

BANCASICURA[®] 98

VIII° Convegno nazionale sulla sicurezza nelle Banche

Bologna, 12-13 febbraio 1998

Quartiere fieristico

CENTRALIZZAZIONI BANCARIE, A CHE PUNTO SIAMO ?

L'esperienza dei CICAL (<i>G.M. Rossi</i>)	2
Le scelte della Banca Popolare di Novara (<i>R. De Rosa</i>)	4
L'esperienza della Banca di Roma (<i>G. Rinaldi - A. Frabotta</i>)	7
L'esperienza della Banca Agricola Mantovana (<i>E. Rossett</i>)	10

L'ESPERIENZA DEI CICAL E LE PROSSIME REALIZZAZIONI

ING. GUIDO M. ROSSI

IDESI S.r.l.

Prima di riportare qualche notizia circa l'avanzamento dei progetti CICAL nel nostro Paese, ritengo sia utile introdurre qualche considerazione più generale a proposito dell'argomento di questa tavola rotonda, facendo il punto della situazione delle centralizzazioni bancarie dal mio osservatorio di consulente e progettista di tali sistemi.

Innanzitutto penso di poter affermare che ormai è assolutamente consolidato in Italia il concetto che la sicurezza bancaria non è tale se gli apparati periferici non sono collegati in qualche modo con una Centrale Operativa presidiata 24 ore su 24.

Il disegno generale di come dovrebbero essere realizzati i sistemi di sicurezza bancari è ormai chiaro per tutti.

Ciò non significa però che poi tutte le banche siano già allineate a tale standard per i seguenti principali motivi:

- non è per tutti evidente quale sia la soluzione migliore dal punto di vista tecnico, operativo e di sicurezza (collegamento alla Vigilanza, centrale operativa propria, collegamento a centrali operative consortili multibanca, ecc.) per cui spesso incontriamo banche che ritengono di essere adeguatamente attrezzate, mentre invece hanno adottato soluzioni del tutto inadeguate, specialmente dal punto di vista della sicurezza (ad esempio impiegano ancora i vecchi combinatori telefonici, ecc.).
- Attualmente il fattore **costi**, sia di investimento che di gestione, è assolutamente preponderante in banca (per i ben noti problemi generali del settore) per cui si tende a scegliere la soluzione a prima vista più economica, senza riuscire (spesso anche per inesperienza specifica di chi deve valutare) a discriminare e quindi pesare i reali costi complessivi e poliennali di ogni alternativa.

Il mondo bancario italiano della sicurezza quindi si è diviso in tre grandi categorie:

- banche che hanno ormai compreso e sposato la logica della centralizzazione e che hanno adottato da tempo dei Sistemi (in molti casi sono già alla seconda generazione) anche molto complessi e sofisticati di tipo:
 - proprietario
 - consortile multibanca;
- banche che non hanno ritenuto economicamente praticabile la realizzazione di sistemi proprietari/consortili o che non hanno ancora preso una decisione definitiva in tal senso, pur però sapendo che tale soluzione è l'obiettivo da perseguire, per cui, nel frattempo, hanno attivato collegamenti sufficientemente sofisticati con Enti di Vigilanza locali o con altre Organizzazioni analoghe e sostengono dei costi anche notevoli;
- banche che non dispongono al loro interno di sufficiente esperienza per analizzare criticamente la situazione, per cui credono di essere ad un sufficiente livello di sicurezza, mentre invece sono attrezzate in maniera inadeguata.

* * * * *

Le iniziative CICAL (Consorti Interbancari per la Centralizzazione degli Allarmi) patrocinata dall'ABI, si inseriscono nello scenario sopra descritto, al servizio di tutte e tre le categorie di banche elencate.

Entrando quindi più direttamente nel vivo dell'argomento affidatomi, posso confermare che ormai da diversi anni l'ABI ha attivato e sta perseguendo con tenacia un progetto per la realizzazione di un numero sufficiente di Consorzi Cical, per coprire alla fine l'intero territorio nazionale. Ad oggi la situazione è la seguente.

