Dispensa corso di aggiornamento

Intervento Ademco International sul tema:

Sistemi di gestione centralizzata per impianti di sicurezza multifunzionali (videosorveglianza, rivelazione incendio, antintrusione)

L’evoluzione tecnologica nel settore sicurezza

Lo scenario di riferimento

Negli ultimi decenni, si è assistito ad un progressivo sviluppo delle tecnologie informatiche, elettroniche, multimediali e ad una loro rapida diffusione nel mondo del lavoro e nella vita quotidiana.
Con il contributo delle tecnologie digitali, le conoscenze acquisite in questi settori convergono oggi in insiemi di prodotti e servizi che stanno cambiando radicalmente il nostro modo di vivere.
Gli strumenti professionali e gli oggetti di uso quotidiano, dagli elettrodomestici ai sistemi di sicurezza, dai semplici interruttori ai personal computer, arricchiranno le loro prestazioni di funzioni autonome ed intelligenti, e si adatteranno ad ogni nostra esigenza, trasformandosi in veri e propri elementi interattivi.

Dalle centraline ai software intelligenti

Nel campo specifico della sicurezza, le prime applicazioni delle nuove tecnologie risalgono alla fine degli anni Settanta, in particolare nel mercato della *building automation*, con i primi tentativi di supervisione dell’insieme dei processi attraverso la condivisione dei dati relativi ai singoli impianti.
Il controllo dei sistemi avveniva attraverso singole unità modulari di governo, centraline collegate ai vari tipi di sensori, con funzioni di segnalazioni locali e di attivazione interventi tramite linea telefonica.
Parallelamente, si sono sviluppati sistemi software di supervisione e gestione dei singoli componenti che, perfezionandosi nel tempo, hanno portato oggi ad un importante traguardo: la gestione centralizzata in tempo reale, con capacità di analisi e di controllo virtuali, di ogni periferica integrata nell’impianto, programmata e interfacciata con l’unità operativa.
Dalle unità centrali di controllo rappresentate da centraline programmabili e telegestibili, dotate di interfacce utente omogenee e dal facile utilizzo, nuove soluzioni vengono proposte sul mercato,

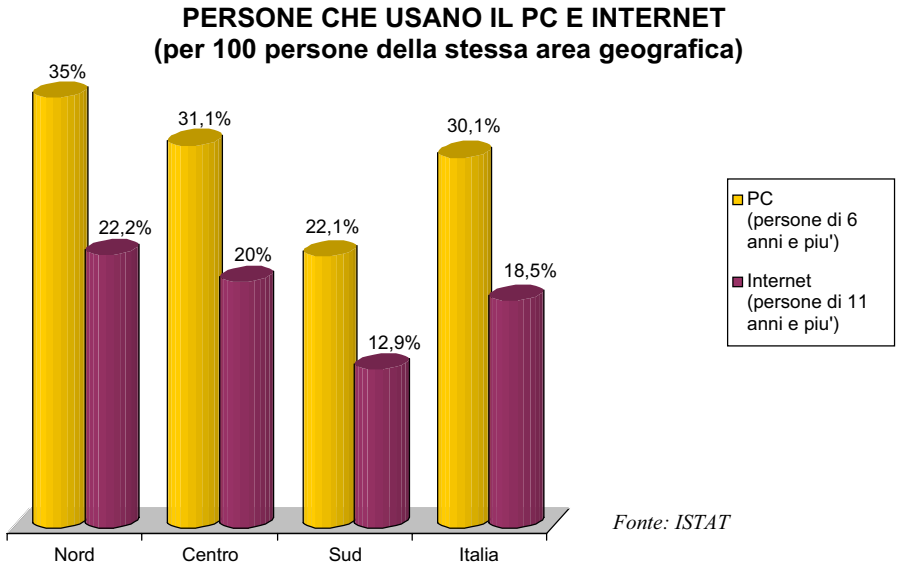
legate alla continua e incalzante evoluzione delle tecnologie in campo informatico, che facilitano e velocizzano l'operatività dei sistemi e del personale preposto al controllo.

Un esempio concreto è una componente del sistema di gestione centralizzata che negli ultimi anni ha acquisito grande importanza, **l'interfaccia utente**, parte del programma che gestisce l'interazione diretta con l'utente. Da un processo di interazione basato su comandi battuti su tastiera o tramite pulsanti, si è passati a interfacce grafiche che utilizzano simboli (rappresentati sullo schermo come icone) e che possono essere selezionati dall'utente con particolari strumenti di input (mouse, penne ottiche ecc.).

Il ruolo di Internet nelle prospettive di sviluppo

Grazie al progresso delle tecnologie digitali, delle telecomunicazioni e alla penetrazione dei PC nei nuclei abitativi, uno degli elementi chiave che molto probabilmente guiderà lo sviluppo dei sistemi integrati di centralizzazione sarà l'utilizzo di Internet e dei servizi forniti dalla rete, estremamente funzionali, accessibili, veloci, e di basso costo.

Basti pensare alle profonde trasformazioni già in atto in diversi settori quali il commercio, l'home banking, le informazioni on line (attraverso i cosiddetti "motori di ricerca"), l'intrattenimento, le comunicazioni (e-mail, chat), il telelavoro e la formazione (nel settore didattico, le proiezioni di crescita del Distance Learning e del Web Based Learning sono nell'ordine del 160% per i prossimi 5 anni).



Fonte: ISTAT

Il sistema integrato multifunzionale

Il concetto di sistema

Un sistema è costituito da un certo numero di elementi interdipendenti, uniti tra loro in modo omogeneo e ben strutturato.
Dal punto di vista ingegneristico, l'unione degli elementi di un sistema è definita "**connessione**": gli elementi sono collegati fra loro allo scopo di

a) interagire con i segnali provenienti dall'ambiente esterno (variabili di entrata)
b) rielaborarli in base alle proprie caratteristiche strutturali (grandezze fisiche interne, diverse da sistema a sistema e con un proprio modus operandi)

per il raggiungimento di un determinato risultato, la cosiddetta "risposta" del sistema.

I SISTEMI DI SICUREZZA

I sistemi di sicurezza relativi alla "**security"** (antintrusione, videosorveglianza, controllo accessi) e alla "**safety"** (antincendio) rispecchiano concretamente la struttura concettuale di un sistema.
Gli input ricevuti dall'esterno (es. un tentativo di effrazione) vengono elaborati dai vari sensori che inviano alla centrale una variazione di stato.
La risposta del sistema consiste nella produzione di segnali in uscita strettamente correlati a quelli in entrata, che nel caso dei sistemi di sicurezza possono essere di diversa natura, in base alle caratteristiche dell'impianto stesso (avvisi acustici o luminosi, collegamenti telefonici, etc.).

I SISTEMI APERTI

Un sistema viene definito "aperto" se **interagisce** con altri sistemi, mantenendo rapporti con un insieme di elementi intercorrelati e coordinati tra di loro, integrati unitariamente per il raggiungimento di un obiettivo comune (es. la sicurezza di determinate aree).

Il concetto di integrazione

Lo strumento basilare per un controllo adeguato, globale e sicuro nel settore della prevenzione e della sicurezza è l'integrazione, intesa come **completamento, coordinazione e fusione di vari elementi**.
Il principio di base dell'integrazione è quello di essere un ambiente sistemistico aperto, scalabile (proprietà del sistema cui è possibile aggiungere nel tempo nuove capacità o funzionalità senza doverne modificare le caratteristiche fondamentali) e ampliamente implementabile (ottimizzabile).

