# Il sistema integrato di sicurezza del Senato della Repubblica

Autori: Giovanni Contardi[1], Fabio Garzia[2], Roberto Cusani[2]

[1]Senato della Repubblica, P.zza Madama, Roma

[2]Ingegneria della Sicurezza
SAPIENZA – Università di Roma
Via Eudossiana, n.18 Roma, Italia
Tel. 0644585626 - Fax 0644585618 - e-mail fabio.garzia@uniroma1.it

**Sommario**

La sicurezza di un sito complesso quale il Senato della Repubblica dipende fortemente dall'utilizzo di sistemi integrati di sicurezza. Ogni debolezza del sistema integrato di sicurezza implica una debolezza del sito stesso. Per tale motivo è stato necessario progettare e realizzare un sistema di sicurezza altamente integrato, efficiente ed affidabile. Gli autori, nel presente lavoro, intendono illustrare quanto fatto per progettare e realizzare il sistema integrato di sicurezza in oggetto.

## 1. INTRODUZIONE

Il Senato della Repubblica è composto da 13 palazzi storici situati nel centro di Roma.

Fig.1 Vista di Palazzo Madama, il palazzo principale dove si trova l'aula parlamentare.

In contesti complessi, quali il Senato della Repubblica, è necessario progettare e realizzare sistemi di sicurezza fortemente integrati che assicurino una elevata interazione tra i differenti sottosistemi

che li compongono. In questo modo i differenti sottosistemi sono in grado di interagire reciprocamente in maniera efficiente e coordinata, mostrando, allo stesso tempo, un elevato grado di utilizzabilità, per permettere al personale di sicurezza di ricevere, in tempo reale, le varie informazioni necessarie a gestire non solo la sicurezza ma anche le situazioni di emergenza [1-10].
Nei sistemi di sicurezza la gestione delle informazioni rappresenta un fattore molto importante per la funzionalità e l'efficienza dei sistemi stessi. Infatti, a causa della loro natura intrinseca, tali sistemi generano un considerevole flusso di informazioni che deve essere correttamente indirizzato, coordinato ed eventualmente memorizzato su supporti di memorizzazione temporanea o permanente, per evitare sovraccarichi o sovradimensionamento dei canali di comunicazione e dei dispositivi di memorizzazione.
Il sistema è opportunamente suddiviso in sottosistemi che sono:

1) il sottosistema di telecomunicazione;
2) il sottosistema di videosorveglianza;
3) il sottosistema controllo accessi;
4) il sottosistema antintrusione;
5) il sottosistema di rivelazione e spegnimento incendi;
6) il sottosistema di supervisione e controllo.

Il sistema garantisce un elevato grado di integrazione tra i differenti sottosistemi, assicurando un corretto ed immediato controllo di tutti i dati e di tutti gli eventi significativi per l'organizzazione e il controllo della sicurezza.
In questo modo è stato progettato un sistema le cui funzionalità sono nettamente superiori rispetto alle funzionalità dei vari sottosistemi.

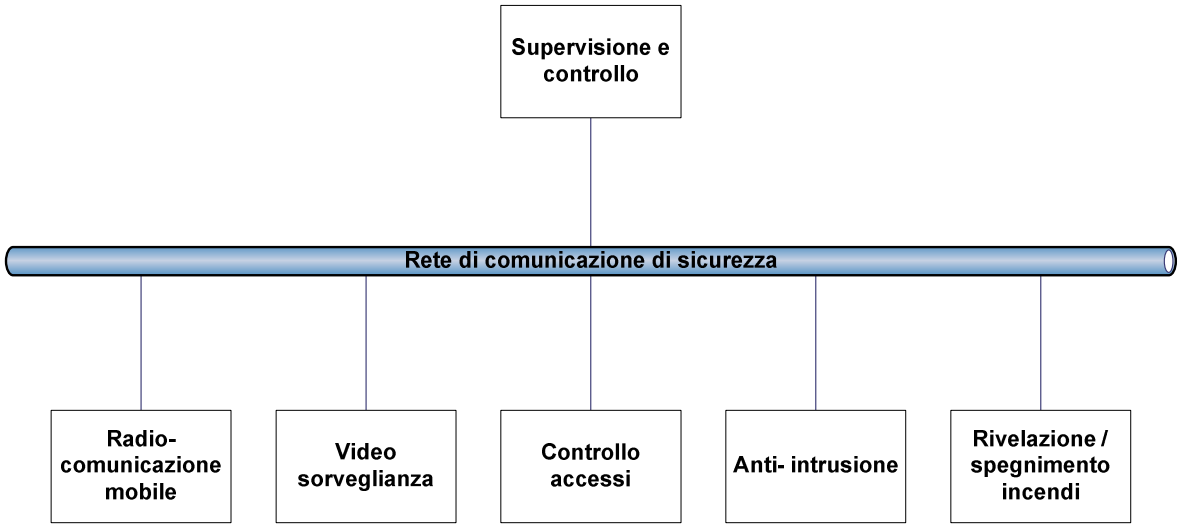


Fig.2 Schema del sistema integrato di sicurezza

Il sistema è stato progettato e realizzato per ridurre, il più possibile, l'impatto estetico sull'architettura dei palazzi del Senato, fornendo le sue funzionalità avanzate senza disturbare lo stile degli edifici da ogni punto di vista.
Il sistema è in grado di operare grazie ad un avanzato sistema di telecomunicazioni, caratterizzato da un'elevata affidabilità, che può lavorare in presenza di qualunque condizione critica. Il sistema di telecomunicazioni è a sua volta suddiviso in sistema fisso e sistema mobile.
Il sistema progettato e realizzato è caratterizzato da un elevato grado di modularità ed espandibilità così che è possibile, in ogni momento, aggiungere e integrare qualunque altro sottosistema, dispositivo o installazione in qualunque punto dei palazzi del Senato, garantendo sempre il pieno controllo di ogni componente.
Ogni componente del sistema è alimentato da fonti elettriche autonome in grado di funzionare anche in assenza dell'alimentazione principale.

Il sistema è controllato da un'opportuna sala di sicurezza principale e da alcune sale secondarie che permettono il totale controllo del sistema in caso di malfunzionamento o danneggiamento della sala principale.
Il sistema integrato è stato progettato e realizzato considerando anche gli aspetti psicologici ed ergonomici degli operatori delle sale di controllo, per evitare sovraccarichi di informazione che potrebbero provocare stress e riduzione del livello di attenzione, diminuendo le prestazioni degli stessi. Per tale motivo il flusso informativo viene elaborato e ridotto opportunamente in condizioni normali ed opportunamente incrementato in condizioni di emergenza, quando gli operatori della sala di controllo e il personale di sicurezza devono fronteggiare e gestire direttamente eventi che potrebbero diventare pericolosi per le persone e i beni.
Gli operatori e il personale di sicurezza sono opportunamente e continuamente formati e informati per renderli in grado di analizzare e gestire eventi pericolosi e per affrontare gli stessi attraverso procedure efficienti e funzionali, consentite dall'elevato grado di integrazione del sistema.
Il sistema è inoltre dotato di capacità di "disaster recovery" che rappresenta la possibilità di trasferire il controllo parziale o totale dell'intero sistema di sicurezza alle sale secondarie in caso di malfunzionamento o danneggiamento della sala principale. In tale maniera viene sempre assicurato il pieno controllo dell'intero sistema di sicurezza.
In questo modo è stato possibile realizzare un potente e versatile sistema integrato che garantisce un elevato livello di sicurezza al Senato della Repubblica.
Per motivi di riservatezza, il sistema integrato di sicurezza viene illustrato nella filosofia generale, senza illustrare i dettagli specifici che potrebbero compromettere la sicurezza del sistema stesso.