CICAL 1

(Piemonte, Valle d'Aosta, Liguria e parte della Lombardia) è operativo da diversi anni ed è addirittura in fase di passaggio alla seconda generazione di sistema di centralizzazione, in collaborazione con Cedacri Ovest.

CICAL 2

(Emilia Romagna, Toscana e parte della Lombardia) è operativo da pochi mesi e sta attivando a tappeto i collegamenti delle dipendenze delle banche socie.

CICAL 3

(Lombardia) dopo il termine dello studio di fattibilità e del progetto, si è ritenuto preferibile, per motivi di costi e di copertura territoriale, sospenderne la concreta attivazione, distribuendo le banche interessate su Cical 1 e Cical 2.

CICAL 4

(Puglia e prossimamente Basilicata e Calabria) sono terminati lo scorso anno lo studio di fattibilità ed il progetto esecutivo; si è in fase di messa a punto, con la O.S.C. di Bari, di un sistema dimostrativo per attivare dei collegamenti pilota di diverse banche interessate all'iniziativa.

Il piano dell'ABI prevede che il resto del territorio nazionale venga coperto nei prossimi anni con alcuni altri Consorzi analoghi, in modo da rendere disponibile, per tutte le banche operanti nel nostro Paese, un servizio al medesimo livello tecnologico e di sicurezza.

Le difficoltà che i CICAL hanno dovuto superare negli anni sono state veramente enormi e possono essere riassunte nelle seguenti categorie:

- necessità di standardizzazione dei protocolli di telecomunicazione di tutti gli apparati periferici (protocollo CEI 79/5 e 79/6),
- problemi di telecomunicazione (tecnologie Argotel, ISDN canale D, ecc.),
- difficoltà di far comprendere e toccare con mano alle banche i reali risparmi ottenibili, a fronte di un servizio qualitativamente superiore.

Le prospettive future delle iniziative Cical sono molto interessanti perché, precorrendo i tempi, si sono poste nell'ottica, attualmente giudicata la sola strategia vincente, di porre in *outsourcing* tutti i servizi non *core business* delle Banche, mettendo a disposizione delle medesime delle organizzazioni, consolidate e con grande know-how, capaci di assumere la responsabilità globale della gestione della sicurezza di tutti i punti periferici importanti.

Termino dicendo che tutto questo processo sta evolvendosi ulteriormente, proprio negli ultimi tempi. ABI e SIA stanno attivando un processo evolutivo con l'obiettivo di integrare sia i Cical tra di loro, sia le banche che hanno dei sistemi proprietari, nell'ambito di un unico sistema di rete generale, al fine di ottimizzare quindi le risorse umane necessarie e che sono quelle che costano (cioè gli uomini di centrale operativa, per capirci), nell'ambito di tutto il territorio nazionale. Questo è un progetto molto grosso, ambizioso e anche complesso per l'aspetto tecnico.

ABI e SIA ci stanno lavorando, cercando di sfruttare tutte le sinergie possibili: quindi ABI per l'esperienza e il know how acquisito e SIA per le capacità tecniche e per la rete di cui già dispone, che è la rete interbancaria. L'obiettivo: una ottimizzazione generale che porti alla ulteriore riduzione dei costi che, in questo momento, nell'ambito dei consorzi, sono i costi di gestione.

LE SCELTE DELLA BANCA POPOLARE DI NOVARA

DOTT. ROBERTO DE ROSA

Capo Ufficio Sicurezza Aziendale Banca Popolare di Novara - Socio A.I.P.S.A.

E' necessario innanzi tutto fare un'analisi corretta dei problemi, per vedere quali sono le soluzioni che portano effettivamente ad avere risposte adeguate. La prima cosa da fare è capire l'importanza della centralizzazione: centralizzazione significa dare ad un sistema la coscienza. Senza centralizzazione il sistema è incosciente.