Nei sistemi di sicurezza integrati, grazie alla collaborazione organica tra i componenti, i livelli di affidabilità del sistema risultano di gran lunga superiori alla somma dei livelli di ciascuna singola parte.
Ad esempio, la possibilità da parte dell'unità centrale di un controllo visivo immediato di un'area in cui si è verificata una segnalazione d'allarme, consente un servizio di sorveglianza estremamente affidabile, e quindi maggiori garanzie di sicurezza rispetto alla sola segnalazione ottico/acustica.

L'integrazione dei sistemi è un'importantissima conquista tecnologica, che si perfezionerà sempre più grazie all'utilizzo massiccio e diffuso delle applicazioni digitali, dalla quale discenderanno una serie di innovazioni tecnologiche e gestionali in grado di rivoluzionare la futura concezione dei sistemi di sicurezza integrati, le cui evoluzioni sono già frutto di ricerca e studio.

IL SISTEMA INTEGRATO

Un sistema integrato è un unico sistema che strutturalmente integra in sé le funzioni e le operatività dei sottosistemi che lo compongono, il cui sviluppo è stato progettato in funzione di un controllo coordinato.

E' importante comprendere la differenza tra sistema integrato e integrazione di sistemi, differenza che risiede a livello concettuale e operativo, piuttosto che tecnologico.

Nel caso dell'integrazione di sistemi, non si parla di un'unica struttura in cui i componenti operano unitariamente, ma piuttosto di sistemi-base studiati e realizzati distintamente, integrati in fase successiva: una sorta di "ombrello" che copre tutti i sistemi e ne consente una gestione semplificata, con un ristretto livello di correlazione.

Esiste attualmente una graduale evoluzione verso sistemi integrati modulari e polifunzionali, con capacità di interattività globale elevata, sia con l'interno che con l'esterno, per una massima efficienza e fruibilità da parte dell'utilizzatore.

IL "DIALOGO" FRA I SISTEMI

Nel settore della sicurezza, fino a qualche anno fa la tendenza era indirizzata verso lo sviluppo di programmi capaci di concentrare sulla stessa macchina i messaggi provenieni da sistemi differenti.
Oggi si punta quasi esclusivamente sull'integrazione, che consente di far dialogare senza difficoltà tutti i sistemi collegati al centro di controllo.

Dal dialogo fra le varie entità nasce la possibilità di correlazioni e interazioni legate non soltanto a logiche ON/OFF, ma a relazioni più complesse, in grado anche, in una certa misura, di prevedere alcune particolari situazioni.
Esempi pratici vengono dalla funzionalità relativa alla manutenzione: i sistemi più "intelligenti" permettono di segnalare in tempo utile il momento del controllo di manutenzione per un sensore fotoelettrico di rivelazione fumi. La segnalazione, in questo caso specifico, della necessità di pulizia del labirinto e della camera ottica, è data dal continuo controllo di parametri significativi e dal confronto con dati storici che consentono il monitoraggio costante del sensore.

Si tratta di in sistema cosiddetto "esperto", in grado di rispondere in uno specifico campo di competenza se interrogato in merito ad un problema del settore. Questo genere di applicazioni, che derivano dal campo dell'intelligenza artificiale, si basano su due principi fondamentali: un database di conoscenze (knowledge base) e un

motore inferenziale, basato su principi logici, in grado di utilizzare il materiale della base di conoscenza per trarre conclusioni da una serie di proposizioni, attraverso un processo deduttivo.

Tali sistemi vengono utilizzati in diversi settori, quali la diagnostica medica, la manutenzione di macchinari, la diagnostica di guasti negli apparati elettronici, etc.

IL SISTEMA INTEGRATO MULTIFUNZIONALE

Esistono attualmente diversi sistemi di sicurezza sul mercato, dai più piccoli e semplici a livello locale a quelli complessi con distribuzione geografica su tutto il territorio nazionale.

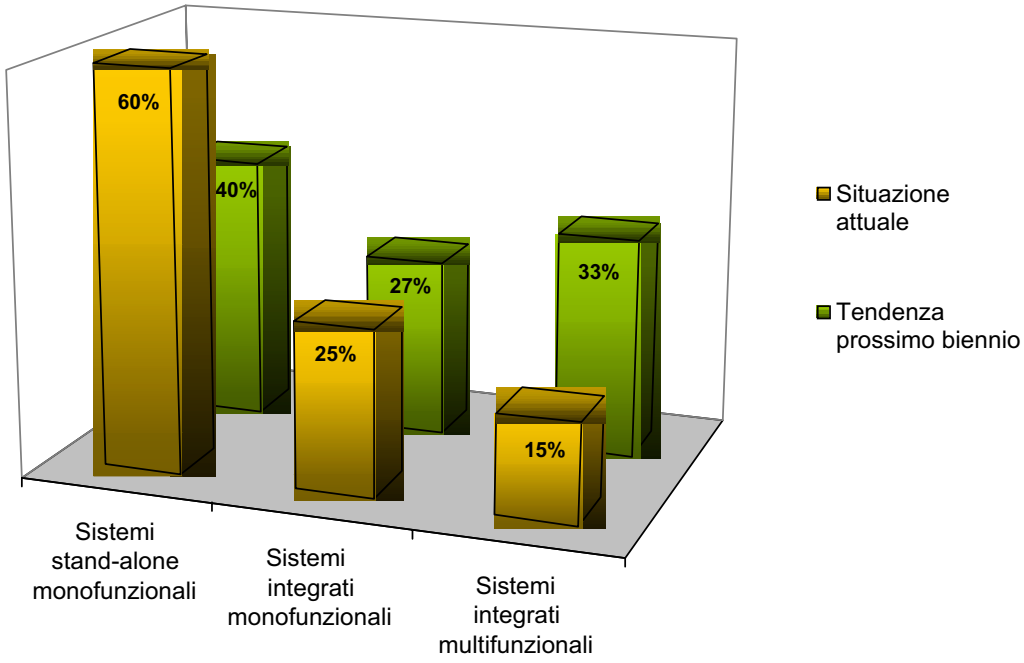
I sistemi sono sostanzialmente di tre tipi:

- **sistema stand-alone monofunzionale**, impianto con una singola funzionalità (antintrusione, TVCC, antincendio, etc.) privo di connessione ad altri sistemi;

- **sistema integrato monofunzionale**, formato dall'integrazione di più sistemi stand-alone monofunzionali con ingressi e funzionalità piuttosto omogenee, trattandosi di integrazione tra sistemi simili;

- **sistema integrato multifunzionale**, top tecnologico e funzionale dei sistemi di controllo, dotato della possibilità di controllare e gestire in maniera omogenea e coordinata l'operatività degli impianti di sicurezza (localmente o in diverse aree geografiche).

IL MERCATO DEI SISTEMI DI SICUREZZA



Considerando le possibilità di ottimizzazione del sistema e i possibili scenari del mercato a medio termine, si può affermare che il sistema integrato multifunzionale rappresenta il futuro nel settore della sicurezza, che richiederà in maniera sempre maggiore soluzioni a esigenze di protezione globale.

La centralizzazione dei sistemi di sicurezza

L’architettura di un sistema centralizzato

Diamo ora una definizione più specifica di un sistema di centralizzazione allarmi: “Processo di costante monitoraggio e gestione di unità periferiche realizzato mediante l’afflusso telematico di dati a un centro di elaborazione e supervisione dotato di software applicativo specializzato”.

Quasi paradossalmente, la condizione fondamentale e imprescindibile per la riuscita di un progetto di centralizzazione e supervisione delle unità periferiche, è il corretto funzionamento dei sottosistemi.
I sottosistemi periferici di antintrusione, antirapina, antincendio, videosorveglianza, controllo accessi, etc. devono infatti alimentare la centrale di supervisione di dati corretti, non inquinati da falsi allarmi o allarmi impropri, che produrrebbero dati inattendibili, tali da presentare al centro di controllo situazioni irreali e difficilmente gestibili.