## 2. IL SOTTOSISTEMA DI TELECOMUNICAZIONE

Il sottosistema di telecomunicazione rappresenta la struttura portante del sistema integrato di sicurezza (videosorveglianza, controllo accessi, antintrusione, rivelazione e spegnimento incendi, ecc.), assicurando funzionalità e prestazioni avanzate.
Nel seguito verrà illustrata solo una sintesi delle principali caratteristiche.
Il sottosistema di telecomunicazione è composto da due sottosistemi fortemente integrati: l'infrastruttura fissa e l'infrastruttura mobile. Entrambe vengono illustrate nel seguito.
L'intero sottosistema di telecomunicazione viene controllato dalle sale operative che controllano non solo la sicurezza del Senato ma anche le funzionalità di ogni componente del sistema integrato, ivi incluso il sottosistema di telecomunicazione. Ogni malfunzionamento viene immediatamente segnalato agli operatori che possono attivare le relative procedure per garantire la massima funzionalità del sistema.
La progettazione del sottosistema di telecomunicazione è iniziata con l'analisi dei dati di sicurezza che devono essere trasportati dal sistema stesso.
I principali flussi di dati del sistema integrato sono generati dalle telecamere, dagli allarmi, dal controllo accessi, dalla comunicazione vocale e dai dati di controllo.
Una volta stimato il flusso totale di dati che devono essere trasportati dal sistema di telecomunicazione è stato possibile progettarlo, suddividendolo in sistema fisso e sistema mobile. Ogni sistema è stato progettato secondo i flussi di dati peculiari che devono essere trasportati, seguendo i criteri illustrati nel seguito.
Il sottosistema di telecomunicazione è totalmente separato dagli altri sistema di comunicazione del Senato, per evitare interferenze che potrebbero indebolire il sistema stesso.
Inoltre esso è stato progettato per garantire un'elevata affidabilità e disponibilità, utilizzando un'elevata ridondanza. In particolare, esso è equipaggiato con fonti energetiche totalmente autonome.
Il sottosistema di telecomunicazione viene continuamente ed automaticamente monitorato in maniera tale che ogni malfunzionamento viene immediatamente segnalato e riparato. Il software di controllo esamina ogni flusso di dati per controllare ogni irregolarità o sovraccarico del sistema. Inoltre, il sistema è stato progettato per garantire una elevata qualità del servizio e della classe dei servizi.

La rete di telecomunicazione è stata progettata in funzione dei differenti ambienti che devono essere serviti e dei protocolli che devono essere trasportati, per garantire un elevato livello di sicurezza e dei servizi.
La rete è stata progettata e realizzata per:

1) ridurre il più possibile i malfunzionamenti;
2) semplificare la gestione;
3) semplificare il riconoscimento dei vari dispositivi;
4) aumentare l'affidabilità grazie all'utilizzo della ridondanza;
5) garantire la futura espandibilità;
6) essere aperta a tutti i tipi di dispositivi;
7) garantire l'inter-operabilità dei differenti dispositivi.

Al fine di garantire una elevata velocità della trasmissione dei dati, sono state utilizzate connessioni a fibre ottiche ridondanti. Tutte le connessioni sono in grado di raggiungere velocità superiori a 10 Gbit/s.
L'architettura di rete è del tipo magliata-stellata, dove sono presenti 2 centri stella, collocati in opportuni locali protetti. In tal modo, un danneggiamento di un centro stella viene immediatamente gestito e recuperato dall'altro centro stella. Ogni palazzo è equipaggiato con un opportuno switch ridondato connesso alle dorsali principali per mezzo di 4 connessioni: 2 verso gli switch dei palazzi adiacenti e 2 verso i centri-stella. I due centri stella sono connessi per mezzo di una doppia connessione in fibra ottica. Ogni connessione della rete segue percorsi fisici differenti in maniera tale che l'interruzione di una connessione (volontaria o involontaria) venga immediatamente recuperata dalle altre. Questo tipo di architettura garantisce un elevato livello di affidabilità.

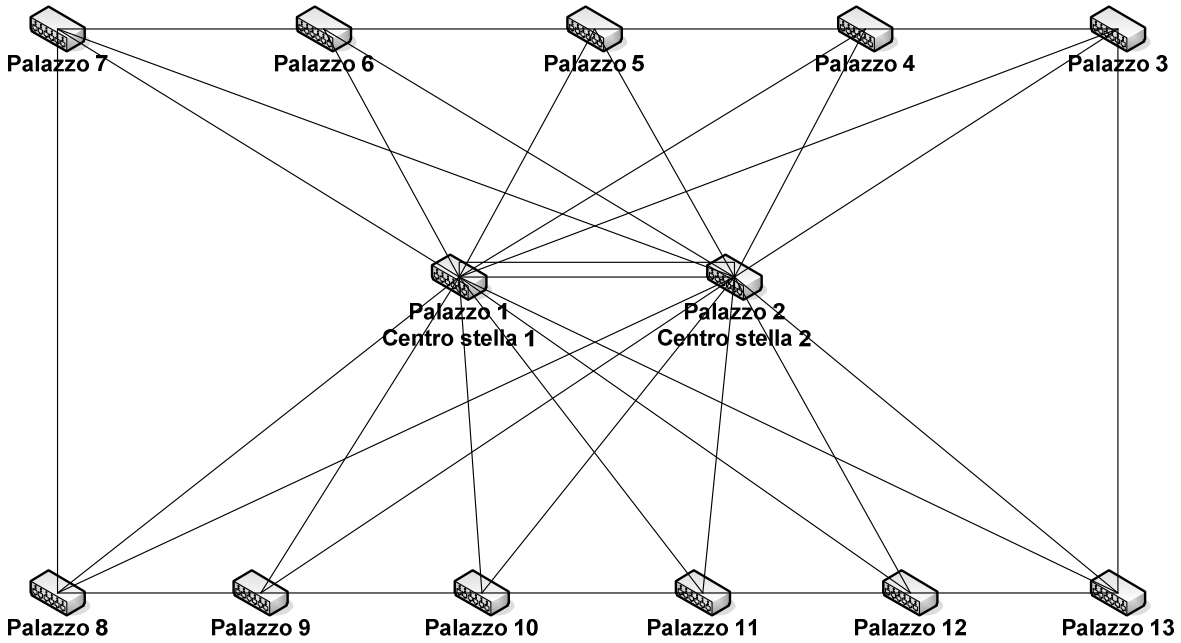


Fig.3 Schematizzazione dell'architettura di rete.

L'infrastruttura di rete fissa è stata progettata e realizzata considerando un modello gerarchico a tre livelli:

1) accesso;
2) distribuzione;
3) nucleo.

Il livello di accesso è rappresentato dai nodi più esterni della rete, chiamati anche foglie.
Le funzioni principali dei nodi sono rappresentate da:

1) introduzione del traffico all'interno della rete;
2) gestione della sicurezza;
3) gestione della banda (compressione, traffico, ecc.);
4) gestione delle congestione (meccanismi di gestione delle priorità, ecc.);

5) servizi proxy (DHCP, ecc.).

Il livello di distribuzione è rappresentato da una serie di funzionalità quali servizi di accesso, gestione e distribuzione delle informazioni di routing, definizione della metrica per la scelta dei percorsi migliori. I principali obiettivi di tale livello sono:

1) aggregazione del traffico proveniente dai nodi;
2) occultamento dei dettagli di rete al nucleo grazie all'aggregazione degli indirizzi IP;
3) controllo delle dimensioni delle tabelle di routing per mezzo di connessioni ridotte al nucleo;
4) gestione delle congestioni per mezzo di meccanismi di controllo delle priorità;
5) gestione della sicurezza per mezzo di liste di controllo accessi;
6) gestione della banda per mezzo di meccanismi di compressione e modellamento del traffico.

Il livello del nucleo svolge le seguenti funzionalità:

1) commutazione veloce del traffico IP;
2) gestione ottimizzata delle risorse di rete, banda, CPU, ecc.;
3) distribuzione del traffico attraverso percorsi dello stesso peso;
4) utilizzo di tecniche avanzate di qualità del servizio per la gestione delle politiche, delle congestioni e delle priorità.

Tutti i server relativi alla gestione della rete sono raggruppati in un'opportuna server farm. Tale server farm è composta da due server ridondati connessi mediante una doppia connessione. Tali server sono connessi ai due centri-stella per mezzo di una doppia connessione in maniera tale da assicurare una piena ridondanza.

Anche se le connessioni sono realizzate in maniera sicura e tutti i dispositivi sono posizionati in locali sicuri, a causa dell'estensione capillare della rete e per incrementare il livello di sicurezza del sistema, tutte le connessioni sono opportunamente cifrate per mezzo di opportuni dispositivi che permettono la creazione di LAN private virtuali (VPN).