In quest'ultimo periodo le banche stanno trasformando l'operatività di sportello, passando da un terminale limitato nella sua operatività, con un programma prefissato, ad un c.d. "terminale intelligente", con un'operatività differenziata in diversi settori. Grazie a questa più ampia operatività l'operatore ha la possibilità di esprimere le proprie capacità professionali in maniera più completa. Si dà anima all'operatore che prima doveva solo viaggiare sul proprio binario. Sono tutte soluzioni che permettono di migliorare l'operatività ed acquistarne coscienza, sapere cosa si sta facendo e non essere indirizzati su un binario da percorrere ad occhi bendati.

Il 25 gennaio 1995 si teneva presso il Centro Space dell'Università Bocconi, in collaborazione con AIPSA, un convegno sugli "Aspetti qualificanti della centralizzazione allarmi in ambito bancario e industriale".

Partecipai ai lavori con una relazione sul tema della "Configurazione fisica di una centrale di supervisione. La componente umana e l'incidenza delle norme procedurali" (cfr. Atti del Convegno pagg. 49-65).

Di particolare rilievo il dibattito che venne riportato negli atti del Convegno con l'amico Gianfranco Bonfante, organizzatore del Convegno stesso, in ordine all'impiego di personale proprio o di terzi per la gestione di una centrale di supervisione.

Di fonte alla legittimazione di una scelta di *outsourcing*, espressa da parte mia e derivante dall'adesione all'iniziativa dell'ABI per la costituzione di Consorzi Interbancari Centralizzazione Allarmi - Cical, l'amico Bonfante evidenziò gli aspetti negativi dell'affidamento a terzi di attività che, per loro natura, dovevano rimanere riservate; prospettò le difficoltà derivanti dalle disposizioni vigenti, con particolare riferimento al TULPS (art. 134), che ostacolavano la terzizzazione del servizio e, anche in un'ipotesi di struttura consortile, con consorzi a mera attività interna, mise in rilievo gli ostacoli di rilevante incidenza giuridico-operativa che avrebbero impedito il successo dell'iniziativa:

- per le implicazioni delle adesioni e dismissioni dei soci;
- per il rilascio delle autorizzazioni prefettizie di P.S.;
- per l'impiego di un vettore trasmissivo comune per tutti gli utenti;
- per le difficoltà di armonizzare esigenze diverse.

A distanza di tre anni la situazione appare capovolta: non solo il Consorzio Cical 1 ha raggiunto la piena operatività, con una componente procedurale di grado elevato ed una gestione articolata con risorse umane interne ed esterne, ma si profila addirittura un'esplosione del fenomeno di *outsourcing* che comporterà la nascita di rapporti sempre più diversificati di *joint venture* tra utenti e fornitori.

L'ultima stesura dello statuto consortile di Cical 1 ha, fra l'altro, inserito la possibilità di adesione da parte di soggetti diversi da banche o istituzioni finanziarie, creando, in tal modo, l'occasione favorevole per instaurare rapporti maggiormente collaborativi fra le diverse componenti della security:

- manager e addetti alla security aziendale;
- società di engineering e tecnici realizzatori e manutentori di sistemi;
- Istituti di vigilanza.

Fra i punti di forza di Cical, già ampiamente illustrati dall'Ing. Rossi, voglio sottolineare i seguenti:

- la determinazione di procedure armonizzate in maniera uniforme fra i Soci, per tutte le componenti, aziendali, consortili ed esterne, che intervengono nella gestione di un sistema centralizzato;
- la definizione di un protocollo di comunicazione standard - CEI 79/5 - che ha finalmente affrancato l'utente dal vincolo di un protocollo proprietario;
- la maggior rilevanza dell'utenza, riunita in consorzio, nei rapporti con l'Autorità di P.S. e con le altre componenti della security.

Il consorzio Cical 1 ha rappresentato una palestra di incontri e di discussioni che ha consentito l'approfondimento di problematiche spesso ignorate a casa propria.

Le adesioni e dismissioni di Soci che si sono succedute nel tempo non hanno mai messo in crisi l'attività o la sopravvivenza dell'istituzione, anzi hanno arricchito con ulteriori esperienze il *know how* del Consorzio, che vanta ormai un patrimonio di conoscenze tecniche, metodologiche, giuridiche, amministrative e contabili di rilevante importanza e comunque, tali da garantirne una lunga e proficua attività.

