

**UNA ADEGUATA SOLUZIONE PER SUPPORTARE LE FF.O.  
NEL CONTRASTO ALLE RAPINE**

IVO BENEDETTI  
*Mega Italia S.p.A.*

**1. LA SITUAZIONE**

Nell'ambito della normale attività delle Dipendenze periferiche delle Banche i rischi più importanti connessi alla Security sono da sempre quelli connessi alle rapine ed ai furti.

Iniziando dagli anni '80 e via via fino al giorno d'oggi l'A.B.I. ha svolto una continua e capillare attività di sensibilizzazione e coordinamento fra tutti gli Istituti di Credito, ottenendo così il risultato estremamente significativo di ridurre a valori molto bassi sia il numero sia, l'incidenza economica dei furti ai mezzi forti (caveaux, casseforti ecc.) e provocando in tal modo di fatto la scomparsa della cosiddetta "banda del buco" formata da professionisti dell'effrazione che, anche investendo notevoli risorse, puntavano a rubare valori ingentissimi sotto forma di gioielli, valuta, titoli ecc.

Analogamente il mondo bancario ha affrontato in modo omogeneo e compatto anche il rischio rapina, adottando numerose ed articolate misure difensive basate sia sul concetto di filtrare chi accede alle Dipendenze "tenendo fuori" i malintenzionati e le armi grazie alle bussole, ai metaldetector ecc., sia su quello di rendere "poco interessante" la rapina dal punto di vista economico, perché i valori disponibili negli sportelli sono stati ridotti al minimo, grazie ai sistemi di stoccaggio e/o distribuzione automatica dei contanti.

A tutto ciò si è sommato il notevole effetto deterrente dei sistemi di ripresa televisiva a circuito chiuso con videoregistrazione, che consentono spesso agli Inquirenti di individuare i malviventi e quindi di procedere nei loro confronti anche dopo l'evento.

L'adozione quindi di misure di sicurezza serie e professionali ha di fatto allontanato dalle Banche i malviventi altrettanto "professionali", riducendo al minimo anche questa tipologia di rischio, probabilmente trasferendola solo ad altri obiettivi meno protetti (gioiellerie, negozi, ecc.).

Purtroppo però sia il rischio di rapina sia quello di furto in Banca non è scomparso: si è solamente modificato tanto in termini di tipologia di malviventi quanto di obiettivi dell'azione criminosa.

Al posto cioè dei cosiddetti "professionisti", in Banca hanno cominciato ad effettuare rapine dei malviventi solitari, sbandati, drogati ecc. che superano i filtri di accesso perché sono armati solamente di temperini, cutters, siringhe sporche, finte bombe ecc., si accontentano di arraffare i pochi contanti disponibili nei cassetti aperti e non si curano delle telecamere perché non hanno nulla da perdere: è comparsa cioè la cosiddetta "microcriminalità".

Anche i furti non sono scomparsi, sono cambiati gli oggetti attaccati, non più i caveau e le casseforti bensì i Bancomat, specialmente posizionati fronte strada, che vengono letteralmente strappati dalla loro sede oppure aperti facendoli esplodere con il gas.

Anche questi atti pertanto sono diventati più simili alle rapine, perché effettuati in brevissimo tempo e senza curarsi dell'effetto dirompente (in termini di rilevazione e segnalazione dell'evento), del rumore e dei danni visibilissimi provocati.

In entrambi i casi le difese storiche delle Dipendenze bancarie risultano del tutto inutili.

Le Banche pertanto si sono trovate in questi ultimi anni a dover subire come ineluttabili tali "rischi residui" che però non possono essere considerati residui e/o trascurabili se si pensa alle conseguenze per le Persone (Dipendenti e Clienti) che subiscono le rapine ed ai notevoli costi connessi agli attacchi ai Bancomat.

Anche la tipologia dei malviventi da "microcriminalità" in realtà non ha nulla di piccolo, anzi in genere questi soggetti risultano essere molto più pericolosi, violenti e socialmente dannosi dei cosiddetti "professionisti".

