazioni elettromagnetiche con lunghezza d'onda compresa tra le gamme superiori delle onde radio e la radiazione infrarossa. Sebbene si tenda a considerarle separate dalle radioonde, le microonde sono comprese nelle parti UHF e EHF dello spettro radio, presentando comunque delle caratteristiche specifiche dovute alla loro alta frequenza. Il confine tra le microonde e le gamme di radiazioni vicine non è infatti netto e può variare a seconda dei diversi campi di studio.

Sono così chiamate perché hanno onde molto corte, comprese tra 1 m (frequenza di 300 MHz) e 1 mm (frequenza 300 GHz).

Al di sopra dei 300 GHz l'assorbimento delle radiazioni elettromagnetiche da parte dell'atmosfera terrestre è così intenso che può essere considerata opaca a queste frequenze. Ritorna però ad essere trasparente nella zona degli infrarossi e della luce visibile.

Produzione
Le microonde possono essere prodotte in vari modi, classificabili in due categorie: a stato solido e con tubi a vuoto.
I dispositivi a stato solido sono basati su semiconduttori (silicio o arseniuro di gallio) e possono essere transistor ad effetto campo (FET), transistor a giunzione bipolare (BJT), diodi Gunn e IMPATT. Versioni speciali dei comuni transistor sono state

sviluppate per le alte frequenze. L'evoluzione per le microonde dei transistor BJT includono il heterojunction bipolar transistor (HBT), mentre le varianti dei transistor FET comprendono: MESFET, HEMT o HFET e LDMOS. I dispositivi integrati a microonde sono chiamati MMIC (monolithic microwave integrated circuit) e sono realizzati a partire da wafer di arseniuro di gallio.
I tubi a vuoto si basano sul movimento balistico degli elettroni nel vuoto sotto l'influenza di campi elettrici o magnetici di controllo. Includono: magnetron, klystron, travelling wave tube (TWT) e gyrotron.

Utilizzi
Ponti radio ovvero trasmissione tra antenne paraboliche terrestri, a distanze fino a centinaia di km, di segnali analogici (ad es. TV) o digitali fino a capacità di centinaia di Mbit/s. Si utilizzano normalmente frequenze comprese fra i 2 GHz ed gli 80 GHz, in bande specificamente stabilite dagli organismi regolatori nazionali ed internazionali. Le potenze utilizzate sono di pochi watt o frazioni di watt, per ogni canale (portante).
I recenti telefoni cellulari GSM operano alla frequenza di 1,8 GHz per comunicare con la stazione radio base.
Il forno a microonde utilizza un generatore a magnetron per produrre microonde alla frequenza di circa 2,45 GHz per cuocere il cibo. Il riscaldamento e la conseguente cottura è dovuto al fatto che le microonde causano un aumento dell'energia rotazionale delle molecole di alcune sostanze e in particolare dell'acqua. Le molecole dell'acqua infatti hanno un momento di dipolo elettrico che ha la stessa energia delle microonde. Dato che la materia organica è composta in prevalenza di acqua, il cibo può essere cucinato facilmente con questa tecnica.
Antenna di un radar Le microonde sono utilizzate per le comunicazioni con i satelliti poiché attraversano l'atmosfera terrestre senza subire interferenze, come accade invece per le onde radio. Si ha inoltre più larghezza di banda (e quindi possibilità di trasportare più informazione) nelle microonde che non nelle onde radio.
I Radar utilizzano le microonde per rilevare a distanza la presenza ed il movimento di oggetti.
I protocolli di comunicazione senza fili, come il bluetooth e il IEEE 802.11 nelle varianti g e b utilizzano microonde nella banda a

2,4GHz; la variante a lavora invece a 5 GHz. In alcune nazioni sono in uso servizi di accesso ad Internet a lunga distanza (25 Km) operanti nelle frequenze tra 3,5 e 4 GHz.
Alcuni servizi di diffusione televisiva, accesso ad Internet e telefonia su Cavo coassiale utilizzano microonde di bassa frequenza.
Le microonde possono essere usate per trasferire energia a distanza. Durante la seconda guerra mondiale furono effettuate ricerche in questa direzione. La NASA studiò negli anni '70 e '80 un sistema di satelliti con ampi pannelli solari per produrre energia elettrica e trasferirla sulla terra per mezzo di un fascio di microonde. Questi studi furono la base dei moderni progetti di centrale solare orbitale.
Il maser è un dispositivo simile al laser ma operante nello spettro delle microonde.
Un campo a microonde viene utilizzato per accelerare particelle cariche in alcuni tipi di cavità risonanti utilizzate negli acceleratori di particelle
Vi sono diversi tipi di armi di nuova generazione che impiegano le microonde. Vedi armi a microonde.

Bande di frequenza
Lo spettro delle microonde è definito solitamente nell'intervallo di frequenza compreso tra 1 GHz e 1000 GHz, ma altre definizioni includono frequenze minori. La maggior parte delle applicazioni operano tra 1 e 40 GHz.
La seguente tabella elenca la suddivisione in bande secondo la Radio Society of Great Britain (RSGB):

Suddivisione in bande del campo delle microonde Sigla della banda Gamma di frequenza
L 1 - 2 GHz
S 2 - 4 GHz
C 4 - 8 GHz
X 8 - 12 GHz
Ku 12 - 18 GHz
K 18 - 26 GHz
Ka 26 - 40 GHz
Q 30 - 50 GHz

U 40 - 60 GHz
V 50 - 75 GHz
E 60 - 90 GHz
W 75 - 110 GHz
F 90 - 140 GHz
D 110 - 170 GHz

Il codice P è a volte usato per le frequenze UHF sotto la banda L.