Oltre alla funzione di monitoring dell’operatività delle unità locali, il centro di controllo espleta un’importante funzione di gestione degli eventi, un continuo “refresh” delle realtà periferiche che conferisce un carattere dinamico all’attività per il continuo variare delle contingenze ambientali.
La caratteristica primaria della centralizzazione è la **qualità**, che deve essere ottenuto attraverso:

- un contenuto tecnologico perfettamente rapportato alle esigenze;
- un rispetto delle normative ufficiali in materia;
- affidabilità;
- facilità d’uso;
- sicurezza del software;
- semplicità di manutenzione.

Le componenti di un sistema di centralizzazione sono le seguenti:

a) il sistema sensoristico e di elaborazione locale delle unità periferiche;
b) i vettori di trasmissione dei dati bidirezionali centro Č periferia Č centro;
c) il centro di supervisione ed elaborazione di tutti i dati del sistema che, in correlazione agli eventi verificatisi, propone adeguati provvedimenti.

Troviamo al primo posto il sistema sensoristico e di elaborazione locale delle unità periferiche in quanto, come affermato in precedenza, è un punto nodale del sistema di centralizzazione che non può prescindere dall'esigenza di ottimizzare i dati informativi generati dalla periferia.

IL SOTTOSISTEMA SENSORISTICO E DI ELABORAZIONE LOCALE DELLE UNITA' PERIFERICHE

I sottosistemi sui quali è impostata la centralizzazione devono:

a) disporre di sensoristica di alta qualità (elevato coefficiente di rapporto disturbo-rumore), rispondente alle norme tecniche CEI, certificata IMQ e correttamente installata;
b) essere dotati di centrale di gestione della sensoristica periferica, rispondente alle norme tecniche CEI, certificata IMQ e correttamente installata, dotata di capacità elaborativa autonoma secondo il criterio dell'intelligenza distribuita, con architettura di tipo modulare, aperta ad ogni implementazione gestionale di sottosistemi, multifunzionale (in grado di eseguire contestualmente più funzioni);
c) essere correttamente cablati, con particolare cure delle alimentazioni primarie e di soccorso, fattore di vitale importanza.

I VETTORI DI TRASMISSIONE DEI DATI

I dati relativi agli stati e agli eventi generati dai componenti dei sottosistemi vengono trasferiti al centro di supervisione tramite diversi supporti di trasmissione.

La tendenza attuale è l'utilizzo di reti tramite l'impiego del protocollo di rete IP (Internet Protocol), progettato soprattutto per gestire l'interconnessione.
Considerata la tipologia delle trasmissioni riguardanti la sicurezza, è condizione irrinunciabile l'adozione di garanzie contro tutti i prevedibili rischi di carattere tecnico, casuale e fraudolento (criptazione dei dati).

IL CENTRO DI SUPERVISIONE ED ELABORAZIONE DATI

Le caratteristiche prestazionali e qualitative fondamentali che il centro di supervisione deve avere sono le seguenti:

- × di ultima generazione;
- × attitudine all'espandibilità;
- × affidabilità sperimentata;
- × linguaggi di programmazione standard;
- × memoria RAM implementabile;
- × disporre di un numero coerente di linee di accesso alle rete di trasmissione dei dati;
- × utilizzo di un protocollo applicativo standard.

IL SOFTWARE APPLICATIVO

I software applicativi di qualità, concepiti per la gestione della sicurezza, devono:

- × costituire un insieme di moduli parametrizzati e specializzati per generare una serie di funzioni identificate;
- × essere predisposti all'implementazione di funzioni di tipo nuovo, personalizzate;
- × essere aperti alla crescita armonica dei punti operativi periferici.

La funzione del software applicativo, oltre a sollevare l'operatore da situazioni decisionali critiche, è quella di sostituirsi a lui per valutare esattamente l'evento, che viene posizionato in una scala multivalore predeterminata e presentato con una serie di specifiche procedure da seguire obbligatoriamente.

I sistemi di sicurezza distribuiti

Il ruolo delle reti nei sistemi centralizzati distribuiti

Un'organizzazione funziona al meglio se è basata, come l'essere umano, su un "sistema nervoso" capace di distribuire istantaneamente le informazioni a tutti coloro che ne hanno bisogno.
Nel "sistema nervoso digitale" rappresentato da un moderno sistema di centralizzazione, occorre far convergere l'enorme flusso di eventi, dati, immagini, suoni, proveniente dalla periferia e ridistribuirlo nella maniera più efficace ed intelligente in accordo alle procedure aziendali.
Le reti, in tali progetti, assumono un'evidente importanza "nevralgica".

Le potenzialità offerte dall'integrazione e dall'evoluzione delle conoscenze informatiche permettono la realizzazione di sistemi di sicurezza che superano le barriere della localizzazione geografica, per lungo tempo ostacoli alla centralizzazione delle informazioni.
Le reti distribuite, di tipo locale o globale, sono state gli elementi chiave per questa rivoluzione.

Nei sistemi integrati multifunzionali, le capacità di elaborazione sono divise fra più unità separate. La connessione fra le unità di calcolo può essere

- stretta (singoli calcolatori con architettura multiprocessore);
- intermedia (reti locali di calcolatori);
- larga (calcolatori connessi in rete geografica).

Il progetto di architetture di sistemi distribuiti presenta problemi tipici fondati sulla necessità di garantire l'efficiente condivisione delle risorse e di regolare il flusso di comunicazione tra le varie unità.
Negli ultimi anni, l'utilizzo di nuove tecnologie per la comunicazione (es. le fibre ottiche) ha permesso un forte incremento della velocità di comunicazione, che ha reso interessante l'utilizzo di una struttura intelligente distribuita.

L'incremento del flusso dei dati ha reso possibile la trasmissione dei segnali video (nei sistemi televisivi a circuito chiuso) con una velocità e una qualità abbastanza elevati, mentre in precedenza era sempre stato necessario ricercare il miglior compromesso tra l'aggiornamento dell'immagine e la sua qualità, comunque a scapito dell'intelligibilità delle immagini ricevute e della loro possibile utilità in casi reali.

La definizione di rete

Per rete, o rete telematica (network in inglese) si intende un insieme di computer collegati tra loro **fisicamente** (tramite cavi e dispositivi hardware) e **logicamente** (tramite protocolli e programmi di comunicazione), in un sistema di comunicazione dati, allo scopo di condividere le risorse dei diversi sistemi informativi.

Una rete telematica comprende una serie di elementi che permettono ai calcolatori di dialogare tra loro. I calcolatori possono essere interconnessi tramite cavi (es. in fibra ottica, in rame, coassiali) o via etere.

LE COMPONENTI STRUTTURALI DELLA RETE

Indipendentemente dalle caratteristiche della rete, questa può essere definita come una struttura costituita da tre componenti logiche a cui corrispondono tre componenti fisiche.

COMPONENTI LOGICHE	COMPONENTI FISICHE
FORNITORI DI SERVIZI	SERVER, COMPUTER SU CUI RISIEDONO LE RISORSE DA CONDIVIDERE
SOTTOSISTEMA DI COMUNICAZIONE	RETE DI TRASMISSIONE
UTENTI	CLIENT, I TERMINALI CHE USUFRUISCONO DELLE RISORSE DI RETE

Le componenti fisiche sono gli host che compongono una rete, e possono essere di due tipi: server o client. I **server** consentono ad altri

computer, detti **client**, di usufruire delle proprie risorse hardware e software. I due tipi di host comunicano attraverso un insieme di protocolli di comunicazione. L'insieme di host e della rete di trasmissione dati costituisce una rete.

