

Il sistema integrato di sicurezza dello Stato Città del Vaticano

Autori: Tullio Bucciarelli¹, Fabio Garzia¹, Gianluca Gauzzi², Massimo Guarascio¹, Enzo Sammarco²

¹Ingegneria della Sicurezza a Protezione
Università degli Studi di Roma “La Sapienza” – Polo di Civitavecchia
Via dei Poggi, n. 18 - Civitavecchia, Italia
Tel. 0644585626 - Fax 0644585816 - e-mail fabio.garzia@uniroma1.it
w3.uniroma1.it/sicurezza

²Direzione Generale Sicurezza e Protezione Civile
Stato Città del Vaticano

Sommario

La gestione della sicurezza, per strutture complesse ed articolate, quali quelle dello Stato Città del Vaticano, non può essere affrontata utilizzando impianti tecnologicamente avanzati, sistemi di comunicazione, sistemi informatici e risorse umane in maniera separata e scorrelata tra di loro, ma deve essere affrontata integrando tutte le componenti suddette in un unico sistema in grado di assicurare la massima funzionalità ed efficienza.

1. INTRODUZIONE

Lo Stato Città del Vaticano si estende su di una superficie di circa 44 ettari, per quando riguarda l'enclave territoriale centrale. Esso include anche territori distaccati quali la Residenza Papale estiva di Castel Gandolfo, le Basiliche di S.Giovanni e S.Maria Maggiore, Santa Maria di Galeria (sede dei trasmettitori della Radio Vaticana), ecc.



Fig.1 La Basilica di San Pietro e il colonnato del Bernini

Anche se l'estensione territoriale è ridotta rispetto alle normali estensioni territoriali degli altri Stati, lo Stato Città del Vaticano presenta le stesse esigenze di sicurezza di un qualunque Stato che sono peraltro maggiormente amplificate in quanto si manifestano in una territorio comunque limitato.

Per tale motivo è stato necessario progettare e realizzare un sistema di sicurezza estremamente avanzato che, integrando accuratamente tecnologie elettroniche, di telecomunicazioni e informatiche, ha permesso di soddisfare tutte le esigenze di sicurezza dello Stato Città del Vaticano, utilizzando un approccio multidisciplinare tipico dell'Ingegneria della Sicurezza, con particolare riferimento, in questo caso, alla Sicurezza dell'Informazione e della Comunicazione.

2. I SISTEMI INTEGRATI DI SICUREZZA

La forte domanda di sicurezza oggi presente nella nostra società ed in particolare in contesti specifici e unici come quelli dello Stato Città del Vaticano, comporta lo sviluppo di sistemi di protezione sempre più complessi e capaci di fornire una reale difesa alle persone ed ai beni, così da rispondere in maniera adeguata a tale domanda.

La tecnologia, oggi, fornisce un'infinità di soluzioni per rispondere a questa domanda di sicurezza, partendo dai sistemi di sicurezza ambientale a quelli di video sorveglianza per finire con i sistemi di comunicazione capaci di gestire, a distanza, gli impianti più svariati.

Ma tale varietà di scelta può diventare un limite dei sistemi di sicurezza, in particolare per gli impianti che hanno il compito principale di controllare grandi strutture o siti di particolare importanza.

In realtà complesse ed articolate, come quella dello Stato Città del Vaticano, non è possibile pensare a un sistema di sicurezza che non sia caratterizzato da capacità di integrazione e di interazione tra le differenti tecnologie che lo costituiscono. Infatti, il concepire la sicurezza in maniera specifica e settoriale in funzione delle esigenze specifiche di un suo sottosistema, senza avere una visione generale del problema, può compromettere in maniera significativa la validità del sistema, portandolo a rispondere in maniera non adeguata alle situazioni di pericolo e di emergenza.

Non è assolutamente inusuale, soprattutto nel settore della sicurezza, che ogni specialista veda il problema esclusivamente in base alle sue conoscenze tecniche e alla sua esperienza personale.