Le contrastanti interpretazioni prefettizie scontano le divergenze interpretative delle disposizioni del TULPS, ormai datate, nelle quali si vogliono far entrare, ad ogni costo, fattispecie non previste né prevedibili dal legislatore.

In ogni caso, la Direzione del Consorzio, utilizzando le proprie risorse, sia interne sia esterne, ha saputo mettersi al riparo dagli interpreti giù restrittivi, portati ad estendere l'ambito dell'ordine pubblico nella sfera privatistica, salvo poi lasciarla priva di tutela.

La scelta del vettore trasmissivo non ha costituito un ostacolo alla centralizzazione, salva la necessità di adottare da parte dei soci scelte compatibili con le caratteristiche tecnico-operative del sistema.

Causa del notevole ritardo nella realizzazione ed estensione del sistema è stata indubbiamente la politica commerciale dell'azienda che gestisce le linee telefoniche, prima SIP ora TELECOM, che ha commercializzato, anni fa, per la centralizzazione allarmi, le linee "Argotel", ancor prive di adeguate caratteristiche di sicurezza e non idonee allo scopo.

Successivamente, nel momento in cui si sono risolti i problemi tecnici, le linee "Argotel" sono state dichiarate non più disponibili, per una scelta politica rivolta alla diffusione delle linee ISDN che, allo stato dei fatti, per carenze della disponibilità tecnica delle linee o delle conoscenze professionali degli addetti ai lavori risultano tuttora "in lista di attesa."

Finalmente, superate le difficoltà di natura tecnica e giuridica, saremo in grado di confrontare le diverse tipologie di sistemi centralizzati, proprietari o terziarizzati, gestiti con personale proprio o affidati a terzi, in termini di efficienza, sulla base degli elaborati statistici, ed in termini di costi e benefici, sulla base delle conseguenze derivate sul conto economico degli utenti, cifre alla mano e non con generici richiami alla economicità, per una dichiarata impossibilità, da parte di alcuni assertori della centralizzazione, di affrontare una impostazione algebrica del confronto costi-benefici.

Così come ci esprimevamo nel Convegno del 1995, ribadiamo che "ciascuna azienda è libera di esercitare il controllo sui propri impianti nella maniera più confacente alle proprie esigenze, con strutture e risorse proprie, consortili o di terzi, purché utilizzi risorse qualificate e mezzi tecnici idonei, in grado di soddisfare pienamente le esigenze di sicurezza evidenziate dall'utente finale".

Resta il problema della qualificazione che, sul piano privatistico, trova soluzione nella certificazione delle aziende fornitrici, dei processi e dei prodotti e, sul piano pubblicistico, necessita di una normativa aggiornata, dal punto di vista giuridico-legale, al dettato costituzionale ed alla normativa europea in corso di elaborazione e, dal punto di vista effettuale, alle esigenze di servizi con prestazioni complesse e di sistemi di avanzata tecnologia, necessari ad assicurare l'efficienza e la competitività di ciascuna azienda fruitrice.

L'ESPERIENZA DELLA BANCA DI ROMA

ING. GENNARO RINALDI - GEOM. ALBERTO FRABOTTA

Banca di Roma

(trascrizione da audioregistrazione)

La Banca di Roma ha portato avanti, in questi ultimi anni, un progetto abbastanza complesso, forse anche ambizioso, la cui prima fase è ormai conclusa.

Facciamo però un passo indietro. La Banca di Roma, com'è a tutti noto, nasce dall'unione di tre Istituti di credito che, ovviamente, avevano ciascuno una propria impiantistica, delle proprie norme operative, i propri criteri di sicurezza. Ognuno era strutturato in un certo modo, in particolare il Banco di Santo Spirito e la Cassa di Risparmio di Roma, che erano delle realtà locali, già dalla fine degli anni 70 avevano dei loro sistemi di centralizzazione, territorialmente limitati che quindi utilizzavano linee punto-punto di un certo costo, e che collegavano soltanto le agenzie di Roma e dell'immediata provincia.