Una serie di LAN virtuali (VLAN) sono definite per ogni switch di palazzo e per i due centri stella. Tali VLAN sono utilizzate per la connessione dei differenti dispositivi del sistema e per la connessione degli switch di palazzo con gli altri componenti dell'infrastruttura di rete.

Tutti gli impianti connessi al sistema scambiano informazioni reciprocamente e con le postazioni del sistema di supervisione: per tale motivo è stato necessario implementare opportune procedure di sicurezza per proteggere la server farm da possibili attacchi quali:

1) accessi non autorizzati;
2) diniego del servizio;
3) riconoscimento della rete;
4) virus and worm;
5) IP spoofing;
6) attacchi layer 2.

Le procedure di sicurezza sono progettate per evitare di ridurre le prestazioni della rete.

Per incrementare il livello di sicurezza della rete è stato introdotto un controllo accessi mediante autenticazione degli utenti e dei dispositivi.

L'infrastruttura di rete è dotata di un sistema di gestione e monitoraggio basato sul protocollo SNMP che assicura le seguenti funzionalità:

1) verifica periodica del corretto stato di funzionamento dei dispositivi;
2) elaborazione di statistiche dei dispositivi quali carichi, errori, carico della CPU, ecc.;
3) ricezione degli allarmi e degli eventi;
4) scoperta della rete ed individuazione automatica delle caratteristiche dei dispositivi trovati;
5) configurazione remota dei dispositivi (porte, VLAN, alberi, sicurezza, gestione del traffico, routing, filtraggio, ecc.);
6) aggiornamento automatico e centralizzato del firmware;
7) memorizzazione automatica della configurazione di ogni dispositivo di rete.

Il sottosistema di comunicazione mobile è progettato per permettere una rapida diffusione delle informazioni di sicurezza e una rapida risposta del personale coinvolto in ogni situazione di emergenza. Esso è fortemente integrato con gli altri componenti del sottosistema di telecomunicazione.

Il sottosistema di comunicazione mobile è basato sullo standard TETRA, una tecnologia espressamente sviluppata a livello di Comunità Europea per le comunicazioni di sicurezza.
A causa della varietà di problematiche presenti, è stato necessario progettare e realizzare un sistema radio ad accesso collettivo. Esso è in grado di soddisfare tutte le esigenze di sicurezza del Senato.
Il sistema radiomobile è composto da una serie di stazioni radio base (Base Station o BS, come nel sistema di telefonia cellulare GSM o UMTS) connesse ad un'unità centrale che gestisce e controlla il servizio dei terminali mobili degli utenti.
Il sistema è quindi composto da un centro di controllo, detto Master Site (MS), e da un numero variabile di BS posizionate nel territorio di interesse.
Ogni BS può supportare 4 canali radio per portante a radiofrequenza e può operare simultaneamente su portanti differenti.
Il Master Site è installato in una zona protetta della sala di controllo principale. La postazione di controllo principale è connessa direttamente al MS dove è possibile operare direttamente sul sistema radiomobile, programmando il database e il profilo degli utenti.
Il MS è connesso direttamente con la centrale telefonica per interfacciarsi con le linee telefoniche interne ed esterne.
Le unità radio sono caratterizzate da ridotte dimensioni e peso e da potenze di emissione controllabili, assicurando sempre la migliore qualità di comunicazione tra le unità radio e la più vicina BS. Tali unità sono dotate di un ricevitore GPS che assicura i servizi di localizzazione delle stesse e un'interfaccia Bluetooth per connettersi con un terminale esterno dove è possibile ricevere e controllare gli allarmi e le segnalazioni provenienti dal sistema di supervisione.
Il numero e la posizione delle BS è stato calcolato per mezzo di opportune e complesse simulazioni e studi di propagazione elettromagnetica (utilizzando algoritmi genetici per l'ottimizzazione): esse assicurano la piena copertura dei palazzi e dei relativi interni, rispettando i restrittivi limiti di emissione imposti alla legislazione vigente.
Il sistema radiomobile permette di servire, nello stesso momento, un numero predefinito di:

1) utenti;
2) gruppi di utenti;
3) chiamate contemporanee;
4) chiamate telefoniche contemporanee.

Le frequenze utilizzate variano nell'intervallo 380 – 400 MHz che assicurano una maggiore propagazione all'interno dei palazzi e nelle strette strade che circondano i palazzi, garantendo una copertura ottimale dell'area.
Nei sistemi radio ad accesso collettivo le frequenze vengono assegnate dinamicamente, secondo necessità, permettendo una gestione efficiente e dinamica del sistema.
Il sistema radiomobile permette inoltre l'interconnessione con le linee telefoniche interne ed esterne, garantendo un elevato livello di connettività.
La tecnologia digitale utilizzata assicura i seguenti vantaggi:

1) migliore qualità della comunicazione vocale;
2) maggiore velocità di trasmissione e ricezione;
3) minore dipendenza dal livello del segnale ricevuto;
4) maggiore sicurezza delle conversazioni grazie agli algoritmi criptografici utilizzati;
5) possibilità di utilizzare i terminali mobili non solo come telefoni ma anche come terminali dati per trasmettere e ricevere ogni tipo di informazione;
6) localizzazione dei terminali mobili grazie al ricevitore GPS integrato.

Ogni connessione radio è divisa in 4 canali differenti che possono essere utilizzati singolarmente o insieme in funzione della banda di trasmissione necessaria.
Il sottosistema radiomobile controlla continuamente la qualità della codifica/decodifica vocale, permettendo un servizio di comunicazione anche in presenza di rumore.
Il sistema permette un'autenticazione multi-livello degli utenti (utente-sistema mobile; sistema mobile-rete fissa; rete–rete; utente–utente), utilizzando algoritmi criptografici ad elevata sicurezza. Esso supporta un profilo multi-traffico che permette servizi voce e dati nello stesso momento sullo stesso terminale. Il traffico voce è basato sul tecnologia di trasmissione TDMA (Time Division Multiplexing Access) mentre il traffico dati è basato sulla tecnologia PDO (Packet Data Optimized).

La tecnologia PDO permette inoltre la piena compatibilità con il protocollo TCP/IP ed i relativi servizi.
Grazie al ricevitore GPS integrato nei terminali mobili, è possibile vedere sopra mappe opportune, all'interno delle sale operative, la posizione degli utenti, aumentando enormemente la qualità e le procedure di sicurezza e di emergenza.
Il sistema radiomobile utilizza due tipi di canali logici;

1) controllo;
2) traffico.

I canali di controllo trasportano le informazioni di segnalazione. I terminali radio, quando non sono impegnati in una comunicazione, ascoltano continuamente i canali di controllo dove ricevono informazioni riguardanti la rete (disponibilità di celle vicine, servizi disponibili, stato dei canali, ecc.) e possono fare le loro richieste per iniziare un particolare servizio.
I canali di traffico trasportano le informazioni relative alla voce e ai dati. I canali di traffico (da 1 a 4 per ogni frequenza utilizzata secondo il servizio richiesto) vengono assegnati ai terminali mobili dal sistema e rilasciati dai terminali o dalla rete quando il servizio è terminato.