Al contrario oggi è fondamentale progettare e realizzare sistemi che siano capaci di interagire tra di loro in modo efficiente e coordinato, mantenendo nel contempo un elevato grado di semplicità gestionale, per fare in modo che un operatore della sicurezza possa accedere in tempo reale alle varie informazioni e possa riuscire a gestire l'emergenza in maniera efficiente ed efficace.

Molto importante risulta essere la gestione dell'informazione all'interno dei sistemi integrati di sicurezza. Infatti, data la loro natura intrinseca, tali sistemi generano al loro interno un elevato flusso informativo che deve in qualche maniera essere correttamente indirizzato, coordinato ed eventualmente memorizzato in maniera provvisoria o permanente, pena il sovraccarico o il sovradimensionamento dei canali di trasmissione o dei dispositivi di elaborazione e registrazione.

Nella definizione della politica di gestione dell'informazione grande attenzione deve essere rivolta all'aspetto psicologico degli operatori che devono utilizzare il sistema per evitare sovraccarichi di informazione che indurrebbero inevitabili situazioni di stress o di riduzione del livello di attenzione.

Per tale motivo è necessario che il flusso informativo nei confronti degli operatori sia ridotto allo stretto indispensabile, aumentando tale flusso solo nelle situazioni di emergenza, quando gli stessi operatori vengono chiamati a gestire direttamente la situazione per evitare il verificarsi di eventi pericolosi per le persone o per i beni.

Da ciò si ricava l'importanza di figure professionali qualificate capaci di analizzare e studiare in maniera efficace il problema sicurezza e di progettare una risposta estremamente funzionale ed efficiente attraverso sistemi fortemente integrati tra di loro.

Questa visione del problema sicurezza ha posto le linee guida sul quale è stato sviluppato il progetto di sicurezza integrata dello Stato Città del Vaticano.

Tale progetto ha implicato, tra l'altro, l'individuazione e la strutturazione del centro di controllo, come posto di gestione e integrazione dei vari sistemi e lo studio e la progettazione della rete di comunicazione, avendo come obiettivo primario la sua capacità di mantenere un alto livello di ridondanza e di espansione in funzione di future esigenze.

Per tale motivo si è deciso di creare una rete dedicata alla sicurezza in fibra ottica, in quanto caratterizzata da una larghezza di banda estremamente elevata, da una elevata qualità trasmissiva, da maggiori capacità di trasporto dei dati, da una relativa facilità di espansione nel passaggio a velocità dati più elevate e da una elevata immunità ai disturbi elettromagnetici e radio.

Successivamente si è passati alla scelta delle tecnologie necessarie a sviluppare il sistema in base alle esigenze di controllo del territorio. Infatti le specifiche esigenze di sicurezza dello Stato Città del Vaticano hanno richiesto la presenza di una rete di allarme, di una rete di video sorveglianza, e di una rete di telecomunicazioni. Le tecnologie scelte dovevano essere affidabili nel tempo e capaci di integrarsi tra di loro, in maniera tale da permettere al centro di controllo di avere in qualunque momento una visione reale della situazione del territorio, soprattutto nelle situazione di pericolo e di emergenza.