## **2. INTERVENTI DIFENSIVI**

A fronte delle valutazioni di criticità appena ricordate, il mondo bancario ovviamente non è rimasto fermo ed ha cercato in questi ultimi anni di individuare ed adottare nuove strategie difensive, specificamente orientate a combattere anche queste evenienze.

Partendo dal concetto che probabilmente la microcriminalità non è destinata a diminuire ed anzi tenderà ad aumentare, per motivi sociali certamente non imputabili alle Banche (immigrazione incontrollata, disoccupazione, perdita di valori etici e morali ecc.) e tenendo conto che le difese classiche sono di fatto pressoché inefficaci, l'unica strategia che sembra percorribile punta a disincentivare i malviventi mediante forti deterrenti preventivi, strettamente correlati ad una decisa ed immediata azione repressiva, cercando di percorrere nuovamente, come nel passato, la strada del "trasferimento del rischio" su altri soggetti più deboli ed indifesi.

Nel concreto si è reso necessario tornare all'impiego dell'elemento umano, pronto ad intervenire per bloccare/reprimere appena l'evento si scatena, dando così al malvivente la quasi certezza di non rimanere impunito.

Visto cioè che non si può impedire l'attacco, farla franca dopo deve risultare quasi impossibile.

La quasi certezza che in Banca si possa venire bloccati ed arrestati deve quindi spingere i malviventi ad andare altrove.

La vigilanza armata che, soprattutto per motivi economici, negli anni passati era andata quasi scomparendo in Banca, sta tornando alla ribalta, magari modernizzata ed ottimizzata (supportata da nuove tecnologie), ma comunque basata sul concetto di un uomo che vede l'evento ed attiva immediatamente tutti i mezzi repressivi predisposti.

Il limite evidente di questa strategia, a prescindere dai costi rilevanti, è che gli Enti di vigilanza e le Guardie Giurate non possono sostituire i compiti istituzionali delle Forze dell'Ordine.

I tempi, le modalità ed i risultati degli interventi delle FF.OO. a seguito di rapina o attacchi ai Bancomat, sono estremamente più efficaci di qualsiasi intervento di Enti privati, anche efficienti ed organizzati.

L'ideale pertanto sarebbe di poter tornare ad affidare alle Forze dell'ordine i loro compiti istituzionali di protezione anche delle Banche e di repressione immediata ed efficace delle azioni criminose, ottenendo così anche delle importanti ricadute di carattere sociale.

Ovviamente non è pensabile di pretendere che le FF.OO. possono presidiare capillarmente le migliaia di Dipendenze bancarie, per ovvi motivi di organico ed organizzativi.

Ciononostante, è possibile ottenere un effetto molto prossimo al presidio puntuale, sfruttando la più moderna tecnologia oggi disponibile e trasferendo anche al mondo bancario un'idea già impostata e collaudata da alcuni anni in quello della piccola e media distribuzione.

### **3. L'INIZIATIVA SECURSHOP**

SECURSHOP nasce per mettere a disposizione della piccola e media distribuzione (orefici, farmacie, tabaccai, piccoli supermercati ecc.) uno strumento difensivo utile contro il rischio rapina, dopo che tali esercizi sono diventati più a rischio a causa proprio del trasferimento su di loro degli attacchi dalle Banche e con la diffusione della microcriminalità.

In estrema sintesi SECURSHOP consente il collegamento, via rete telefonica normale, dei negozi alle Centrali Operative delle FF.OO. mediante un apposito, piccolo ed economico sistema in grado di inviare in tempo reale sia gli allarmi rapina sia soprattutto le immagini di ciò che sta succedendo, con la possibilità di rivedere l'evento rapina registrato, consentendo così alle FF.OO. di verificare le situazioni, filtrare i falsi allarmi ed intervenire con la massima tempestività ed efficienza solamente nei casi di reale emergenza, con alta probabilità di arrestare il malvivente.

Inoltre solo le immagini utili vengono anche registrate localmente per gli usi giudiziari conseguenti.

L'iniziativa SECURSHOP è interessante perché consente, con estrema facilità, a costi bassi e con buona efficienza, di collegare siti periferici tecnologicamente disomogenei con le Centrali Operative delle FF.OO. facilitandone notevolmente il lavoro ed aumentandone l'efficacia.