Con la fusione dei tre istituti la realtà è completamente cambiata: una presenza capillare su tutto il territorio nazionale, e quindi è sorta la necessità di identificare in tempi rapidi una soluzione che potesse consentire un controllo dello stato degli impianti di sicurezza di tutte le agenzie. Abbiamo quindi dovuto individuare una soluzione che tenesse conto degli investimenti fatti e non cambiasse tutto completamente, perché non potevamo permetterci il lusso, con le problematiche connesse al contenimento dei costi, di fare tutto ex novo.

In questi ultimi due anni abbiamo quindi utilizzato la rete Telecom per collegare tutti gli impianti di allarme ad un nostro centro. Abbiamo utilizzato un dispositivo esistente sul mercato (Ademco) che ci dava particolare affidamento. Installato in tutte le agenzie è stato poi interfacciato ad un'apparecchiatura centrale, per cui siamo riusciti a trasferire al centro 7-8 criteri che ritenevamo interessanti o particolari.

Già in questa prima fase abbiamo assicurato un certo livello di sicurezza, prescindendo tuttavia dall'affidabilità vera e propria della rete. E questa prima fase del progetto è così praticamente ultimata, dopo averci lavorato per buona parte del '96 e per tutto il '97.

La seconda parte del progetto, immediatamente a seguire, dovrebbe - salvaguardando il centro, che è stato predisposto per interfacciare qualsiasi tipo di rete - consentire il passaggio alla rete X25 (la rete aziendale) e quindi sfruttare questo tipo di rete per centralizzare le informazioni di sicurezza.

Il progetto è ancora più ambizioso perché, nel medio termine, vorremmo anche collegare e tenere sotto controllo non soltanto gli impianti di sicurezza, ma anche l'impiantistica in senso lato delle agenzie, quindi impianti tecnologici, impianti elettrici, di condizionamento, insegne luminose ecc.

Questo perché la nostra centrale, gestita da uomini dell'azienda, nelle nostre intenzioni, filosofia dovrebbe costituire l'*help desk* di tutte le installazioni impiantistiche e di sicurezza, quindi di tutte le realizzazioni tecnologiche della rete.

Ovviamente il progetto è stato ed è di una certa complessità, perché non consisteva solo in un intervento tecnico, di implementazione od installazione di nuovi apparati d'allarme. Contestualmente, si sono dovuti effettuare interventi per l'aspetto organizzativo, interventi con gli istituti di vigilanza.

Abbiamo dovuto razionalizzare tante cose, individuando una nuova filosofia comportamentale

e prevedendo anche nuovi servizi, conseguenti alla necessità di dover installare degli apparati anche presso gli istituti di vigilanza, sui quali "rimbalziamo", attraverso il nostro centro, l'impianto d'allarme. Quindi è stato necessario il perfezionamento di una nuova e diversa contrattualistica con gli istituti di vigilanza per la tenuta chiavi (di accesso e dell'impianto), ottimizzando nel contempo questo tipo di interventi. E questo per fare in modo che l'intervento di verifica da parte dell'Istituto di vigilanza avesse luogo in un tempo quanto più prossimo al tempo reale del nostro controllo e per far sì che l'impianto potesse essere ripristinato nel più breve tempo possibile, tornando così alle condizioni iniziali di sicurezza.

In simile contesto possiamo anche ottimizzare gli interventi di manutenzione, possiamo monitorare gli interventi delle ditte incaricate (abbiamo contratti full, e quindi interventi 24 ore su 24), e possiamo agire in maniera preventiva, perché possiamo controllare lo stato degli impianti, ed abbiamo quindi un minor numero di interventi.

La centralizzazione per noi ha significato dunque un intervento a largo raggio di revisione della sicurezza. Si è dovuta creare anche una certa cultura nella rete, quindi nel personale, attraverso i corsi che sono stati fatti e che sono serviti a divulgare le conoscenze minime basilari per intervenire, per mantenere il livello di sicurezza.