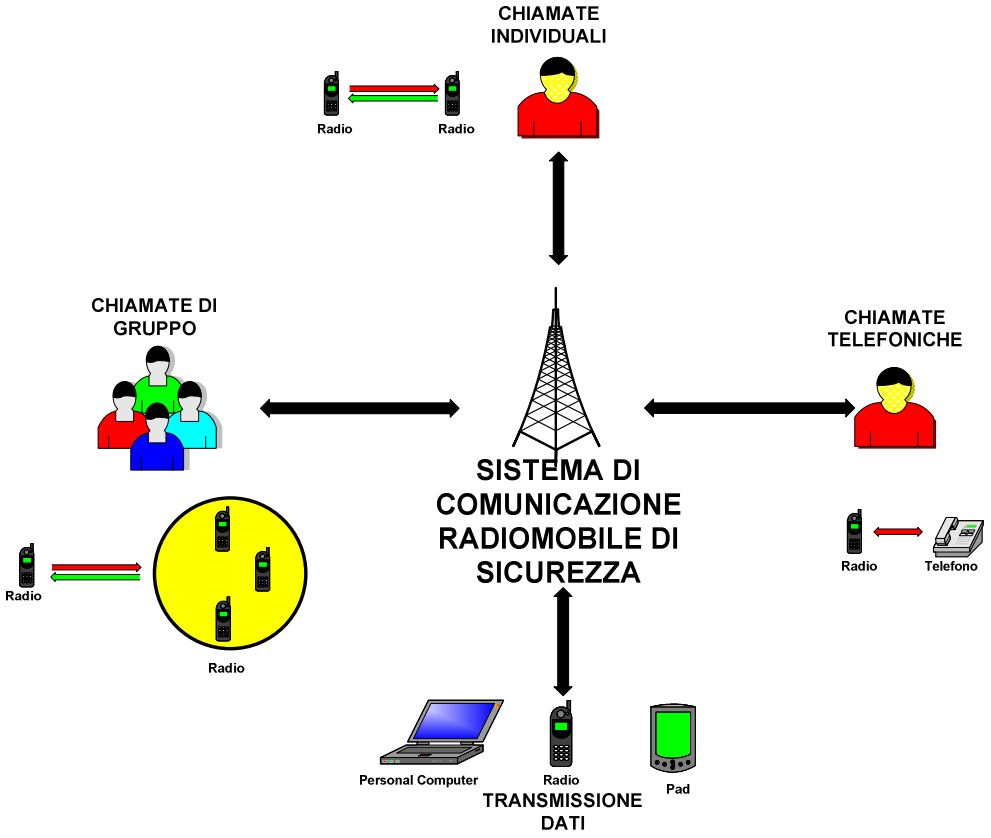


Fig.5 Principali funzionalità del sistema di comunicazione mobile.

Il sistema radiomobile offre i seguenti servizi vocali:

1) chiamate individuali: tale servizio è equivalente alla comunicazione attraverso un telefono cellulare (un utente chiama un altro utente);
2) chiamate di gruppo: un utente chiama un gruppo predefinito. Ogni membro del gruppo può parlare ed ascoltare gli altri membri del gruppo. Il gruppo viene definito in maniera flessibile, cioè ogni utente può essere aggiunto o cancellato dal gruppo in ogni momento;
3) chiamata diretta: due o più terminali radio comunicano direttamente senza il supporto della stazione radio base;

4) chiamata pubblica: che rappresenta una chiamata undirezionale punto –multipunto in una certa zona. Le zone e gli utenti possono essere definiti dinamicamente;
5) chiamata di emergenza: che permette di effettuare una chiamata ad elevata priorità premendo un pulsante di emergenza sull'unità radio;
6) chiamata inclusiva: che permette di chiamare o inserire in una chiamata uno o più utenti supplementari;
7) canale aperto: un gruppo di utenti può conversare su un determinato canale radio e tutti gli utenti possono ascoltare o parlare in qualunque momento.

Il sistema radiomobile offre i seguenti servizi dati:

1) trasmissione di stato: che permette di trasmettere messaggi corti e predefiniti dalla rete alle unità mobili e viceversa;
2) servizio dati corti: che permette di inviare messaggi predefiniti ad utenti singoli o gruppi di utenti;
3) trasmissione dati utilizzando una modalità di commutazione di circuito;
4) trasmissione dati utilizzando una modalità a commutazione di pacchetto (X25, TCP/IP).

Inoltre, il sistema radiomobile è caratterizzato da un'elevata sicurezza attraverso:

1) utilizzo di autenticazione mutua (unità radio – staziona radio base e viceversa);
2) comunicazioni crittografate utilizzando sia chiavi statiche che chiavi dinamiche;
3) supporto di comunicazioni "end to end" crittografate;
4) disabilitazione delle unità radio perse o rubate;
5) organizzazione dei dati direttamente attraverso la rete IP utilizzando protocolli cifrati.

## 3. IL SOTTOSISTEMA DI VIDEOSORVEGLIANZA

Il sottosistema di videosorveglianza (SVS) è progettato per permettere agli operatori di controllare ogni zona dei palazzi e di ricostruire, in un secondo momento, ogni evento grazie alle elevata capacità di memorizzazione del sottosistema stesso. Esso integra, inoltre, gli allarmi provenienti dagli altri sottosistemi, fornendo un accesso visivo alle zone allarmate.
L'integrazione con gli altri sottosistemi viene realizzata per mezzo di:

1) sistema di supervisione, che rappresenta l'elemento centrale per l'organizzazione dell'intero sistema di sicurezza;
2) integrazione diretta, ottenuta attraverso la connessione diretta dei differenti componenti degli altri sottosistemi.

Il SVS utilizza i servizi di comunicazione offerti dalla rete di sicurezza, descritta in precedenza, per trasmettere immagini, sia in tempo reale che registrate, agli operatori interessati. L'accesso alle immagini registrate è ovviamente controllato per rispettare le normative nazionali sulla privacy.
Il SVS è in grado di individuare ogni tentativo di intrusione attraverso i perimetri dei palazzi. Per tale motivo è necessario trasmettere, in tempo reale, tutte le immagini utili a valutare gli eventi o essere aiutati da opportuni dispositivi automatici che analizzano le scene riprese e generano un allarme per l'operatore solo nelle situazioni critiche.

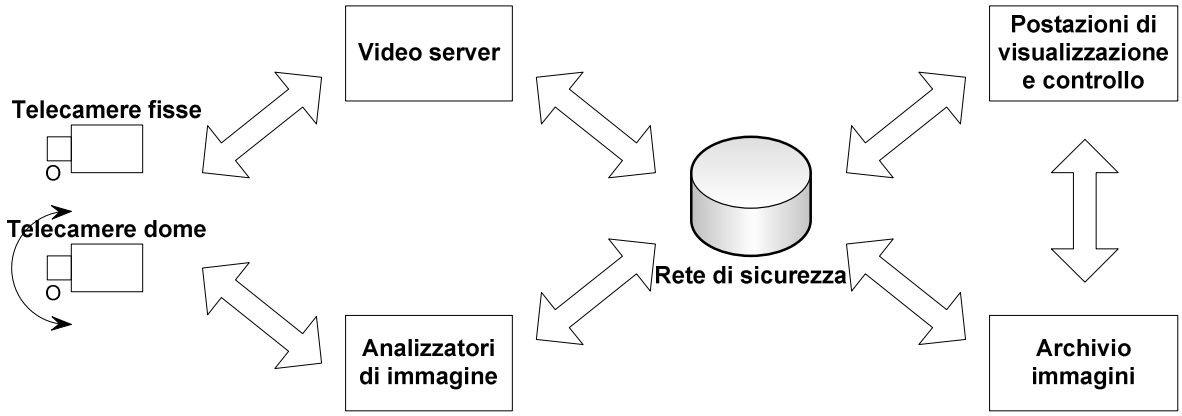


Fig.6 Schema del sottosistema di videosorveglianza.

L'acquisizione delle immagini viene fatta attraverso un inquadramento ottimale delle aree controllate, utilizzando sia obiettivi grandangolo che obiettivi ad angolo ristretto, secondo le caratteristiche delle zone.
Il SVS è anche dotato di elevate capacità di memorizzazione ed è in grado di:

1) registrare le immagini provenienti da tutte le telecamere;
2) permettere un facile accesso all'archivio delle immagini per analizzare, in un secondo momento, ogni evento critico.

Il SVS è stato progettato e realizzato per garantire un elevato standard di efficienza, qualità, scalabilità, apertura, flessibilità operativa, affidabilità e sicurezza.
Il SVS è basato su di un'architettura mista analogica/digitale. Tutte le telecamere sono analogiche, per garantire un'elevata qualità delle immagini che devono essere analizzate, localmente, da opportuni dispositivi di analisi. Le immagini vengono convertite localmente, per mezzo di opportuni video server, ed inviate verso le sale di controllo e verso le altre postazioni che hanno bisogno delle stesse, utilizzando il protocollo TCP/IP: Il SVS è composto dai seguenti elementi:

1) telecamere: vengono utilizzati 2 differenti tipi di telecamere: fisse, per controllare gli ingressi dei palazzi; dome, per controllare le aree esterne;
2) video server: essi convertono il segnale analogico proveniente dalle telecamere in segnale digitale da inviare attraverso la rete dedicata di sicurezza;
3) analizzatori di immagine: essi analizzano le immagini provenienti dalle telecamere, mediante tecniche ed algoritmi avanzati, per rivelare, automaticamente, situazioni critiche. I relativi allarmi vengono inviati agli operatori delle sale attraverso la rete di telecomunicazione;
4) postazioni di controllo e visualizzazione: le postazioni sono presenti nei seguenti punti: sala di controllo principale; portinerie dei palazzi;
5) sistema di registrazione: esso memorizza tutte le immagini provenienti dalle telecamere attraverso la rete ed è collocato nella sala di controllo principale. L'accesso all'archivio delle immagini è opportunamente protetto per rispettare le norme sulla privacy;
6) rete di telecomunicazione: essa rappresenta l'ossatura portante dell'interno sistema di sicurezza ed è stata già illustrata in precedenza. Essa permette la comunicazione tra tutte le componenti del sistema di videosorveglianza.