Il punto di forza più importante di tale iniziativa consiste nel fatto che, in circa due anni, è stato attrezzato un grande numero di Centrali Operative SECURSHOP delle FF.OO. con gli apparati necessari per ricevere sia gli allarmi sia le immagini video (generate dagli apparati SECURSHOP periferici), creando così di fatto uno standard di interconnessione sia telecommunicativo sia soprattutto applicativo di compatibilità con le Forze dell'ordine.

Oggi le centrali di ricezione SECURSHOP posizionate presso le Centrali Operative delle FF.OO. sono a tutti gli effetti il gateway di collegamento tra il mondo esterno e gli organi istituzionali preposti all'intervento.

Si ritiene pertanto molto interessante valutare l'opportunità e la possibilità di utilizzare un'analoga logica periferica ed il medesimo gateway anche per la risoluzione nelle Banche del problema del rischio di rapina e furto da microcriminalità.

### **4. L'IDEA SECURBANK**

Come già detto nel precedente par. 1, le Banche, nella maggioranza dei casi, sono già attrezzate con impianti antirapina ed antifurto e con sistemi televisivi a circuito chiuso locali, praticamente sempre completati con dei videoregistratori (ormai molti digitali).

Inoltre spesso tutti questi apparati sono collegati a delle Centrali Operative (delle Banche stesse o della Vigilanza).

Tali Centrali Operative ovviamente non possono fare altro che prendere atto a posteriori degli eventi delittuosi avvenuti e qualche volta richiedere telefonicamente alle FF.OO. locali di intervenire, quasi sempre dopo che i malviventi si sono allontanati.

Poche Dipendenze bancarie hanno anche collegato punto a punto i loro impianti antifurto con le FF.OO., mentre praticamente nessuna può inviare le proprie immagini video alle C.O. di Polizia e Carabinieri, perché mancano di compatibilità.

SECURBANK nasce con l'obiettivo di trasferire la tecnologia di SECURSHOP alle Banche, sfruttando soprattutto il gateway già disponibile presso le numerose Centrali Operative delle Forze dell'ordine già attrezzate.

SECURBANK inoltre aggrega i contributi di tecnologia, esperienza e "know-how" di quattro primarie Aziende, operanti da molti anni nel settore della Sicurezza, ottenendo così un mix di servizi e prodotti fortemente integrati, capace di coprire tutti i settori nei quali spazia il progetto.

Le Aziende (in ordine alfabetico) partners nell'iniziativa SECURBANK sono le seguenti, presentate con i relativi contributi specifici nel progetto:

▪ Gruppo Beta Elettronica S.r.l.

Azienda con Sede a Treviglio (BG) produttore di apparecchiature e di soluzioni nell'ambito della sicurezza, specializzata nell'ambito TVCC e sempre attenta alle nuove esigenze di mercato. Produce la centralina CPU VS1, dispositivo periferico in grado di collegare gli impianti antirapina ed antifurto periferici preesistenti, i pulsanti via radio per l'invio degli allarmi aggressione e fino a n. 4/8/16 telecamere a colori e di inviare il tutto, opportunamente compattato e criptato alle Centrali Operative SECURSHOP delle FF.OO. sia via telefono (PSTN/GSM/GPRS ecc.) sia via rete Ethernet (Routers/Fastweb/ADSL ecc.).

Consociata di Securshop S.p.A. che ha provveduto ad implementare i centri di controllo, ad attrezzare le Centrali Operative delle FF.OO. ed a proteggere e collegare diverse migliaia di negozi distribuiti sull'intero territorio nazionale.

▪ Hewlett Packard (HP) S.p.A.

Azienda leader mondiale dell'informatica, ha realizzato il sistema AFIS (Automatic Fingerprint Identification System) per il Ministero degli Interni - Polizia scientifica.

Il sistema AFIS offre funzioni relative alla gestione (acquisizione, ricerca, memorizzazione ecc.) di impronte digitali, consentendo di automatizzare la gestione del casellario centrale di identità.