Abbiamo fatto questa scelta perché era necessario, per la nostra capillarità di diffusione sul territorio, che avessimo una omogeneità di intervento sia dal punto di vista tecnico, sia dal punto di vista normativo, su tutte le agenzie. In questo modo, avendo un'unica centrale strettamente connessa a noi, perché in linea gerarchica dipende dalla sicurezza, abbiamo il controllo in tempo reale di tutte le situazioni.

Tra l'altro è stato necessario creare anche un servizio di reperibilità (personale direttivo): gli addetti alla centrale, che operano con turnazioni sulle 24 ore, in caso di necessità possono avvalersi dell'intervento di alcuni funzionari, reperibili nelle 24 ore, per particolari decisioni.

* * * * *

Per la diversa tipologia di impiantistica presente nelle tre banche, non è stato facile individuare una modalità unica che consentisse di accentrare tutti i segnali che venivano dalle periferie. Abbiamo individuato un apparato, installato nel corso del 96-97 presso ogni impianto periferico. Ciò ci consente oggi di accentrare su rete commutata ben otto segnali, individuati quali più significativi.

Il problema non era tanto quello di fare arrivare al centro le segnalazioni, perché in un modo o nell'altro arrivano, anche se la rete commutata non presenta grandissima affidabilità, bensì quello di creare un centro in grado di ricevere le informazioni, ma soprattutto di gestirle dal punto di vista operativo.

Uno specifico software di gestione tratta le segnalazioni in arrivo e le presenta su tre monitor, a disposizione degli operatori della centrale. I monitor sono tre perché, per il gran numero di agenzie, abbiamo ritenuto opportuno prevedere nella configurazione attuale una ripartizione del territorio in tre parti: una zona nord, una zona sud ed una zona Roma e Lazio. Ovviamente i tre monitor possono essere intercambiabili ed è anche possibile, in caso di necessità, indirizzare automaticamente tutte le segnalazioni su un monitor solo o su due.

Ci sono poi degli accorgimenti di visualizzazione differenziata (per colori) in relazione alla situazione e sono previste elaborazioni statistiche, utili anche per gestire sia la manutenzione che l'impianto in quanto tale.

Gli operatori operano in base a normative precise che impongono la gestione degli eventi che si conclude con la scheda dell'intervento.

Tutto ciò che viene dalla periferia genera automaticamente una scheda di evento che in parte è anche "intelligente", ovvero va in autocompilazione in relazione al tipo di evento che perviene. La scheda contiene dati significativi, come gli indirizzi dei responsabili, ed è anche interattiva, perché dai campi che racchiudono le numerazioni telefoniche l'operatore può effettuare direttamente la telefonata per mettersi in contatto con l'agenzia.

Tutto questo viene trasferito in modo automatico, dopo una certa ora, agli istituti di vigilanza convenzionati per il pronto intervento. Gli istituti di vigilanza ricevono queste informazioni in chiaro su rete commutata.

Il tutto, integrato anche dalla possibilità che gli operatori hanno di portare a video le planimetrie dei locali, quindi dal pannello che loro hanno dell'agenzia, nel quale sono riportati i segnali trasferiti. Hanno anche un pulsante per richiamare la planimetria, sulla quale sono evidenziati tutti i sensori e tutte le parti che si ritengono più a rischio, quindi anche guidare l'intervento della vigilanza in determinati punti.

Tutte queste cose rendono il sistema abbastanza complesso, sia dal punto di vista tecnico che dal punto di vista operativo.

La macchina del centro è in grado già da adesso di acquisire altri sistemi di trasmissione, e quest'anno avremo la possibilità di portare sulla rete aziendale X25 tutti questi segnali che rimarranno come backup, ed integreremo i sistemi di allarme con altri sistemi di sicurezza, anche quelli impiantistici. Questa rete ci consentirà anche l'interattività con la periferia, e quindi il comando dal centro su determinati impianti o su altri sistemi di sicurezza.

L'elaboratore che gestisce il centro è un unico elaboratore, al quale fanno capo i tre posti operatori, e potranno essere poi integrati con altri posti con specificità.