La classificazione di una rete

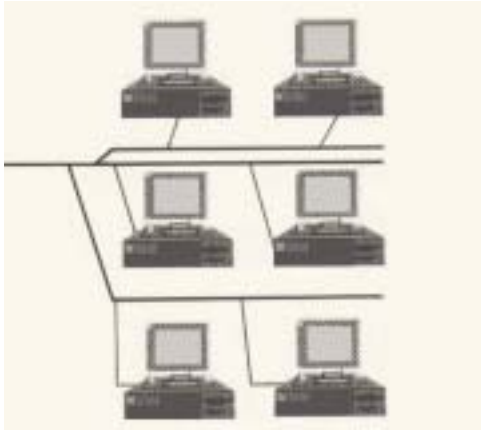
Una rete si può classificare in base alle dimensioni, alla topologia, alla natura fisica e al protocollo.

DIMENSIONE

Dipende dal numero dei computer connessi in rete.
Qualsiasi rete organizzata entro brevi distanze (area geografica relativamente ristretta) è una **LAN** (Local Area Network), indipendentemente dal numero di computer e dal modo con cui è stata realizzata. Le **WAN** (Wide Area Network) sono l'estremo opposto delle LAN, in quanto reti di comunicazione che coprono grandi distanze geografiche, dell'ordine di km. Tra le LAN e le WAN si trovano le **MAN** (Metropolitan Area Network), che collegano i nodi di una stessa città.

TOPOLOGIA

Gerarchiche. I nodi di connessione sono organizzati ad albero.

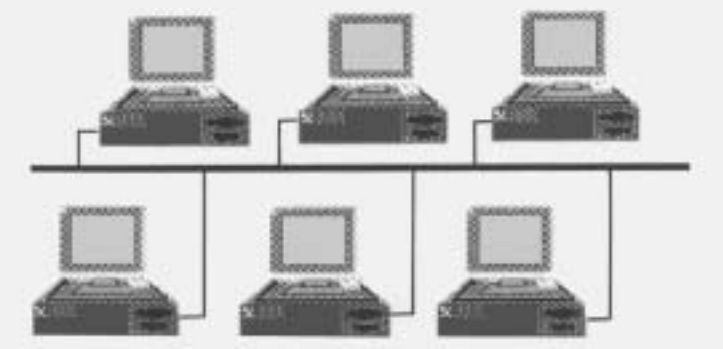


RETE AD ALBERO

Questo tipo di topologia è spesso utilizzato per realizzare reti all'interno delle aziende che si estendono sul territorio nazionale. I singoli uffici

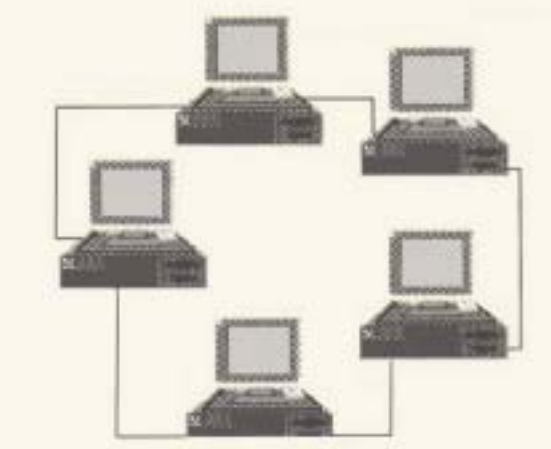
possono essere collegati ad un ufficio principale locale, questi ultimi ad un ufficio regionale e gli uffici regionali alla sede centrale. Hanno un basso costo ma anche basse velocità.

A bus o lineari. Quest'architettura prevede un singolo canale di comunicazione diviso, il bus, a cui sono collegati direttamente tutti i nodi. Il mancato funzionamento del bus determina il blocco dell'intera rete.
E' una topologia usata tipicamente nelle reti locali.
I vantaggi sono la semplicità, l'economicità e la velocità, se la banda del bus non costituisce colli di bottiglia.



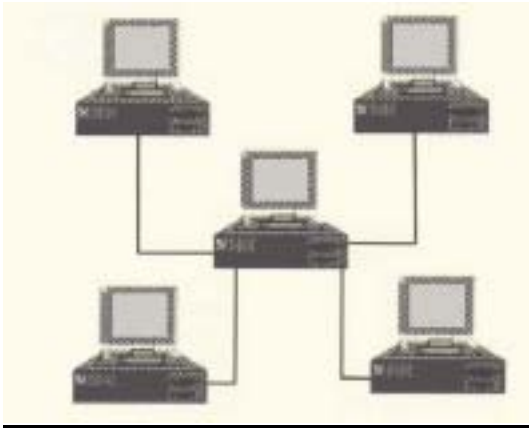
RETE A BUS

Ad anello. Tutti i computer sono collegati tra loro in un cerchio logico; ogni nodo è collegato al precedente e al successivo in modalità punto-punto (un collegamento per ogni coppia di nodi).



AD ANELLO

A stella. Sebbene si sia sviluppata più tardi, quella a stella è diventa la topologia più popolare. Tutti i computer sono connessi, tramite un tratto dedicato, a un nodo centrale (hub); i pacchetti inviati da una stazione ad un'altra sono ripetuti su tutte le porte dell'hub, permettendo a tutte le stazioni di vedere qualsiasi pacchetto inviato sulla rete. Questa topologia è più robusta rispetto a quella a bus in quanto se vi è un'interruzione su una delle connessioni della rete, solo il computer collegato a quel segmento ne risente, mentre gli altri continuano ad operare normalmente.



A STELLA

NATURA FISICA DELLA RETE

Consiste nella definizione del mezzo fisico con cui si realizza la rete.
Il più comune apparecchio usato per connettersi alle reti è il **modem**, che permuta una normale connessione telefonica in un collegamento in rete. Il metodo più comune per connettere delle macchine e creare una LAN, è invece quello di utilizzare delle schede **Ethernet**. Esistono anche delle trasmissioni via radio, anziché via cavo. Queste reti sono dette CLAN (Cordless Local Area Network).

Il collegamento

Esistono due tipi principali di collegamento tra due stazioni:

× commutato, quando la connessione viene realizzata solo quando è necessaria e richiesta. Questa tipologia è la più diffusa (tipica delle linee telefoniche) ed è quella utilizzata dagli utenti di Internet;

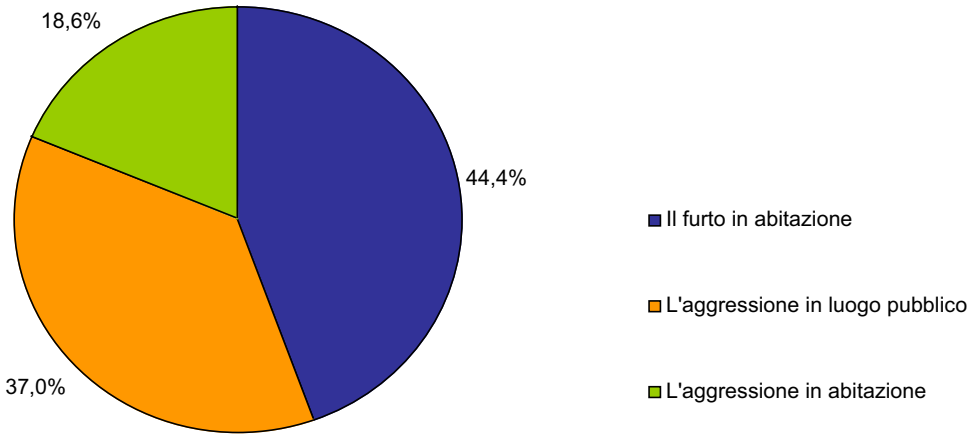
× permanente, quando viene dedicata ad uso esclusivo la linea che collega i due dispositivi (più costoso del commutato ed utilizzato prevalentemente da aziende).