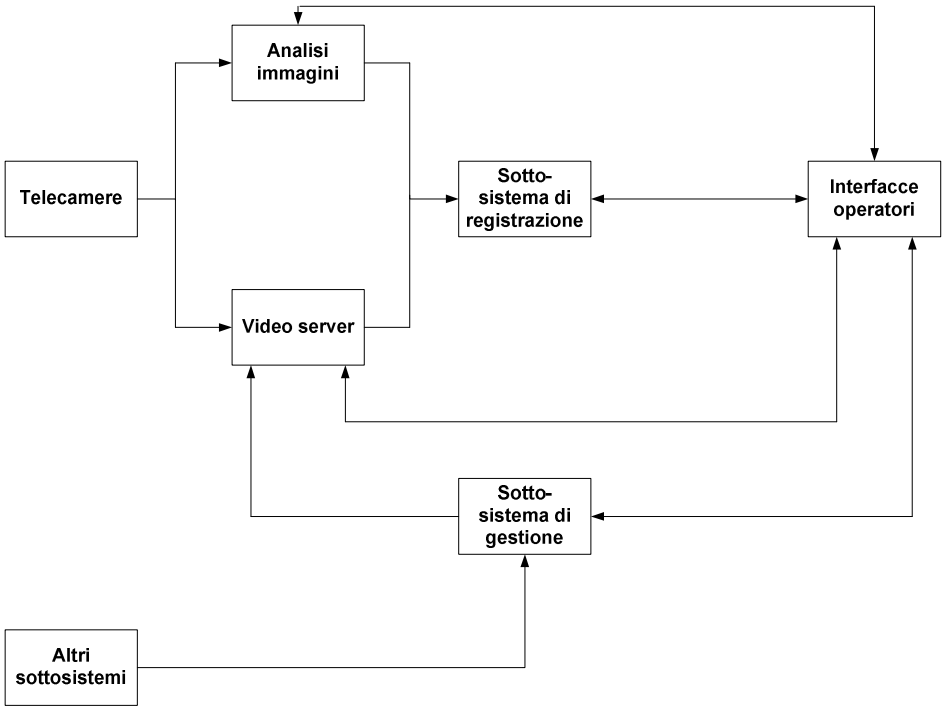


Fig.7 Architettura logica del sistema di videosorveglianza.

Il SVS è composto dai seguenti elementi logici:

1) dispositivi di campo (telecamere);
2) dispositivi di digitalizzazione;
3) dispositivi di analisi delle immagini;
4) dispositivi di registrazione;
5) dispositivi di gestione;
6) interfacce operatore.

Il SVS può essere considerato come diviso in tre tipologie di elementi:

1) periferiche: composte dalle telecamere (fisse e dome con commutazione automatica day&night), illuminatori all'infrarosso, dispositivi di analisi di immagine, video server;
2) punti di accesso: rappresentati dalle postazioni delle sale operative e delle portinerie. Esse permettono il pieno accesso (secondo le loro funzionalità e finalità) alle immagini in diretta; l'accesso alle immagini registrate è ristretto a particolari operatori secondo le normative sulla privacy. In particolare, nelle sale di controllo sono presenti non solo monitor LCD ma anche maxi schermi al plasma dove è possibile visualizzare le immagini di interesse. Particolare attenzione è stata rivolta nella progettazione dell'interfaccia uomo-macchina dal punto di vista del controllo. Infatti, tutti i controlli vengono eseguiti per mezzo di interfacce semplificate quali menù guidati, tastiere e joystick, riducendo il più possibile la complessità e rendendoli familiari all'uso. In tal modo lo stress degli operatori viene ridotto, rendendoli in grado di affrontare qualunque evento critico con la necessaria concentrazione;
3) centro di controllo: rappresentato da tutti i dispositivi dedicati alle gestione e al controllo dell'intero sottosistema (server, registratori, ecc.).

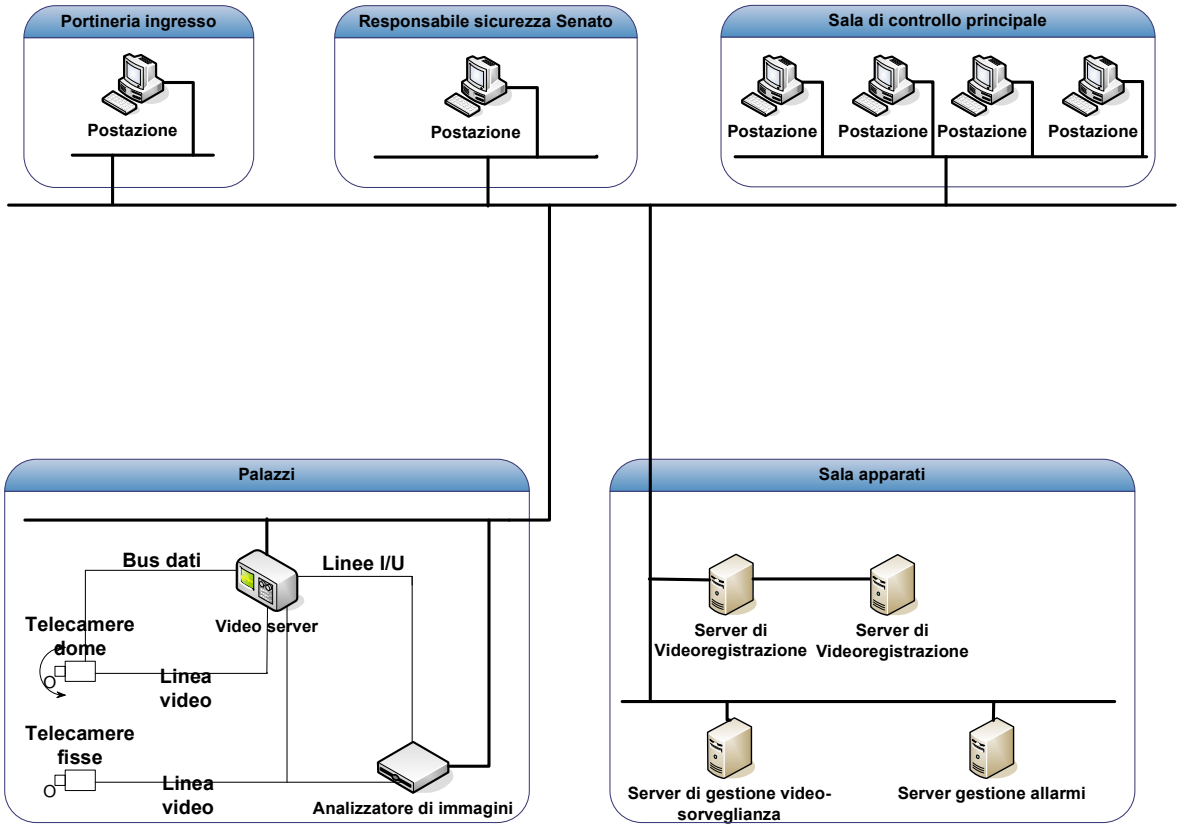


Fig.8 Architettura fisica del sottosistema di videosorveglianza.

## 4. IL SOTTOSISTEMA DI CONTROLLO ACCESSI

Il sottosistema di controllo accessi (SCA) controlla tutti gli ingressi dei palazzi e dei locali delle centrali tecnologiche.
Esso è caratterizzato da un'elevata modularità così che è possibile aggiungere in qualunque momento ulteriori ingressi senza alcun problema.