Per quanto attiene ai costi, c'è da precisare che partivamo da un'impiantistica periferica in massima parte esistente e quindi gli investimenti sono stati abbastanza modesti, nell'ordine di circa 200 milioni per i soli apparati di centrale.

E' ovvio che parlando di un progetto ambizioso, e che quindi ha mosso tutte situazioni di contorno, nell'ambito di questa completa ristrutturazione sono andati in porto anche altri tipi di progetto, come l'ammodernamento degli impianti periferici. Questo però non fa parte del progetto di centralizzazione, che comunque è stato di spinta per ammodernare un parco "impianti" di allarme che in qualche caso risaliva agli anni settanta e perciò poco affidabile.

Per quanto riguarda i costi annuali di gestione, in centrale sono presenti (per turni) sedici operatori, per cui direi che siamo nell'ordine 1,5 miliardi di costo del personale. Il costo di manutenzione degli apparati di centrale è stato (nel 1997) di circa sessanta milioni. Altro costi non ce ne sono, perché la manutenzione degli impianti periferici comunque andrebbe fatta. Il costo totale quindi è di poco superiore ad 1,5 miliardi l'anno, e cioè circa 1,2-1,3 milioni a punto operativo (circa 1300 agenzie).

L'ESPERIENZA DELLA BANCA AGRICOLA MANTOVANA

ENRICO ROSSETTI

Banca Agricola Mantovana

La decisione di acquisire un sistema di centralizzazione allarmi in Banca Agricola Mantovana è stata presa nel corso del 1993.

C'erano stati approcci, in precedenza, al sistema CICAL per verificarne i contenuti funzionali ed economici ma proprio i costi ci spinsero a cercare altre soluzioni.

A quel tempo la Banca Agricola Mantovana disponeva di :

- un Centro Controllo Sicurezza con guardie proprie
- impianti di allarme, nella maggior parte, da rivedere o migliorare e un certo numero di nuove centrali, di tipo centralizzabile, fornite da due differenti produttori.
- un sistema informatico con un sistema Host IBM e rete di trasmissione dati tipo SNA

I *must* per la acquisizione di un impianto di centralizzazione allarmi dovevano essere:

- costi contenuti
- sicurezza delle trasmissioni
- utilizzo di centrali di allarme centralizzabili di fornitori diversi
- Sw applicativo e di gestione degli allarmi in linea con le norme CEI 79-5 CEI 79-6 , a quel tempo in fase "preliminare".

La proposta Regulus, adottata in seguito dal nostro Istituto, poggiava su un software innovativo che consentiva di realizzare un sistema centralizzato per il controllo e la gestione degli allarmi utilizzando le risorse HW e Sw rese disponibili dal settore Sistemi Informativi non richiedendo, quindi, l'inserimento di apparecchiature specializzate né di software non standard.

Ciò garantisce continuità, manutenzione meno onerosa, availability del sistema molto alta e una previsione di costi futuri di gestione molto bassi.

Il sistema "Guardian" interfaccia le centrali di allarme tramite un P.C. e, utilizzando la rete di trasmissione dati SNA, garantisce l'inoltro dei messaggi in parallelo con i dati di altre applicazioni in modo trasparente e sicuro.

Il sistema Guardian, dal punto di vista applicativo, pur utilizzando le strutture di base del sistema informativo, consente la totale e completa autonomia nel controllo e supervisione della sicurezza, in quanto la applicazione di gestione risiede interamente in ambiente client/server P.C. .

L'host viene utilizzato come "veicolo sicuro" per il trasporto dei messaggi tramite meccanismi di message switching.

Il sistema Guardian è, per quanto riguarda le periferiche, una soluzione Hardware independent.

Ciò ha consentito di collegare apparecchiature di fornitori diversi e di investire su Software in linea con le future evoluzioni del mercato della sicurezza.

Poiché la soluzione è in linea con le norme CEI 79, si offre la possibilità di aprirsi all'interfacciamento di altre centrali con costi aggiuntivi molto bassi per adattamenti o personalizzazioni .