Il mercato attuale dei sistemi di sicurezza

Nel 2001, il mercato italiano dell'intero settore della sicurezza, dalle serrature ai sofisticatissimi sistemi elettronici, ha raggiunto quote 2.549 milioni di Euro.
La domanda di sistemi e impianti elettronici per la sicurezza è cresciuta del 12% (fonte: IMQ), uno degli incrementi più importanti degli ultimi anni.
Punta di diamante la TV a Circuito Chiuso, risultato dovuto soprattutto all'impiego che ne hanno fatto le pubbliche amministrazioni, specie a livello locale, per controllare il territorio e fare da deterrente alla criminalità diffusa. A fronte di una rapidissima evoluzione delle tecnologie messe a disposizione della sicurezza collettiva sono emerse due esigenze: la necessità di prodotti ed installatori affidabili e il bisogno di una nuova legge a tutela della sicurezza privata, in sostituzione di una normativa del tutto superata.

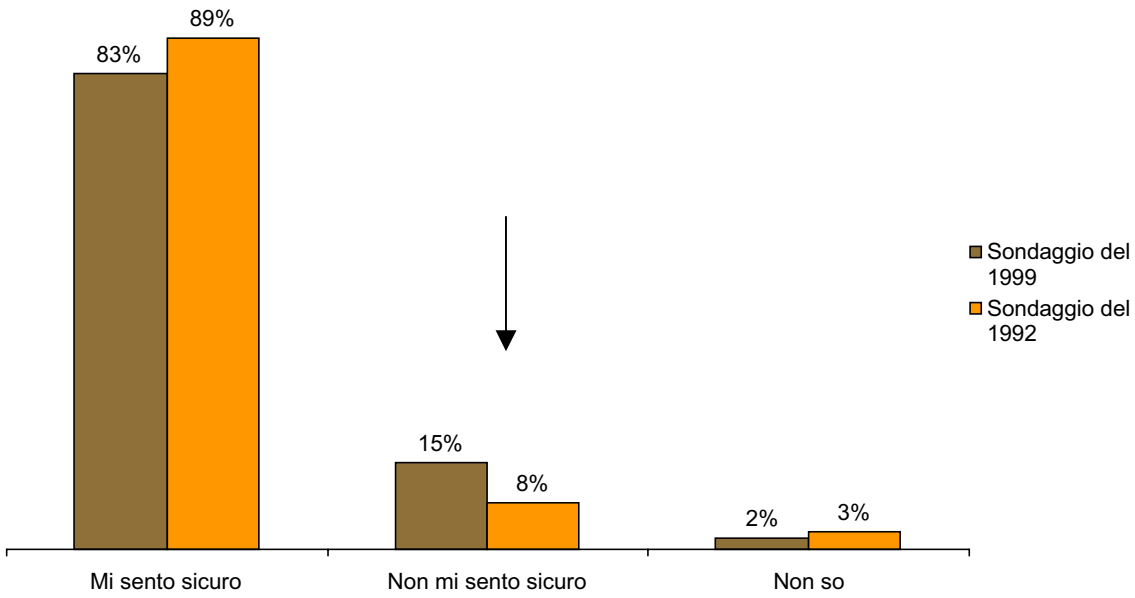
I grafici riportati di seguito illustrano il punto attuale della sicurezza in Italia:

RISCHI PIU' TEMUTI DAGLI ITALIANI



Fonte: Cirm

SENSAZIONE DI SICUREZZA A CASA PROPRIA

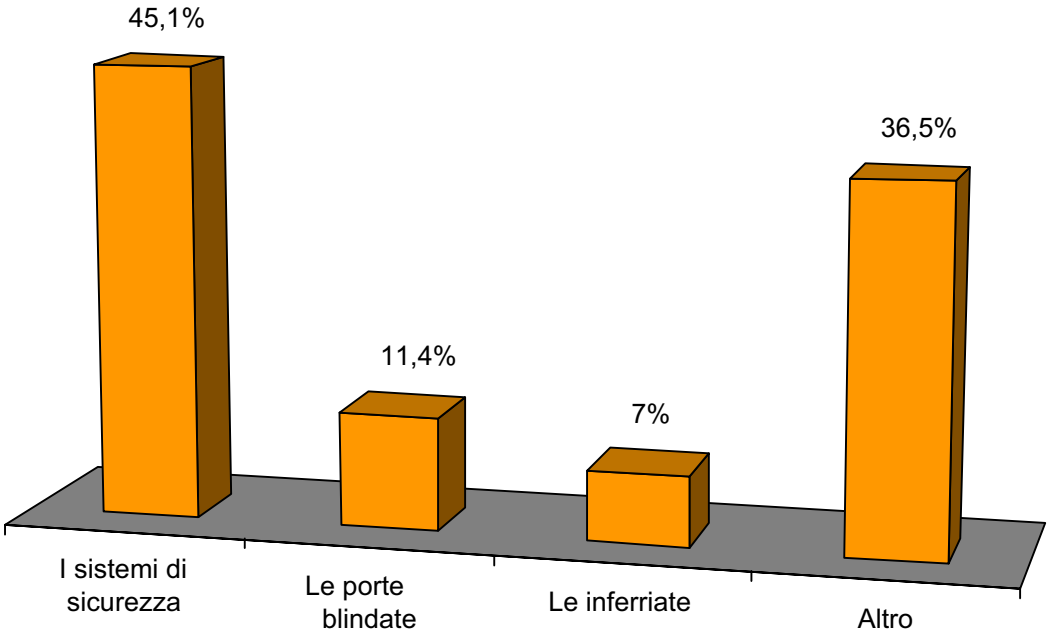


Fonte: Doxa

Da questa indagine Doxa, è interessante notare come, da un sondaggio del 1992 in cui un 8% di intervistati non si sentivano sicuri a casa propria durante la notte, nel 1999 questa percentuale sia quasi raddoppiata.

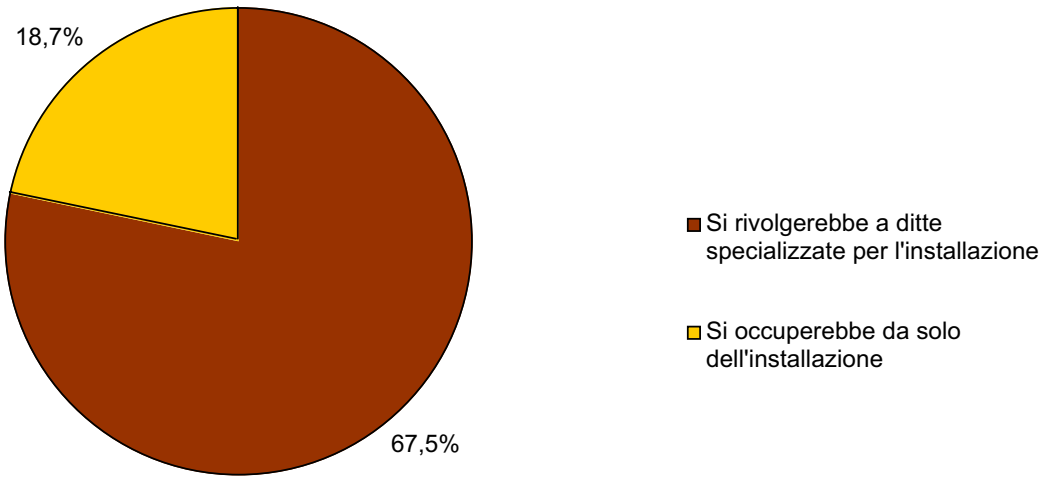
Questo significa che 15% di italiani adulti, vale a dire 7 milioni e mezzo di persone, non si sentono abbastanza sicuri, e cioè del tutto al riparo dei rischi della delinquenza, neppure la notte, quando sono chiusi in casa propria.