Il SCA utilizza badge a mani libere (a radiofrequenza) insieme con un riconoscimento biometrico del volto degli utenti mentre tutti gli eventi vengono opportunamente visualizzati e registrati per mezzo del sottosistema di videosorveglianza. Localmente è anche presente uno schermo che mostra il volto della persona entrante insieme con l'immagine registrata nell'archivio per consentire un immediato riconoscimento visivo da parte del personale di sicurezza degli ingressi.
Il SCA permette:

1) l'identificazione delle persone;
2) la gestione delle aree interne in funzione del livello di sicurezza richiesto;
3) un maggior livello di sicurezza degli ambienti lavorativi;
4) una maggior protezione dei beni;
5) una riduzione dei costi grazie ad un uso più razionale delle risorse umane;
6) un doppio livello di protezione (persone e beni);
7) un elevato livello di sicurezza poiché è possibile conoscere, in situazioni di emergenza, l'esatto numero di persone presenti in ciascun palazzo;
8) un'opportuna integrazione con il sistema di sicurezza per ottenere funzionalità avanzate.

Il SCA è basato su di un'architettura distribuita con un archivio centrale e vari archivi locali. In tal modo, in caso di perdita temporanea della rete, il sottosistema è in grado di operare senza alcun problema, aggiornando l'archivio centrale quando la comunicazione viene ripristinata.
Il SCA è composto dai seguenti elementi principali:

1) server centrale;
2) server biometrico centrale;
3) server locale;
4) controllore d'ingresso;
5) postazione di portineria.

Il server centrale memorizza i profili degli utenti, le configurazione di installazione, lo storico degli allarmi e degli eventi. Esso duplica tali informazioni sui server locali.
Il server biometrico centrale memorizza le immagini dei volti degli utenti, importando le relative informazioni e i profili dal server centrale. Esso duplica tali informazioni sui server locali.
I server regionali memorizzano tutte le informazioni relative agli utenti e tutto lo storico degli allarmi e degli eventi che si sono verificati negli ingressi controllati. Essi comunicano con il server centrale e con il server biometrico centrale per mantenere aggiornato l'archivio centrale.
I controllori di ingresso lavorano come interfacce tra i server locali e i lettori di badge, i sensori e le serrature elettriche degli ingressi automatici.
Le postazioni di ingresso sono posizionate vicino agli ingressi e vengono utilizzate dal personale di sicurezza. Esse permettono:

1) di visualizzare i transiti e il volto delle persone che accedono;
2) di gestire gli allarmi;
3) di gestire gli ingressi;
4) di controllare lo stato di ogni dispositivo di ingresso (sensori, attuatori, lettori di badge, ecc.);
5) configurare i componenti locali del SCA.

Ogni operazione eseguita dagli operatori viene opportunamente registrata nel SCA ed è disponibile per essere controllata in un secondo momento.
I lettori di badge a radiofrequenza rispettano tutte le normative internazionali e nazionali concernenti l'esposizione umana ai campi elettromagnetici e sono caratterizzati da un ridotto livello di emissione.
I badge sono composti da tre sezioni:

1) radiofrequenza;
2) banda magnetica;
3) microchip;

per poter essere utilizzati con tutti i servizi operativi interni del Senato.
In caso di malfunzionamento di una modalità di ingresso (badge a radiofrequenza o riconoscimento del volto), i varchi possono essere abilitati a lavorare in modalità singola invece che doppia per garantire l'accesso alle persone. In tale modalità il personale di sicurezza viene coadiuvato dalla

comparazione, sul monitor disponibile, del volto della persona entrante con quello memorizzato nell'archivio.
Opportune postazioni sono installate nell'ufficio permessi e sono dedicate alle generazione e alla stampa dei badge e alla memorizzazione delle immagini dei volti degli utenti.

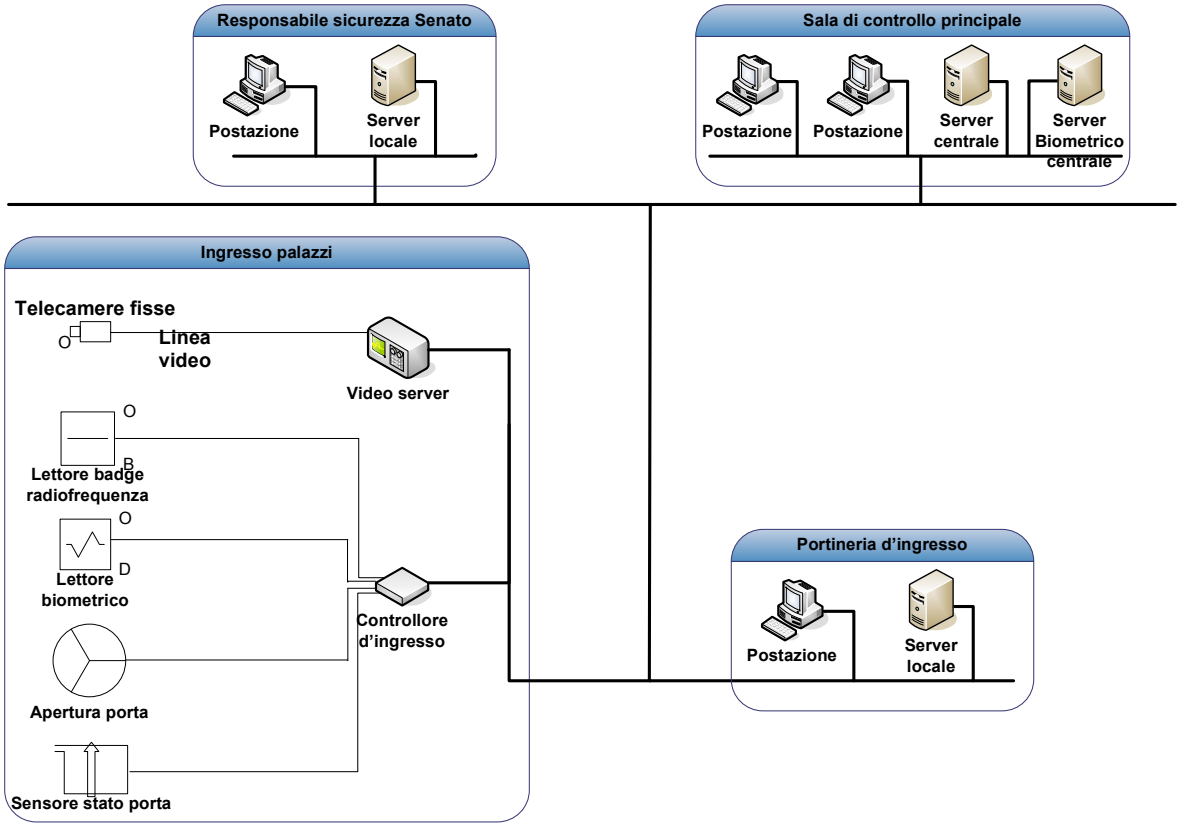


Fig.9 Architettura fisica del sottosistema di controllo accessi.

## 5. IL SOTTOSISTEMA ANTINTRUSIONE

Il sottosistema antintrusione (SAI) è dedicato al controllo perimetrale dei palazzi e all'acquisizione degli allarmi interni attivati per mezzo di opportuni pulsanti. Esso utilizza adeguati moduli di ingresso/uscita (I/U) che acquisiscono le informazioni dai sensori sul campo e le inviano, attraverso la rete, alle postazioni di controllo delle sale operative. Esso permette:

1) la concentrazione degli allarmi verso le postazioni di controllo;
2) il controllo dei dispositivi sul campo per informare il sistema centrale, in tempo reale, di eventuali anomalie e malfunzionamenti che richiedono opportune procedure di riparazione;
3) l'interfacciamento con gli altri sottosistemi, in particolare con la videosorveglianza, per attivare procedure congiunte in caso di allarme (quali l'attivazione della telecamera più vicina per vedere le zone allarmate).

Il SAI, come gli altri sottosistemi, è totalmente autonomo ed auto-consistente in maniera tale che sia in grado di operare anche in assenza del controllo del sottosistema di supervisione.
I sensori sul campo sono rappresentati da:

1) barriere perimetrali sui terrazzi;
2) contatti magnetici su porte e finestre;
3) pulsanti antiaggressione;
4) pulsanti di allarme portatili a radiofrequenza.