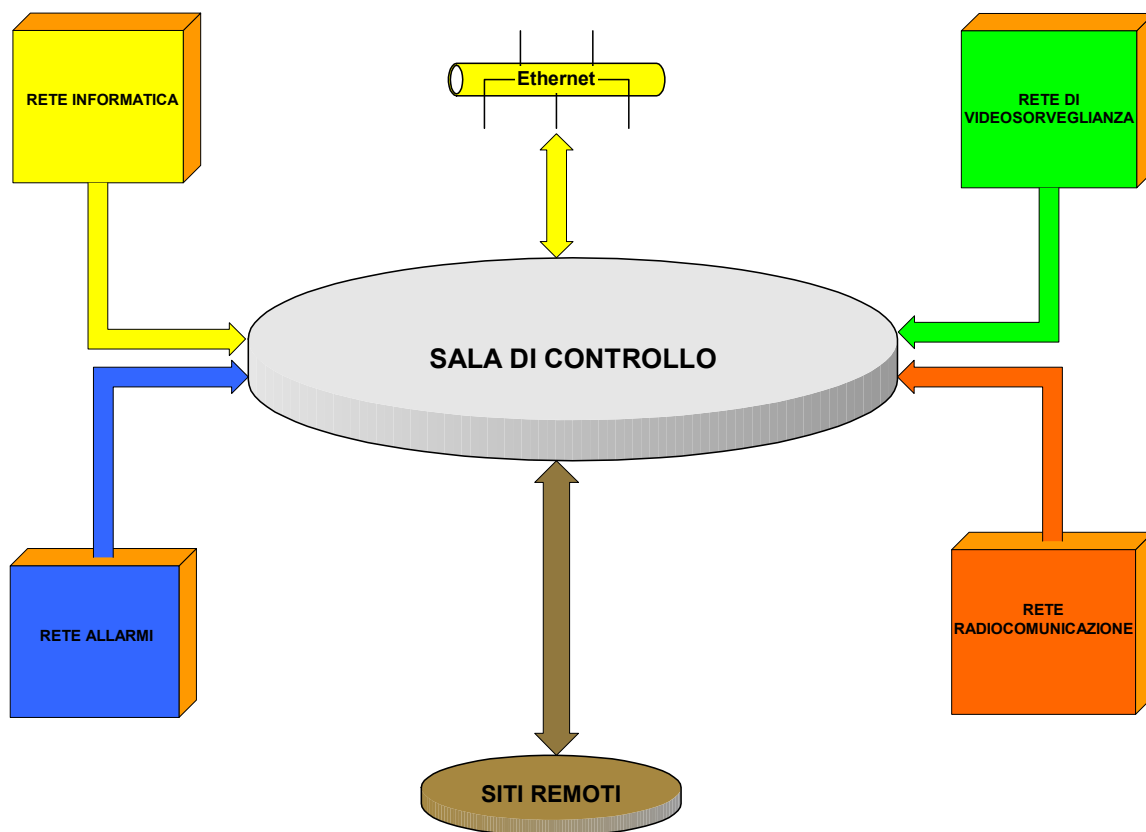


Fig.2 Schematizzazione del sistema integrato di sicurezza progettato e realizzato

Di seguito sarà riportata una descrizione sintetica dei sistemi utilizzati nel progetto sicurezza integrata, senza potere purtroppo illustrare particolari e dettagli che comprometterebbero la sicurezza del sistema stesso.

3. IL SISTEMA DI VIDEOSORVEGLIANZA TV A CIRCUITO CHIUSO (TVCC)

Un impianto di TVCC, attualmente, non può essere considerato esclusivamente come un sistema passivo di visione e registrazione delle immagini ma è sicuramente più appropriato considerarlo come un sistema attivo in grado reagire alle situazioni d'allarme, in modo autonomo con "Activity" o "Motion Detector", oppure come un completamento di un sistema antintrusione, previo adeguato interfacciamento.

Un sistema TVCC di nuova generazione deve dare all'operatore la possibilità di verificare in tempo reale gli eventi, permettendone l'immediata gestione attraverso il collegamento con le reti di comunicazione radio e telefoniche che permettono di interagire in tempo reale con gli operatori dei vari servizi interessati alla sicurezza.

Nello stesso tempo il sistema TVCC deve dare la possibilità, in un secondo momento, di verificare, comprendere, analizzare e studiare come l'evento si è venuto a sviluppare nel tempo. E' evidente come tali esigenze necessitino di una qualità d'immagine tale da permettere all'operatore la corretta comprensione degli avvenimenti visualizzati.

Per questo motivo è stato necessario progettare soluzioni e sistemi caratterizzati da un elevato contenuto tecnologico, orientati verso elevate qualità d'immagine, e da una elevata flessibilità nella gestione dei segnali video, della registrazione e della installazione delle apparecchiature. Da qui la scelta di telecamere professionali ad alta qualità di immagine sia di tipo fisso che di tipo *Speed Doome* (telecamere brandeggiabili controllabili a distanza e racchiuse all'interno di un involucro semisferico), capaci di rispondere in maniera adeguata alle esigenze di controllo del territorio dello Stato Città del Vaticano.