In questo ambito è in fase di ultimazione anche un gateway per la ricezione di impronte in formato standard provenienti da Enti esterni e la fornitura delle medesime a chi ne ha la necessità (il tutto ovviamente nel rispetto delle norme sulla privacy).

L'integrazione tra il sistema AFIS ed il BIODIGIT (che verrà illustrato più avanti) consentirà l'immediata individuazione e segnalazione delle impronte digitali di eventuali malviventi già schedati ed anche, in senso rovescio, il costante aggiornamento in tempo reale del data base del Ministero degli Interni.

▪ Mega Italia S.p.A.

Azienda leader italiano nei sistemi di sicurezza integrati e multifunzionali, ha copertura Nazionale ed è specializzata nella progettazione, installazione, configurazione e manutenzione dei sistemi di Sicurezza specialmente nelle Banche. Ha progettato la soluzione SECURBANK. Sarà responsabile dell'installazione dei sistemi periferici e soprattutto poi del loro mantenimento in perfetta efficienza.

▪ MESA S.r.l.

Azienda con sede ad Arezzo, facente parte del gruppo SAIMA, leader Nazionale nella realizzazione di bussole autogestite per ingresso alle Agenzie delle varie Banche e soluzioni ad hoc per il controllo accessi. Mesa produce il dispositivo BIODIGIT, il cui scopo è di registrare l'identità delle persone che accedono ad un ambiente protetto (passando nella bussola) attraverso la memorizzazione dell'impronta digitale di un dito associata ad una serie di immagini riprese da una microtelecamera posizionata all'interno della bussola.

Il sistema BIODIGIT è stato realizzato nel rispetto del documento "Linee guida per l'implementazione e la gestione dei sistemi di rilevazione cifrata delle impronte digitali" emesso dall'A.B.I. nel Febbraio 2004, a sua volta basato sul D.Lgs. 196/03 relativo alla protezione dei dati personali.

Per quanto riguarda poi l'impatto dell'iniziativa SECURBANK sulle Dipendenze periferiche delle Banche, ovviamente la loro situazione è diversa da quella dei negozi, perché quasi sempre vi sono già dei sistemi di Sicurezza preesistenti, che naturalmente dovranno essere salvaguardati.

Nella pratica si possono presentare le seguenti principali situazioni (salvo diverse varianti intermedie):

- Dipendenza priva di qualsiasi protezione: potrà essere applicata la soluzione base (vedi Par 5.1) o qualunque altra migliorativa.
- Dipendenza dotata di impianto antirapina/antifurto ma priva di TV/CC: potrà essere applicata la **soluzione mista con TV** (vedi Par 5.2) o qualunque altra migliorativa.
- Dipendenza priva di impianti antirapina/antifurto ma dotata di TV/CC: potrà essere applicata la **soluzione mista con antirapina** (vedi Par 5.3) o qualunque altra migliorativa.
- Dipendenza dotata sia di impianto antirapina/antifurto sia di TV/CC: potrà essere applicata la **soluzione integrativa base** (vedi Par 5.4) o migliorativa.
- Dipendenza comunque attrezzata ma valutata ad alto rischio: potrà essere applicata la **soluzione top** (vedi Par 5.5) completa di Antifurto/Antirapina/TV-CC/BIODIGIT.

Nel prossimo par. 5 si presenteranno sinteticamente le diverse aggregazioni di tipo sistemistico dei vari elementi che compongono la soluzione globale SECURBANK oggi disponibile.

## 5. SINTETICA DESCRIZIONE DELLE PRINCIPALI SOLUZIONI SISTEMISTICHE DI AGGREGAZIONE

Riprendendo le situazioni descritte al termine del precedente paragrafo, si riporta nel seguito una sintetica descrizione delle principali soluzioni sistemistiche oggi disponibili.

### 5.1 Soluzione base (Impianti completamente da realizzare)

Si prenda come riferimento lo schema a blocchi di Fig. 5.1, nel quale appare evidente che, per realizzare il Sistema, si dovranno prevedere alcune telecamere (**min n. 4, max n. 16**) da collegare all'unità di controllo e trasmissione CPU VS1 alla quale saranno connessi direttamente anche alcuni sensori antifurto/antirapina e che sarà in grado di ricevere via radio gli allarmi antirapina trasmessi da appositi piccoli dispositivi portatili, che dovranno essere, in prima ipotesi, tenuti indosso dal Personale.