Il SAI è caratterizzato da un'elevata modularità in maniera tale che è possibile aggiungere in qualunque punto ulteriori moduli I/U, grazie alla presenza capillare della rete di sicurezza in ogni palazzo, e ulteriori sensori.

I moduli I/U si possono connettere ai sensori di campo per mezzo di connessioni dirette o per mezzo di bus seriale. Essi possono essere programmati per interfacciarsi con ogni tipo di dispositivo e protocollo di comunicazione.
Tutti gli allarmi ed eventi sono mostrato sulle postazioni delle sale di controllo.

## 6. IL SOTTOSISTEMA DI RIVELAZIONE/SPEGNIMENTO INCENDI

Il sottosistema di rivelazione/spegnimento incendi (SRSI) è in grado di controllare ogni punto dei palazzi, permettendo al personale, grazie alle opportune postazioni, di essere informato immediatamente in caso di incendio.
Esso è composto da differenti centrali (una o più d'una centrale per palazzo), installate nelle portinerie di ingresso dei palazzi dove è sempre presente il personale di sicurezza. Le centrali sono interfacciate con la postazione di portineria dove vengono mostrate le zone allarmate attraverso opportune mappe grafiche per permettere una rapida localizzazione degli incendi. Tale postazione permette una visione diretta della zona allarmata attraverso la più vicina telecamera del sottosistema di videosorveglianza. Le centrali sono ulteriormente interfacciate con il sistema centrale di supervisione e controllo per segnalare gli eventi incidentali anche nelle sale operative.
Il SRSI è complementato da un sistema di diffusione vocale (SDV). Ogni postazione di portineria è interfacciata con il SDV per permettere una immediata diffusione locale dei messaggi. Ogni SDV è interfacciato con il sistema di supervisione e controllo centrale, attraverso la rete di sicurezza, in maniera tale che è possibile, dalle sale di controllo, inviare messaggi vocali alle differenti zone dei palazzi.

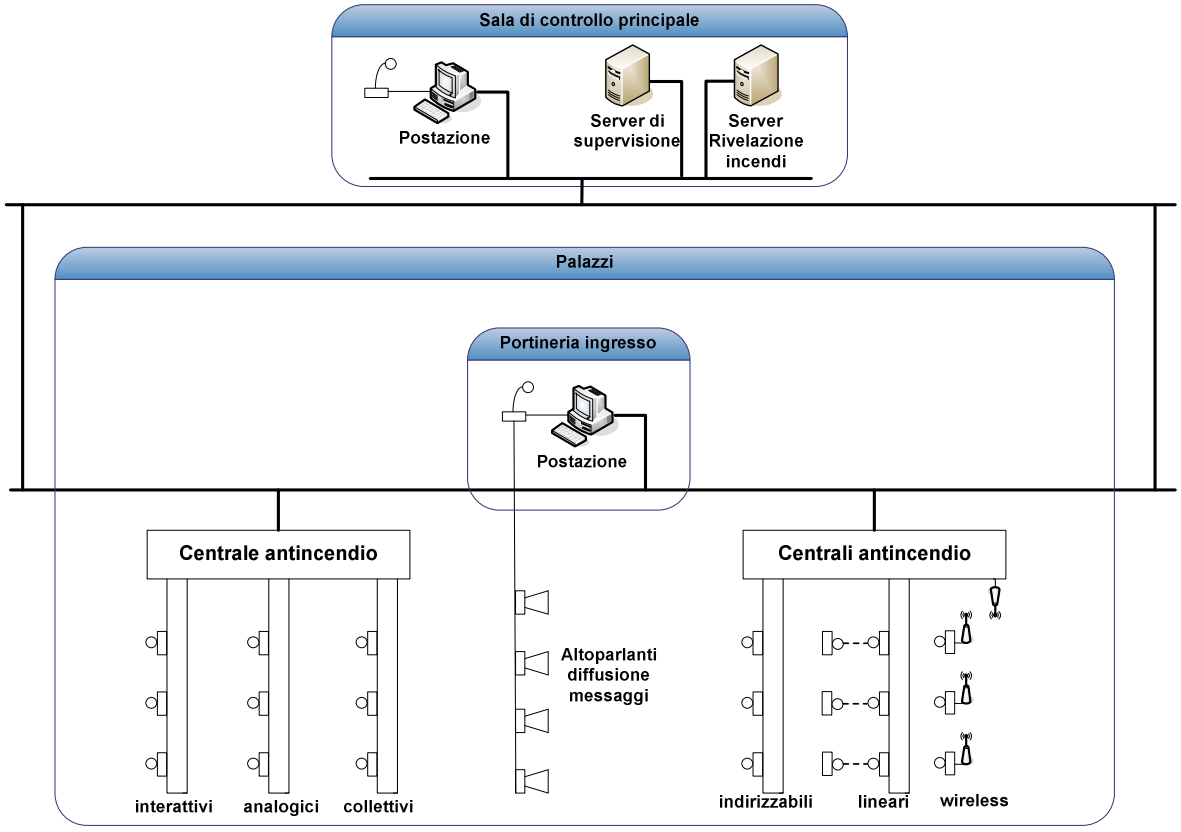


Fig.10 Architettura del sottosistema di rivelazione incendi.

Il SDV è inoltre dotato di differenti canali audio ed è in grado di emettere sia messaggi pre-registrato che messaggi diretti degli operatori.
La suddivisione del SRSI in differenti centrali (centrali locali) assicura una elevata affidabilità ed una capacità di operare anche in presenza di perdita delle componenti di controllo gerarchicamente superiori (postazioni locali, rete di comunicazione, sale di controllo).

Il SRSI utilizza vari tipi di rivelatori in funzione degli ambienti controllati. Essi sono rappresentati da:

1) rivelatori interattivi;
2) rivelatori analogici;
3) rivelatori collettivi;
4) rivelatori indirizzabili;
5) rivelatori a barriera lineare;
6) rivelatori wireless.

Tutti i sensori sono stati installati seguendo le normative nazionali ed internazionali.
Nelle centrali tecnologiche sono inoltre installati sensori di gas (anidride carbonica, metano, idrogeno, ecc.).
Le centrali antincendio sono anche connesse a:

1) pulsanti di segnalazione incendi;
2) pannelli luminosi di allarme lampeggianti;
3) magneti di ritenuta delle porte tagliafuoco;
4) impianti di spegnimento incendi.

Tulle le condotte di adduzione dell'aria climatizzata sono opportunamente controllate da unità di analisi dell'aria.
Un opportuno server di integrazione è installato nella sala di controllo. Esso viene utilizzato per interfacciare tutte le centrali antincendio con il sistema di supervisione e controllo.

## 7. IL SOTTOSISTEMA DI SUPERVISIONE E CONTROLLO

Il sottosistema di supervisione e controllo (SSC) rappresenta l'elemento integrante dei differenti sottosistemi (anche se questi ultimi sono anche connessi in alcuni casi a livello più basso) offrendo funzionalità superiori rispetto alle funzionalità offerte dai sottosistemi separatamente.
Esso permette l'ottimizzazione delle procedure di gestione e controllo, riportando tutte le segnalazioni e gli allarmi sulle postazioni delle sale di controllo.
Il SSC utilizza una piattaforma software di tipo aperto estremamente flessibile e programmabile in maniera tale da semplificare l'utilizzo e l'espansione futura per aggiungere nuovi componenti in un secondo momento.
Il SSC utilizza la rete di comunicazione dedicata per scambiare le informazioni con i vari sottosistemi e per controllarli, anche se questi ultimi sono totalmente autonomi dal SSC, essendo in grado di operare anche in assenza di coordinamento.
Le avanzate funzionalità del SSC sono disponibili sulle postazioni delle sale di controllo anche se qualunque postazione può essere aggiunta in ogni punto del Senato per necessità particolari o temporanee grazie alla diffusione capillare della rete di comunicazione dedicata.
Tutte le informazioni vengono mostrate su opportune mappe, per permettere una chiara ed immediate visione e organizzazione degli eventi attraverso appositi pulsanti software presenti sulle mappe stesse.
Tutti gli allarmi e le segnalazioni e le azioni degli operatori vengono memorizzate nell'archivio storico del SSC.
Il SSC è caratterizzato da:

1) integrazione con gli altri sottosistemi;
2) autonomia dagli altri sottosistemi;
3) espandibilità;
4) scalabilità;
5) flessibilità operativa;
6) affidabilità;
7) elevato livello di sicurezza.