MISURE DI SICUREZZA ADOTTATE NELLE ABITAZIONI CONTRO I FURTI E I DANNI DOVUTI A FUGHE DI GAS E INCENDI



Fonte: Sistema Casa

ITALIANI INTERESSATI AD INSTALLARE UN SISTEMA DI ALLARME = 8,3%, DI CUI:



Fonte: Cirm

I software gestionali

I sistemi di centralizzazione allarmi in rete locale, realizzati attraverso software gestionali sempre più funzionali, flessibili e semplici nelle modalità di utilizzo, stanno ottenendo importanti consensi, grazie alla possibilità di estendere i sistemi di sicurezza - dalla rilevazione incendi e videosorveglianza, all'antintrusione, alle protezioni perimetrali, al controllo accessi - a **configurazioni molto complesse**, sia dal punto di vista delle dislocazioni geografiche delle varie ubicazioni (filiali commerciali, catene alberghiere, banche con decine di filiali sparse su tutto il territorio nazionale, etc.) sia da quello strutturale/organizzativo (musei, comprensori militari, aree industriali, centri residenziali ed altri).

Questi software sono indicati sia per impianti con un'unica tipologia realizzativa, sia per quelli fra loro diversi ma integrati in un unico ambiente operativo. Di conseguenza, risultano adatti in particolar modo al controllo e alla gestione di piccole, medie e grandi dimensioni nonché per quelle realtà complesse ed articolate che richiedono una certa praticità d'impiego, con monitoring e comandi impartiti da una postazione centrale in ambito locale.

MATERIALE HARDWARE

Considerate alcune delle caratteristiche fondamentali di questi pacchetti applicativi, quali la flessibilità, la semplicità di funzionamento e la destinazione (dalle abitazioni private a complesse realtà organizzative), è conseguenza logica la necessità di utilizzare strumenti hardware standard, di facile reperibilità, accessibili sia dal punto di vista economico **(investimento minimo, compreso di software gestionale, di circa 2.000 Euro per un massimo di 15.000 Euro)** che dal punto di vista dell'uso (compatibilità con sistemi operativi diffusi, come Windows).

Apparecchiature hardware di base (gestione di piccole centralizzazioni)

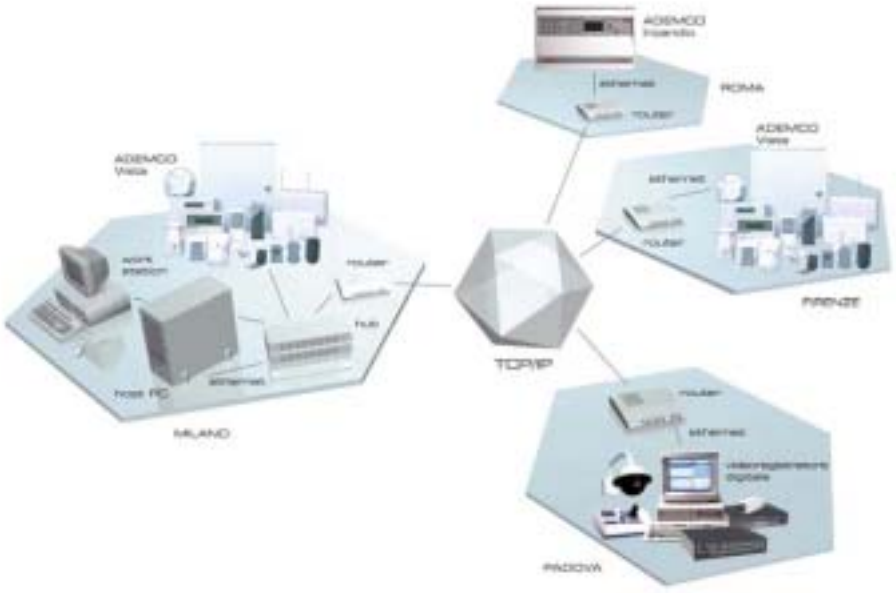
Personal computer tipo P4 2 Ghz, dotato di 256 MB di RAM

Lettore cd-rom o masterizzatore

Monitor 17” con grafica minima e risoluzione 1024 x 768

Sistema operativo Windows – NT – 2000 installato

Il panorama attuale propone dei pacchetti applicativi innovativi, attraverso i quali si concretizzano in maniera efficace ed efficiente il concetto di sistema integrato nel campo della sicurezza, basato su tecnologie diversificate per quanto concerne ogni singola area applicativa (intrusione, video, incendio, etc.).



Lo schema applicativo illustra in maniera inequivocabile le potenzialità delle soluzioni più performanti presenti oggi sul mercato: ogni singolo sistema (situato in qualsiasi area geografica purchè raggiungibile da un collegamento dati) ed ogni singola tecnologia applicativa (antintrusione e/o videosorveglianza e/o rivelazione incendio comunque combinate fra loro) possono essere interconnesse in un solo sistema, pur mantenendo inalterate le loro caratteristiche di sistemi autonomi. Da qualsiasi postazione, tramite opportuni livelli di accesso; si possono

gestire tutti i sistemi della rete oppure si possono introdurre delle limitazioni in funzione della configurazione operativa voluta.

I software dialogano e interagiscono (bidirezionalità delle informazioni) via rete con tutte le apparecchiature componenti il sistema, utilizzando i protocolli di comunicazione di ogni singola macchina, con un livello di integrazione molto elevato e una gestione completa, efficiente e sicura. Operano senza compromettere in alcun modo il funzionamento indipendente di ogni sottosistema: un guasto eventuale del pacchetto di gestione o di un singolo sottosistema non influisce in alcun modo sull'operatività globale.

Il sistema di centralizzazione prevede dunque un'assoluta **autonomia** fra la sicurezza indipendente delle centrali situate in campo (funzionalità delle interfacce di rete) e la gestione della centralizzazione delle stesse attraverso i vari computer installati presso il centro di controllo, a garanzia di un'affidabilità totale.

I componenti del sistema

IL CENTRO DI CONTROLLO

Il centro di controllo viene fornito da uno o più computer che, installati sulla stessa rete Ethernet, consentono una piena gestione di tutte le centrali periferiche: installato in prossimità dell'area di cui il sistema gestisce la protezione, si occupa sia della comunicazione con tutte le unità collegate, sia della supervisione del sistema completo.