L'attivazione di questi trasmettitori potrà essere manuale oppure in alternativa automatica mediante mazzette civetta, cassette allarmati ecc.

L'unità centrale CPU VS1 provvede poi ad inviare sia gli allarmi sia le immagini **video (al momento max 4)** alla Centrale Operativa delle FF.OO. attraverso un modem che impiega una qualsiasi delle tecnologie telecomunicative (elencate nel precedente Par. 4) disponibili in Agenzia.

### 5.2 Soluzione mista con TV/CC (Impianto TV/CC da realizzare)

Prendendo come riferimento lo schema a blocchi di Fig. 5.2 risulta chiaro che l'impianto è sostanzialmente identico a quello precedente, salvo che viene salvaguardato il preesistente impianto antifurto/antirapina, collegando la relativa centralina direttamente all'unità di controllo e trasmissione allarmi, la quale poi funzionerà in maniera del tutto identica a quanto già descritto nel precedente punto.

### 5.3 Soluzione mista con antirapina (Impianto antirapina/antifurto da realizzare)

Prendendo come riferimento lo schema a blocchi di Fig. 5.3 si può notare che l'impiantistica

antifurto/antirapina ed i relativi sensori sono nuovi e vengono collegati direttamente alla CPU mentre l'impianto TV/CC è già esistente e quindi viene mantenuto.

Devono essere solamente selezionate un massimo di n. 4 telecamere (installate nelle posizioni più idonee in ottica antirapina) ed esse saranno collegate, attraverso un distributore video passivo, oltre che al preesistente videoregistratore, anche alla nostra unità CPU di gestione e trasmissione, la quale poi funzionerà in maniera del tutto analoga a quanto già spiegato precedentemente.

#### **5.4 Soluzione integrativa base** (Nessun impianto locale da realizzare)

Si prenda come riferimento lo schema a blocchi di Fig. 5.4, nel quale sia l'impianto TV/CC sia quello antifurto/antirapina risultano già esistenti, per cui la nostra unità CPU di gestione e trasmissione sarà interfacciata alle telecamere ancora mediante un distributore video passivo ed ai sensori antifurto attraverso l'esistente centralina di impianto.

In questo modo tutta l'impiantistica preesistente verrà salvaguardata e si installeranno soltanto le componenti specifiche per l'interfacciamento con la Centrale Operativa delle FF.OO.

#### **5.5 Soluzione top SECURBANK** (Se vi sono degli impianti preesistenti vengono mantenuti ed interfacciati, altrimenti possono essere realizzati ex novo)

Esaminando lo schema a blocchi di Fig. 5.5 appare evidente che in questo caso l'unità di gestione e trasmissione CPU VS1 **viene integrata** nel sistema BIODIGIT, il quale è in grado di ricevere direttamente le immagini di un numero massimo di 8 telecamere (delle quali 2 utili per la memorizzazione dei transiti).

Il BIODIGIT è inoltre a tutti gli effetti anche un videoregistratore digitale, per cui diventa superfluo prevederne un altro in Agenzia.