Esso può controllare:

1) singoli sensori e telecamere;
2) interi impianti;
3) ogni altro elemento e dispositivo sul campo.

Esso è composto da:

1) server centrali ridondanti;
2) postazioni di controllo;
3) rete di telecomunicazione di sicurezza.

L'architettura logica permette di suddividere il SSC in due moduli funzionali:

1) il modulo di controllo;
2) il modulo operatore.

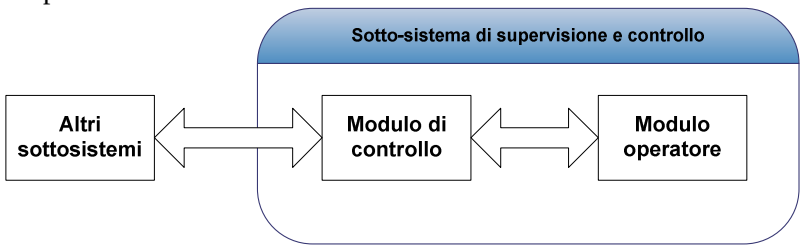


Fig.11 Architettura logica del sottosistema di supervisione e controllo.

Il modulo di controllo è composto da tre sotto-moduli:

1) acquisizione dati;
2) elaborazione dati;
3) gestione operatore.

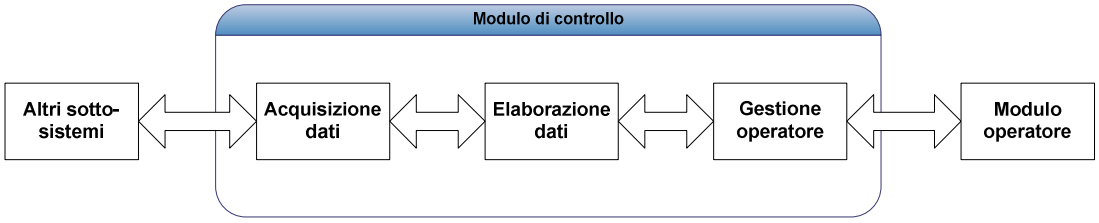


Fig.12 Architettura logica del modulo di controllo.

Il sotto-modulo di acquisizione dati si occupa dell'interfacciamento con gli altri sottosistemi, gestendo tutte le problematiche relative alle connessioni con gli altri impianti e relative alla codifica/decodifica dei messaggi (protocolli di comunicazione). Esso principalmente adatta i dati ricevuti dai sensori sul campo e dagli impianti in un formato standard utile per il modulo di controllo.

Il sotto-modulo di elaborazione dati rappresenta il nucleo del sottosistema e si occupa di controllare i dati, generare gli allarmi ed attuare le azione associate agli allarmi. Esso può operare sotto la supervisione degli operatori o automaticamente secondo procedure predefinite. Le azioni automatiche possono essere suddivise in:

1) memorizzazione della variazione di stato nell'archivio storico;
2) generazione di allarmi e notifica all'operatore di postazione interessato;
3) memorizzazione degli allarmi nell'archivio storico;
4) attivazione, senza ausilio dell'operatore, di comandi pre-definiti dopo un'opportuna segnalazione;
5) riproduzione di un file audio, sulla postazione dell'operatore interessato, per segnalare un particolare evento;
6) apertura automatica di una finestra sullo schermo, sulla postazione dell'operatore interessato, per mostrare le immagini relative ad un particolare evento;
7) apertura automatica di una mappa sinottica, sulla postazione dell'operatore interessato, per mostrare un particolare evento.

Il sotto-modulo di gestione operatore controlla lo scambio di informazioni con gli operatori, rispondendo alle richieste delle interfacce e inviando loro tutti i dati.

Il modulo operatore rappresenta l'elemento del SSC che interagisce con gli operatori.

Il modulo operatore è costituito da due differenti sotto-moduli:

1) supervisione e controllo;
2) configurazione e gestione.

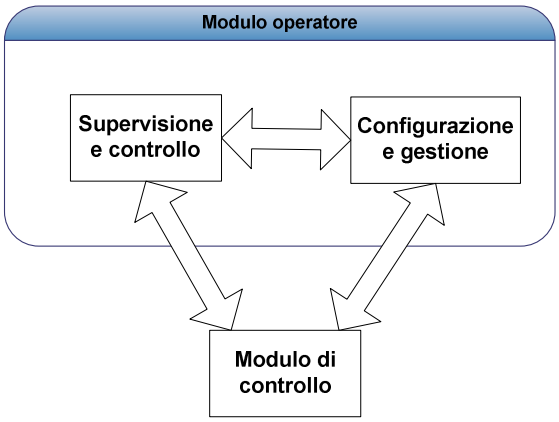


Fig.13 Architettura logica del modulo operatore.

Il sotto-modulo di supervisione e controllo si occupa dell'interfacciamento con gli operatori per consentire il pieno controllo dei sottosistemi.
Il sotto-modulo di configurazione e gestione permette al personale specializzato di configurare e gestire l'intero sistema. Esso è controllabile attraverso una postazione dedicata, il cui accesso è opportunamente protetto.
Entrambi i sotto-moduli comunicano con il modulo di controllo, in particolare con il sotto-modulo gestione operatore per:

1) ricevere la segnalazione degli eventi provenienti dai sotto-sistemi controllati e inviare loro le azioni da eseguire;
2) inviare le informazioni di configurazione.

## 8. CONCLUSIONI

La gestione della sicurezza in contesti complessi quali il Senato della Repubblica Italiana necessita di una dettagliata analisi dei rischi e un corretto studio, progettazione e realizzazione di un efficiente sottosistema di telecomunicazione che sia in grado di integrare i differenti sottosistemi di sicurezza, grazie all'ausilio di un sottosistema di supervisione e controllo, assicurando la massima interazione reciproca tra i differenti sottosistemi coinvolti.
In tal modo è stato possibile realizzare un potente e versatile sistema di sicurezza integrato che garantisce un elevato livello dei servizi di sicurezza del Senato della Repubblica Italiana.

**Bibliografia**

[1] E. Waltz, "Information Warfare – Principles and operations", Artech House Publisher, Boston (USA), 1998.
[2] D.E. Denning, "Information Warfare and Security", Addison-Wesley, Boston (USA), 1999.
[3] R.K. Nichols, P.C. Lekkas, "Wireless Security: Models, Threats, and Solutions", McGraw-Hill", New York (USA),2002.
[4] F. Garzia, "The integrated safety/security system of the Accademia Nazionale dei Lincei at Corsini Palace in Rome", *Proc. of International Conference on Integrating Historic Preservation with Security, Fire Protection, Life Safety and Building Management Systems*, Rome (Italy), pp.77-99, 2003.
[5] F. Garzia, G. M. Veca, "Integrated security systems for hazard prevention, management and control in the Italian high speed train line", *Risk Analysis III*, WIT Press, Southampton (UK), pp.287-293, 2002.
[6] E. Antonucci, F. Garzia, G. M. Veca, "The automatic vehicles access control system of the historical centre of Rome", *Sustainable City II*, WIT Press, Southampton (UK), pp.853-861, 2002.
[7] F. Garzia., E. Sammarco, M. De Lucia., "The security telecommunication system of the Vatican City State", *Risk Analysis IV*, WIT Press, Southampton (UK), pp.773-782, 2004.
[8] F. Garzia, E. Sammarco, "The integrated security system of the Vatican City State", *SAFE 2005*, WIT Press, Southampton (UK), pp.391-403, 2005.
[9] F. Garzia, "The integrated supervision and control system of the Gran Sasso mountain", *SAFE 2005*, WIT Press, Southampton (Boston), pp.699-711, 2005.
[10] F. Garzia, E. Sammarco, R. Cusani, "The integrated access control system of the Vatican City State", *SAFE 2007*, WIT Press, Southampton (UK), pp.431-440, 2007.