GLI ULTRASUONI:

Gli ultrasuoni sono delle onde meccaniche sonore. A differenza dei fenomeni acustici propriamente detti le frequenze che caratterizzano gli ultrasuoni sono superiori a quelle mediamente udibili da un orecchio umano. La frequenza convenzionalmente utilizzata per discriminare onde soniche da onde ultrasoniche è fissata in 20 kHz. Lo stesso termine ultrasuono chiaramente indica ciò che è al di là (ultra) del suono, identificando con suono solo il fenomeno fisico udibile.

Come ogni altro tipo di fenomeno ondulatorio gli ultrasuoni sono soggetti a fenomeni di riflessione, rifrazione e diffrazione e possono essere definiti mediante parametri quali la frequenza, la lunghezza d'onda, la velocità di propagazione, l'intensità (misurata in decibel), l'attenuazione (dovuta all'impedenza acustica del mezzo attraversato).

Gli ultrasuoni in natura
Un pipistrello mentre effettua una cattura nella notte, grazie al suo sistema sensoriale ad ultrasuoni. Nonostante, come detto, l'essere umano, non sia in grado di udire gli ultrasuoni, altri animali hanno tale capacità. Ad esempio i cani (per i quali sono in commercio appositi fischietti di richiamo agli ultrasuoni), i delfini e le balene che li usano per comunicare tra loro e i pipistrelli che li usano per vedere gli ostacoli mentre volano di notte.

Applicazioni
Utilizzo degli ultrasuoni in campo medico (ecografia).Gli

ultrasuoni trovano utilizzo per lo più in campo medico ed industriale essendo ampiamente utilizzati nelle ecografie, nei controlli non distruttivi e in molti apparecchi utilizzati per la pulizia superficiale di oggetti di piccole dimensioni.

Anche il sonar impiega intervalli di frequenze che non di rado sconfinano nella gamma degli ultrasuoni.

Utilizzo degli ultrasuoni nelle operazioni di saldatura

Le principali applicazioni oltre quelle sopra indicate riguardano anche il campo meccanico, soprattutto la saldatura di materiali plastici e il controllo non distruttivo di cordoni di saldatura.

La saldatura di materiali plastici per mezzo di ultrasuoni viene sovente utilizzata quando è richiesta una certa qualità estetica ma soprattutto velocità di esecuzione; due oggetti plastici (preferibilmente dello stesso materiale in modo che l'attrito molecolare risulti alto) vengono messi a contatto fra loro e un parallelepipedo metallico (sonotrodo) si appoggia ad uno di essi scaricando ultrasuoni e quindi mettendolo in vibrazione. L'attrito generato fonderà le parti plastiche a contatto unendole. La forma e la frequenza alla quale vibrerà il sonotrodo dipendono dalla geometria dell'oggetto che si andrà a saldare.

La qualità estetica è eccellente anche se non viene assicurata la tenuta stagna quindi, nel caso sia essa un requisito fondamentale, è preferibile prendere in esame un altro tipo di saldatura (es. saldatura a lama calda).

Gli ultrasuoni sono anche uno dei controlli non distruttivi che si possono eseguire sui cordoni di saldatura fra metalli. L'attrezzatura necessaria è composta da uno schermo che visualizza in un grafico (molto simile ad un oscilloscopio) il ritorno (eco) delle onde di ultrasuoni che si propagano nel metallo e da una sonda dove è contenuto il materiale piezoelettrico che genera gli ultrasuoni. La sonda viene messa a contatto col cordone di saldatura da controllare, gli ultrasuoni si propagano nel metallo e ogni volta che nel cordone in questione è presente un'imperfezione (bolla d'aria,

accumulo di impurezze o una cricca) la massa volumica (densità) cambierà rispetto al resto del cordone di saldatura e parte degli ultrasuoni verranno riflessi. Noi vediamo questa onda di riflesso (eco) nello schermo e in base alla scala dello schermo riusciamo anche ad individuare la posizione approssimativa del difetto. Questo tipo di controllo è molto diffuso dato che risulta non distruttivo e permette di controllare cordoni di saldatura molto lunghi in brevissimo tempo individuando anche la posizione del difetto.

Generazione degli ultrasuoni

Gli ultrasuoni vengono generati per mezzo di materiali con particolari caratteristiche meccanico-elettriche, i materiali piezoelettrici. Questi particolari materiali come ad esempio il quarzo o titanato di bario hanno la caratteristica di generare una differenza di potenziale se compressi o stirati in senso trasversale, viceversa se applicata una differenza di potenziale ai loro estremi questi si comprimono o dilatano in senso trasversale. Proprio quest'ultima caratteristica viene sfruttata per generare queste onde meccaniche sopra il campo dell'udibilità (ultrasuoni). In base al materiale scelto avremo quindi diverse frequenze di ultrasuoni, diverse propagazioni nei materiali e quindi diverse caratteristiche di potenza della macchine generatrici

{ INDEX \e "

" \h "A" \c "2" \z "1040" }

{

PAGE **}**