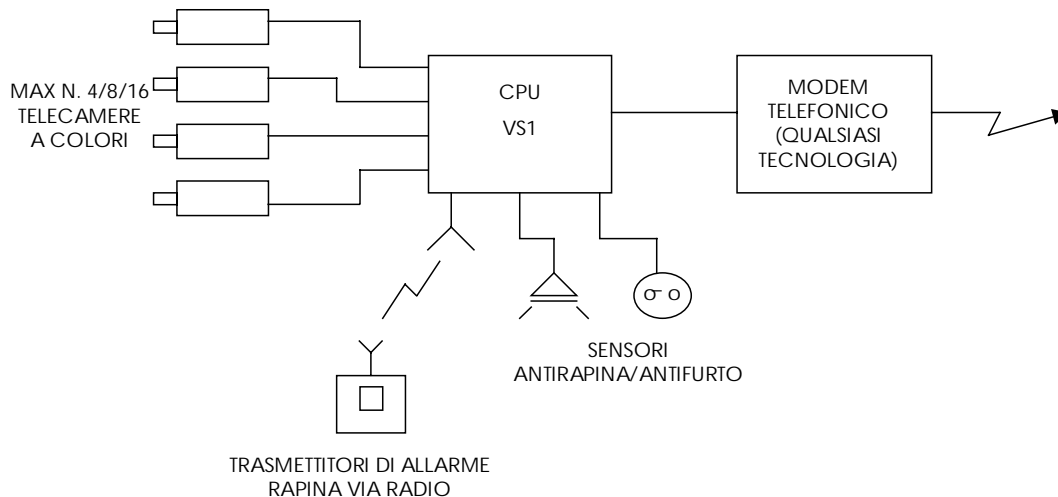
Al medesimo apparato è anche collegato un lettore di impronta digitale, previsto all'interno della bussola, il cui compito è di rilevare le impronte delle Persone in transito ed accoppiarle alle relative immagini.

Il tutto (**immagine e impronte**) in caso di evento criminoso potrà essere trasmesso **attendendosi alle direttive del garante (se richiesto)** alle FF.OO.

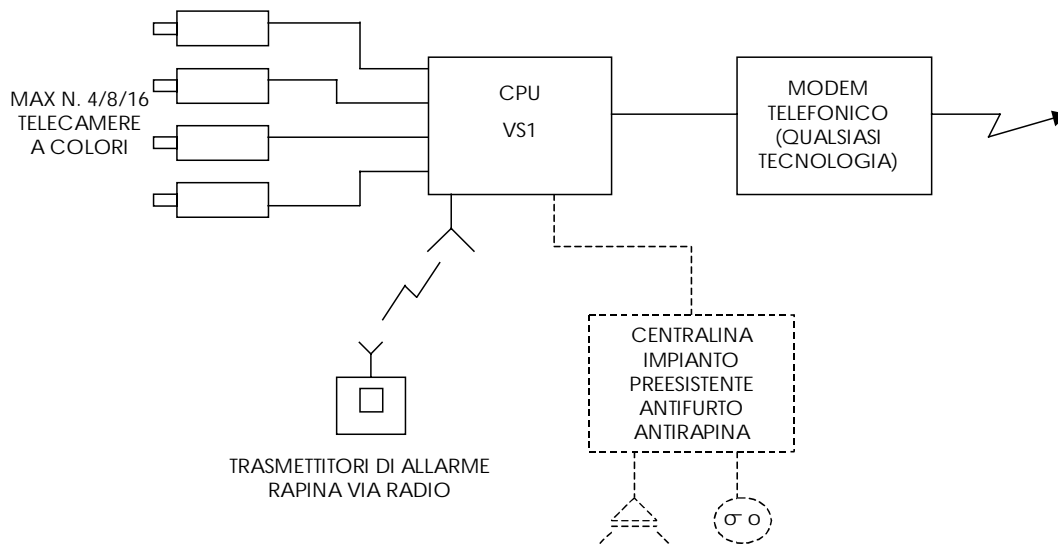
Anche l'impianto antifurto/antirapina eventualmente preesistente può essere direttamente collegato al BIODIGIT oppure, se risulta mancante, è possibile installarne uno nuovo.

Il BIODIGIT collegherà poi anche il trasmettitore via radio di attivazione dell'allarme ed invierà tutti i suoi dati alla Centrale Operativa delle Forze dell'ordine impiegando, analogamente ai casi precedenti, qualunque tecnologia telecomunicativa disponibile presso la Dipendenza periferica.