Il sistema di gestione dell'impianto di video sorveglianza è caratterizzato da un'elevata capacità di integrarsi con la rete informatica, in maniera tale da garantire un adeguato controllo delle componenti remote dell'impianto.

L'utilizzo della fibra ottica per la connessione delle telecamere ha permesso di impiegare tecnologie di natura differente in base alle esigenze operative ed alla struttura del territorio, creando, dove è stato necessario, sistemi remoti di controllo e registrazione dell'immagini, mantenendo nel contempo un reale controllo da parte della sala operativa.

Estremamente importante si è rivelato essere lo studio, la progettazione e la realizzazione del sistema di gestione dell'impianto di video sorveglianza mediante tastiere e joystick i quali, pur permettendo un controllo manuale di tipo tradizionale, al fine di evitare difficoltà di gestione dell'impianto da parte degli operatori, sono stati affiancati da software sviluppati appositamente dagli autori per soddisfare le esigenze operative e per garantire agli operatori della Sala di Controllo una gestione estremamente intuitiva e semplificata del sistema.

Da quanto detto sopra è evidente che una grande attenzione è stata ovviamente rivolta agli operatori nella progettazione del sistema. Infatti nessun progetto di un sistema di sicurezza può prescindere dall'analisi e dall'acquisizione del profilo operativo e psicologico del personale che deve utilizzarlo, tenendo conto delle capacità, da parte degli operatori stessi, di interagire con l'interfaccia utente. Se non si tenesse conto di tale aspetto si rischierebbe di creare un sistema di altissimo livello tecnologico ma ingestibile sul piano pratico.

Nella progettazione e realizzazione del sistema una particolare attenzione è stata riservata alla sezione riguardante la video registrazione.

Data la definitiva affermazione della registrazione digitale anche per il mondo della TVCC, che permette di mantenere un elevato livello di qualità delle immagini, si è deciso di utilizzare tale tecnologia. La registrazione digitale, grazie alla sua capacità di accesso causale alla memoria di massa, facilita l'accesso all'immagini salvate, riducendo in questo modo, rispetto ai vecchi sistemi di registrazione su videocassetta, i tempi di analisi degli eventi registrati. Un'ulteriore punto di forza della tecnologia di registrazione digitale è rappresentato dalla sua affidabilità nel tempo.

L'impianto di video sorveglianza è stato corredato da un sistema di "*Motion Detector*" di tipo evoluto, in grado di controllare sia ambienti chiusi che aree esterne, evitando di generare falsi allarmi. Tale sistema è stato integrato con l'impianto di video sorveglianza, attraverso la creazione di apposite interfacce software, che permettono di visualizzare gli allarmi acquisiti sui monitor utilizzando indicatori che evidenziano in modo chiaro l'oggetto o la persona che ha generato l'allarme.

Il sistema di video registrazione così ideato e realizzato consente agli operatori della sala di controllo di conoscere con precisione qualunque evento critico ai fini della sicurezza, permettendo di mettere in atto una serie tecniche di controllo del territorio diversamente irrealizzabili con sistemi differenti.

4. LA RETE FISSA DI ALLARMI

Anche la rete che gestisce gli allarmi è stata sviluppata seguendo una filosofia di integrazione con le restanti componenti dell'impianto, con la capacità, quindi, di connettersi con i sistemi di video sorveglianza e di radiocomunicazione esistenti.

Fondamentale si è rivelata essere la scelta della centrale di gestione, che possiede tutte le caratteristiche di interoperabilità con la rete informatica e nello stesso tempo permette di visualizzare in modo adeguato la situazione reale dell'impianto, la sua efficienza operativa e le intrusioni non autorizzate negli ambienti protetti.

La rete permette inoltre all'operatore di interagire con l'impianto, in base alle sue autorizzazioni di accesso, e di supportare in maniera adeguata il personale che deve intervenire nella zona dove è stato generato l'allarme, mentre la centrale operativa provvede all'attivazione, in maniera automatica, dei sistemi di registrazione digitale per l'acquisizione in tempo reale dell'immagini relative all'evento che ha generato l'allarme.