Il Software di Guardian può essere diviso in tre moduli essenziali:

1. Guardian Campo - gestisce i messaggi da e per la centrale di allarme

2. Guardian Host - gestisce le code di messaggi tra Server e periferiche
3. Guardian Console - gestisce l'interfaccia operatore/sistema

Dal punto di vista del carico di rete le prestazioni sono ottime in quanto il Polling verso le centrali viene effettuato dal Guardian Campo .

Questo esegue anche le verifiche di congruenza degli eventi segnalati dalla centrale cui è collegato. Infine invia le cosiddette transazioni di vita ai server di supervisione.

In caso di richiesta dal sistema centrale, tutte queste verifiche vengono forzate consentendo una notifica in tempo reale dello stato.

Le caratteristiche principali della soluzione adottata si possono riassumere in:

- utilizzo della struttura di rete esistente
- ottimizzazione delle risorse di rete
- utilizzo dell'HOST in qualità di Router
- utilizzo di piattaforme tecnologiche standard sia in periferia che al centro
- interfacciamento a periferiche multivendor
- semplicità d'uso del sistema
- basso costo di gestione
- espandibilità funzionale del sistema

Infine la soluzione adottata in Banca Agricola Mantovana è stata completata con moduli software per la gestione del Backup.

Il meccanismo entra in funzione nel momento in cui venga a mancare un qualsiasi box Hardware o Software e il colloquio tra periferia e centro avviene tramite un'anormale linea telefonica commutata con l'utilizzo di un modem asincrono che deve rispettare gli standard CCITT V22 (1200 bps) o V22bis (2400bps) e deve essere in grado di eseguire il set base dei comandi HAYES.

In pratica le centrali di allarme sono corredate di modem che si attiva quando Guardian Campo non riesce ad interrogare la centrale e quest'ultima abbia necessità di inviare messaggi di allarme o notificare un abbassamento del livello di sicurezza del sistema di allarme.

I messaggi, inviati ad un collettore chiamato "Guardian FEP", vengono notificati alla console di sistema.

La soluzione applicativa prevede:

- Ricezione degli eventi inviati dal PC CAMPO nel caso di non disponibilità della rete geografica
- Invio dei comandi dalla console nel caso di non disponibilità della rete geografica - **opzione non attivata**
- Gestione della crittografia dei dati mediante algoritmo DES con generazione automatica delle chiavi - **opzione non attivata**

In questo modo si copre quell'1% di mancanza di disponibilità generale del sistema informativo dovuta a cambiamenti nel software di rete, di sw di base o manutenzione ..

Viene altresì coperta l'eventualità di mancanza di collegamento dovuta a interruzioni di corrente in quanto il modem è a bordo della centrale.

Alla data i 3/4 delle nostre dipendenze sono collegate al sistema Guardian e, secondo un piano elaborato suo tempo, completeremo la connessione delle rimanenti agenzie entro l'anno corrente.

I tempi medi di risposta tra periferia e centro sono pari a 5-6 min/sec. in condizioni normali, con un ritardo massimo di 19 sec., nei momenti di punta su tratte con forte traffico di dati.

Dall'analisi dei dati statistici abbiamo potuto rilevare

- il bassissimo impegno richiesto al sistema centrale che viene impegnato per poche decine di secondi nel corso di un'ora;
- il traffico, nel rispetto delle velocità disponibili, è al di sotto di qualsiasi soglia di attenzione;
- nella maggior parte dei casi, si tratta di notifiche di cambio di stato (inserimenti-disinserimenti) o attività dei poller da/per la periferia.

Termino con i costi. Ho fatto un piccolo paragone con De Rosa: lui dice 4 milioni, noi quest'anno dovremmo essere intorno ai tre, con 200 filiali.

Il nostro sistema centrale non prevede dei supporti informatici di una certa rilevanza, ma sono dei PC in line, con un costo piuttosto basso. Quest'anno abbiamo previsto anche un *alterate* del software e dell'hardware, quindi contando anche queste modifiche e la manutenzione, arriviamo ad una spesa che è inferiore ai 600 milioni/annui.