I SERVER

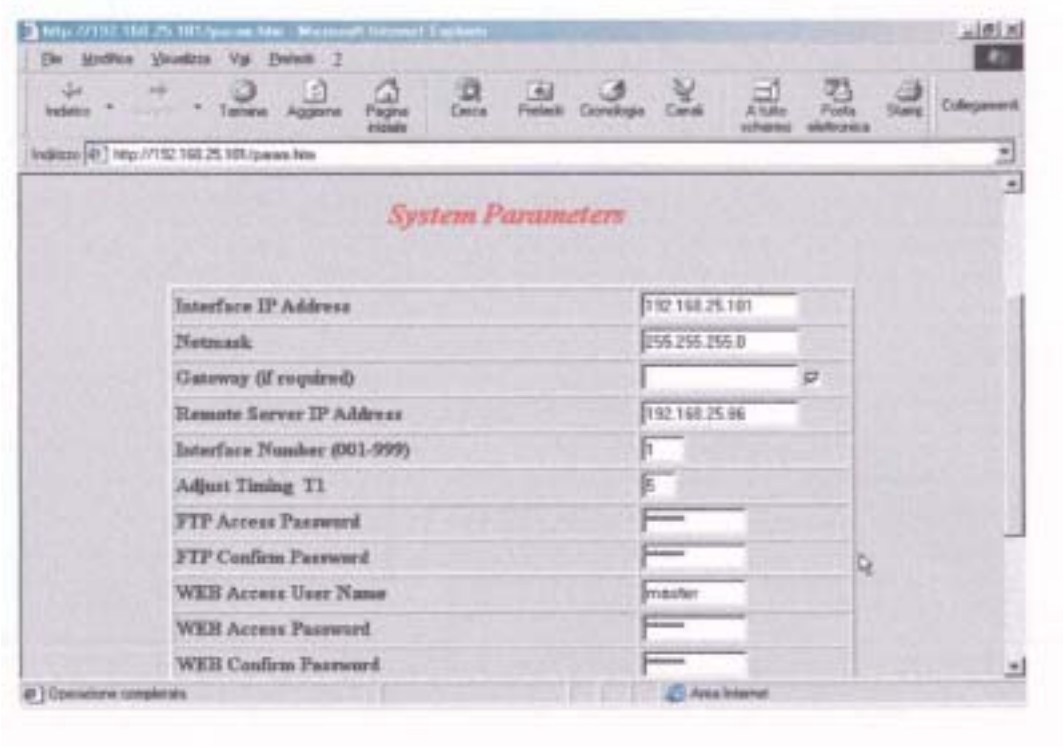
A garanzia di sicurezza, è possibile suddividere il carico di lavoro su differenti server, che gestiscono separatamente parti della configurazione rimanendo in comunicazione fra loro. In questo modo, anche in presenza di problemi tecnici, il sistema continua a funzionare correttamente nel suo complesso.

L'INTERFACCIA DI RETE

La composizione del sistema viene realizzata utilizzando una interfaccia per ogni unità periferica. Questa interfaccia consente di trasmettere lo stato della centrale al centro di controllo, nonché di ricevere dallo stesso eventuali comandi da inviare alla centrale, utilizzando come "mezzo di trasporto" il protocollo TCP/IP.
L'interfaccia, inoltre, ha anche la capacità di memorizzare gli eventi in caso di interruzione del collegamento TCP/IP.
Alcune caratteristiche delle interfacce oggi in commercio:

- possibilità di selezionare quale tipologia di eventi trasmettere al centro di supervisione;
- memorizzare fino a 100 eventi, in modo da avere sempre una situazione aggiornata anche in caso di momentaneo scollegamento da parte del centro;
- invio di tutte le segnalazioni con data e ora;
- test periodico di supervisione di tutte le periferiche impostabile da 1 a 999 minuti;

- possibilità di impostazione della configurazione di tutte le interfacce remote direttamente dal centro di controllo utilizzando un browser;
- possibilità di aggiornamento del firmware utilizzando un programma FTP;
- possibilità di visualizzazione della singola centrale attraverso un browser.



Esempio di configurazione di una interfaccia attraverso browser.

LA RETE ETHERNET

Ethernet è la tipologia standard di una rete locale ideata nel 1972 da Robert Metcalfe e Davis Bloggs. E' una rete che sfrutta le tecnologie a diffusione di tipo bus con controllo operativo decentralizzato.

La versione più diffusa, su cavo coassiale, può raggiungere velocità di traferimento di 10 Mbit/s.

Il nome è stato ideato e registrato da Xerox e suggerisce l'idea dell'etere.

Ethernet usa un solo cavo per collegare decine di stazioni di lavoro, ciascuna delle quali riceve contemporaneamente tutto quello che

passa sulla rete, mentre solo una stazione alla volta ha la facoltà di trasmettere.
L'utilizzo di una rete Ethernet come mezzo di trasporto fa sì che sia possibile realizzare configurazioni in rete geografica (WAN) o in rete locale (LAN), senza stendere linee dati dedicate, ma sfruttando linee dati già esistenti.

IL PROTOCOLLO TCP/IP

Il TCP/IP è un protocollo di comunicazione, i cui due principali elementi sono il TCP (Transmission Control Protocol) e l'IP (Internet Protocol).
Un protocollo è un insieme di regole che permettono di gestire lo scambio di informazioni e dati tra due computer interconnessi fra loro.
Sviluppato alla fine degli anni Settanta da Vincent Cerf e Robert Kahn, era inizialmente di proprietà del Dipartimento della Difesa degli Stati Uniti.
Venne poi utilizzato come architettura network per Internet e per la maggior parte dei sistemi in ambito universitario.

Lo scopo per cui era stato ideato era permettere l'interoperabilità tra sistemi di tipo diverso. Successivamente, negli anni Ottanta, le imprese iniziarono a rendersi conto che i servizi resti possibili dal TCP/IP potevano essere utilizzati diversamente (ad esempio, l'FTP per trasferire velocemente i dati o l'SMTP per la posta elettronica) e per migliorare la comunicazione tra le diverse sedi.
Il TCP/IP si arricchì così di nuovi servizi e fu sviluppato per poter essere utilizzato anche su macchine non Unix: questo ne decretò il successo come protocollo di trasmissione ufficiale di Internet.
Oggi il TCP/IP può essere definito come un insieme di regole pubbliche (open system) che permette l'interconnessione di reti anche molto differenti, indipendentemente dalla tecnologia usata per ogni rete. Il principio di base dell'interconnessione è rendere indipendenti le applicazioni dalle caratteristiche tecniche delle reti in modo semplice e flessibile. Affinchè il sistema funzioni, i vari protocolli devono essere rispettati da tutti i computer connessi.

Il TCP/IP è sostituito da due protocolli principali:

- **il protocollo TCP**. Opera al livello trasporto, gestendo la trasmissione dei dati tra due computer connessi, il mittente e il destinatario. Garantisce la comunicazione tra computer e spezzetta i dati in pacchetti di dimensioni prefissate, in relazione alle impostazioni e alle caratteristiche del ricevente. Dopo la spedizione, verifica se i dati sono giunti a destinazione e, in caso contrario, li invia nuovamente. Se la trasmissione ha avuto buon esito, il protocollo TCP sul calcolatore ricevente è in grado di riassemblare i pacchetti, ricomponendo i dati originari.

- **Il protocollo IP.** Occupa il secondo livello del protocollo TCP/IP e provvede all'instradamento dei pacchetti nella rete e all'indirizzamento verso i vari router che consentono ai dati di seguire la via ottimale, in quello specifico momento, per giungere a destinazione. Se l'indirizzo del destinatario appartiene a un computer di una rete esterna, il protocollo si serve dei router per instradare correttamente i pacchetti. Se è interno a una rete locale, il protocollo invia direttamente il pacchetto al computer destinatario.

Funzionalità e caratteristiche dei software gestionali

L'INTELLIGENZA DISTRIBUITA

I pacchetti applicativi di gestione del sistema, attualmente in commercio, soddisfano un'ampia fascia di utenti e di esigenze in quanto, oltre ad utilizzare le centrali di allarme a tecnologia mista (via cavo, multilplexer e radio), assicurano il riconoscimento univoco della zona o del punto controllato, che può essere rappresentato sul terminale di gestione con descrizione in chiaro e simbologia configurabile (icona).

Le modalità di comunicazione garantiscono inoltre che la gestione dei vari impianti collegati si svolga **in tempo reale**, ovvero con scambio reciproco e costante di informazioni tra periferiche e centro di controllo. Ogni impianto periferico collegato può essere preconfigurato dal centro in modo tale che possa essere soltanto supervisionato (controlli sullo stato della centrale), oppure parzialmente o totalmente gestito attraverso semplici comandi indirizzabili; in entrambi i casi, gli impianti periferici conservano anche una loro individuale funzionalità ed autonomia.