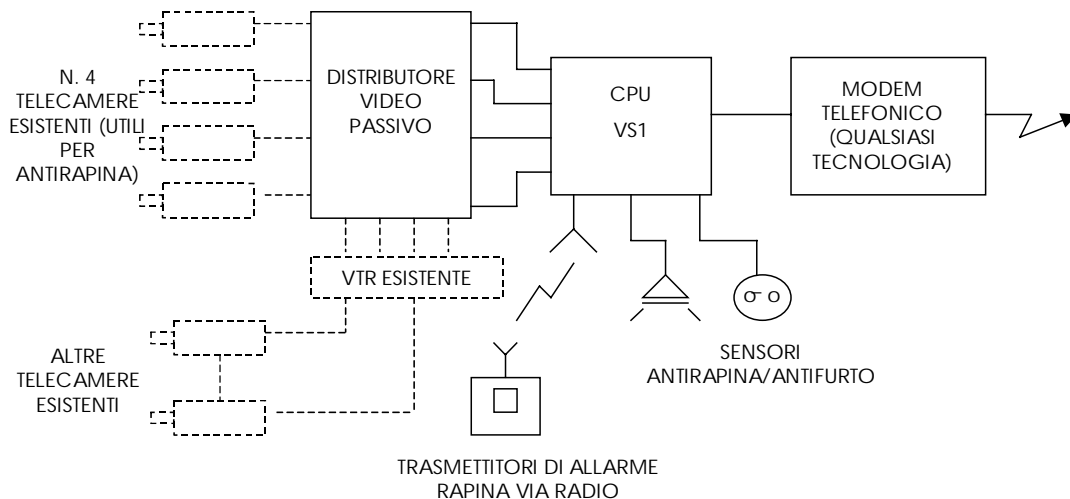
**FIG. 5.1) SOLUZIONE BASE (IMPIANTO COMPLETAMENTE DA REALIZZARE)**



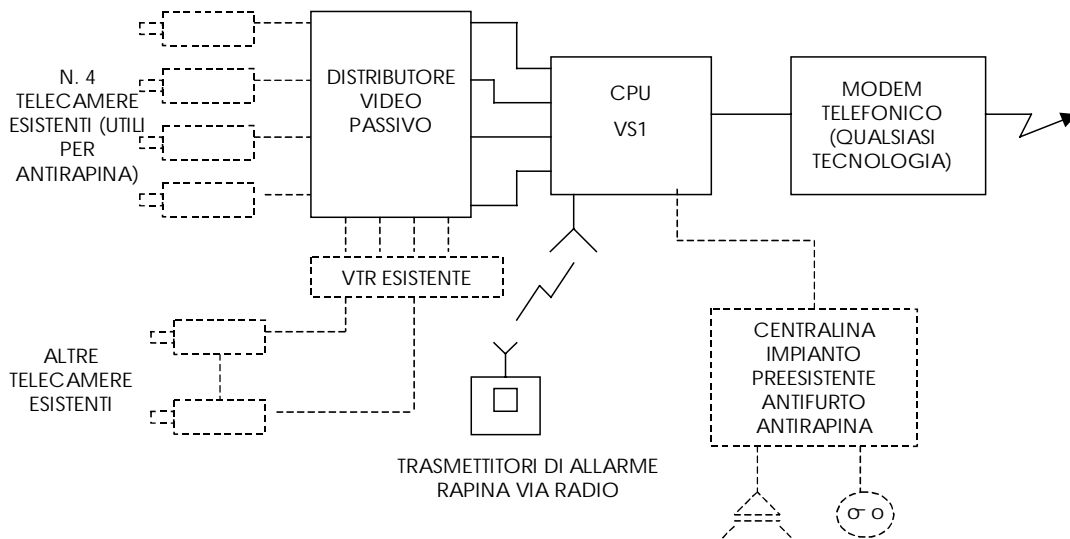
**FIG. 5.2) SOLUZIONE MISTA CON TV/CC (IMPIANTO TV/CC DA REALIZZARE)**



**FIG. 5.3) SOLUZIONE MISTA CON ANTIRAPINA (IMPIANTO ANTIRAPINA/ANTIFURTO DA REALIZZARE)**



**FIG. 5.4) SOLUZIONE INTEGRATIVA BASE (NESSUN IMPIANTO LOCALE DA REALIZZARE)**



**FIG. 5.5) SOLUZIONE TOP (SE VI SONO IMPIANTI PREESISTENTI VENGONO MANTENUTI ED INTERFACCIATI)**