Con questa soluzione sono stati rispettati i canoni di sicurezza, adottando una **configurazione ad intelligenza distribuita** che, rispetto ad un'architettura ad intelligenza centralizzata, consente una maggiore flessibilità d'impiego ed una elevata economicità, garantendo alti livelli di affidabilità ed efficienza anche in caso di guasto di una o più unità periferiche.
Tutte le informazioni riguardanti il sistema vengono presentate all'operatore della stazione di lavoro in modo chiaro e tempestivo, con pagine grafiche a colori di intuitivo utilizzo, con mappe associate agli allarmi che semplificano l'interpretazione delle segnalazioni e con la possibilità di utilizzare ampiamente il mouse per tutte le operazioni degli applicativi.

Sviluppati per funzionare in ambiente Windows, possono essere utilizzati da parte di personale non specificatamente addestrato od esperto nelle tecniche informatiche.

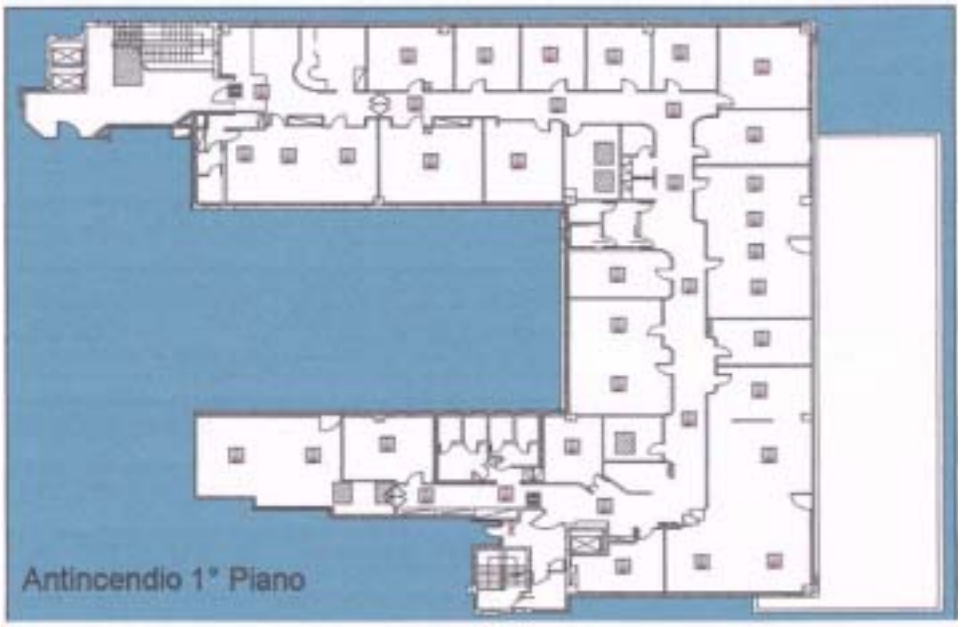
Le principali caratteristiche dei software di gestione più innovativi presenti oggi sul mercato sono:

- rappresentazione grafica dello stato di tutte le periferiche;
- diversi livelli di mappe per ogni singolo sensore (da 3 a 5);
- gestione degli operatori a livello di codice di accesso con eventuali limitazioni alla funzionalità del programma;
- possibilità da parte del centro di inviare comandi verso le periferiche quali Inserimenti, Disinserimenti e Esclusioni zone;
- archiviazione automatica dei dati ricevuti, mensilmente, trimestralmente o semestralmente;
- possibilità di inserire nel sistema più posti operatori, in modo da dividere il carico di lavoro per singolo operatore;
- funzione di Chat fra i vari terminali remoti;
- possibilità di creare più sistemi autonomi che comunichino fra loro;
- possibilità di personalizzazione a livello grafico del programma;
- accesso al sistema di supervisione anche attraverso rete telefonica PTSN e ISDN utilizzando Accesso Remoto;
- possibilità di connettere fino a 300 periferiche per ogni server;
- fino a 99 postazioni remote per ogni server di gestione;
- mascheramento di tutti i dati trasmessi ed inviati con protocollo CEI-ABI 79/5 79/6;
- test periodico di supervisione di tutte le periferiche;
- a seguito di eventi provenienti dalle periferiche, possibilità di commutare relé locali ed inviare stringhe ASCII (standard di testo americano riconoscibile da tutti i programmi) su porta seriale per ottenere dei dati gestibili dal software;
- semplicità di esclusione e ripristino dei singoli punti;
- ricerca nell’archivio storico di tutti gli eventi ricevuti per differenti chiavi di ricerca (data, ora, operatore, etc.).

Esempi pratici:

GESTIONE SISTEMA DI VIDEOSORVEGLIANZA:

- possibilità di richiamare visivamente e gestire una o più telecamere a fronte di un allarme proveniente dal campo
- visualizzazione del posizionamento di ogni telecamera su mappa grafica;
- ricerca delle immagini registrate di più siti contemporanei;
- visualizzazione contemporanea di immagini “live” e “registrate”.



Tipica maschera di visualizzazione dello stato degli impianti a livello grafico.

GESTIONE SISTEMA RIVELAZIONI INCENDI

- localizzazione immediata dell’incendio;
- completa visibilità dell’architettura dell’impianto;
- operazioni di manutenzione semplificate: lo stato dei rivelatori è costantemente sotto controllo;
- semplicità di esclusione e ripristino dei singoli punti (alberghi, ospedali, etc.)

I collegamenti via Internet

Alcuni sistemi di gestione centralizzata basati su software permettono l'accesso al pc gestore via Internet, offrendo la possibilità di visionare lo stato degli allarmi da qualunque pc collegato alla rete.
Il problema primario è la sicurezza dei dati che viaggiano su Internet, risolto nei software più avanzati con il sistema di criptazione DES.

LA PROTEZIONE DEI DATI

Per minimizzare il rischio di intercettazioni dei dati durante il trasferimento via Internet, si adottano procedure basate su algoritmi crittografici, utilizzati per sviluppare sistemi per la cifratura dei messaggi aventi contenuti riservati (criptazione).

DES (Data Encryption Standard) è uno standard crittografico sviluppato dalla IBM nella metà degli anni Settanta, inizialmente adottato dal governo degli Stati Uniti. Fa parte della categoria degli *algoritmi a chiave segreta* (uso di una sola chiave per la cifratura e la decifratura del messaggio). Le chiavi utilizzate hanno lunghezza di 64 bit, pari a 8 caratteri ASCII.
Tale metodo è basato sull'uso di un algoritmo di generazione di chiavi costituite da 64 bit di dati, che sono combinati e modificati con i primi 64 bit del messaggio con cui vengono trasmessi. Per codificare il messaggio, questo viene suddiviso in blocchi da 64 bit, ciascuno dei quali può essere combinato con la chiave segreta grazie a procedimenti complessi che ne garantiscono l'assoluta protezione.

CONCLUSIONI

Le società di fornitura dei sistemi di supervisione degli allarmi stanno immettendo sul mercato prodotti sempre più avanzati e performanti, dal facile utilizzo e dalle prestazioni intelligenti, per il monitoraggio e il controllo costante dello stato degli impianti.

Un servizio centralizzato di prevenzione e manutenzione altamente affidabile e modulare, i cui vantaggi

1. visualizzazione dei dati in tempo reale;
2. estrema facilità di installazione e di utilizzo;
3. versatilità (implementazione e personalizzazione);
4. qualità certificata;
5. elevate prestazioni tecnologiche a costi congrui

saranno la risposta chiave alle esigenze sempre maggiori di soluzioni globali nel settore della sicurezza.

Indice