5. LA RETE DI RADIOCOMUNICAZIONE MOBILE

Un sistema integrato di sicurezza non può prescindere dalla presenza di un efficiente sistema di comunicazione in quanto qualsiasi emergenza rilevata dai sistemi di allarme e da quelli di video sorveglianza deve essere gestita in maniera immediata dall'operatore di sala operativa e dal personale che opera sul territorio.

A questo riguardo esiste attualmente sul mercato una vasta scelta di sistemi che il progettista della sicurezza deve accuratamente selezionare tenendo sempre presente che la rete di comunicazione deve essere caratterizzata da un'elevata affidabilità e da una funzionalità indipendente da fattori esterni non gestibili.

Un sistema di comunicazione deve permettere un'agevole interazione di tutti gli operatori di sicurezza del sito da proteggere e un'interfacciamento con tutti i sistemi di comunicazione radio esistenti. A questo proposito le postazioni operatore presenti presso la sala di controllo sono state progettate per interfacciarsi con sistemi radio analogici tradizionali, di tipo multiaccesso analogici, con sistemi radio digitali e con i sistemi telefonici.

I sistemi di radiocomunicazione sono dedicati esclusivamente alla sicurezza ed alla gestione dei servizi ad essa riservati. Le reti di comunicazione pubblica possono interagire con essi ma non sono ovviamente in grado di sostituirli. Infatti, l'esperienza di questi anni ha dimostrato in maniera inequivocabile che la gestione delle emergenze o dei grandi eventi (Giubileo 2000) non può prescindere dalla disponibilità e dall'affidabilità di un sistema di radiocomunicazione dedicato tra il centro di controllo e gli operatori che lavorano nel territorio.

Le nuove reti di comunicazione radio permettono attualmente una reale interoperabilità tra i servizi ed una gestione efficiente delle frequenze radio. In questo modo tutti i servizi possono operare in maniera autonoma, senza che si verifichino mutue interferenze tra le comunicazioni, pur permettendo, durante l'emergenza, l'interazione tra gli operatori che operano su diversi settori nel campo della sicurezza.

A queste considerazioni bisogna anche aggiungere le possibilità che offrono queste reti di comunicazione radio, in particolar modo quelle digitali, di interagire con la rete informatica e la loro possibilità di trasmettere e ricevere dati, che rappresentano funzioni estremamente importanti per un reale controllo del territorio ai fini della sicurezza.

Dopo un'accurata analisi delle esigenze del sistema, con particolare attenzione al rapporto costi/benefici, la scelta è caduta sui sistemi di radiocomunicazione ad accesso multiplo che rappresentano le applicazioni più moderne di radiocomunicazione per scopi professionali e per scopi di sicurezza (PMR/PAMR1), privati e pubblici. Contrariamente ai vecchi sistemi analogici convenzionali a canale fisso (ad ogni servizio e ad ogni utente viene attribuito in permanenza un determinato canale radio), con i sistemi di radiocomunicazione ad accesso multiplo le frequenze vengono assegnate in modo flessibile ai singoli utenti e servizi. In questo modo è possibile sfruttare il guadagno del collegamento ad accesso multiplo e aumentare l'efficienza dello spettro. Inoltre, con la tecnica digitale, si aumenta considerevolmente la qualità e la sicurezza dei sistemi di radiocomunicazione.

È grazie a questa efficienza dello spettro e alla flessibilità del sistema ad accesso multiplo che è stato possibile dotare ogni servizio (pubblica utilità, sicurezza ambientale, sicurezza del territorio, ecc.) di un efficiente sistema di comunicazione radio, capace di rispondere in maniera adeguata ed efficiente alle esigenze di operatività del personale presente sul territorio.

La scelta dei sistemi di radiocomunicazione ad accesso multiplo rispetto a quelli di telefonia mobile, quali GSM o UMTS, nasce soprattutto dalla velocità con cui questi stabiliscono i collegamenti, quali le chiamate di gruppo, le chiamate prioritarie, la codifica punto a punto e la chiamata diretta da una stazione mobile ad un'altra stazione mobile senza dover passare per la stazione di base (il cosiddetto direct mode).

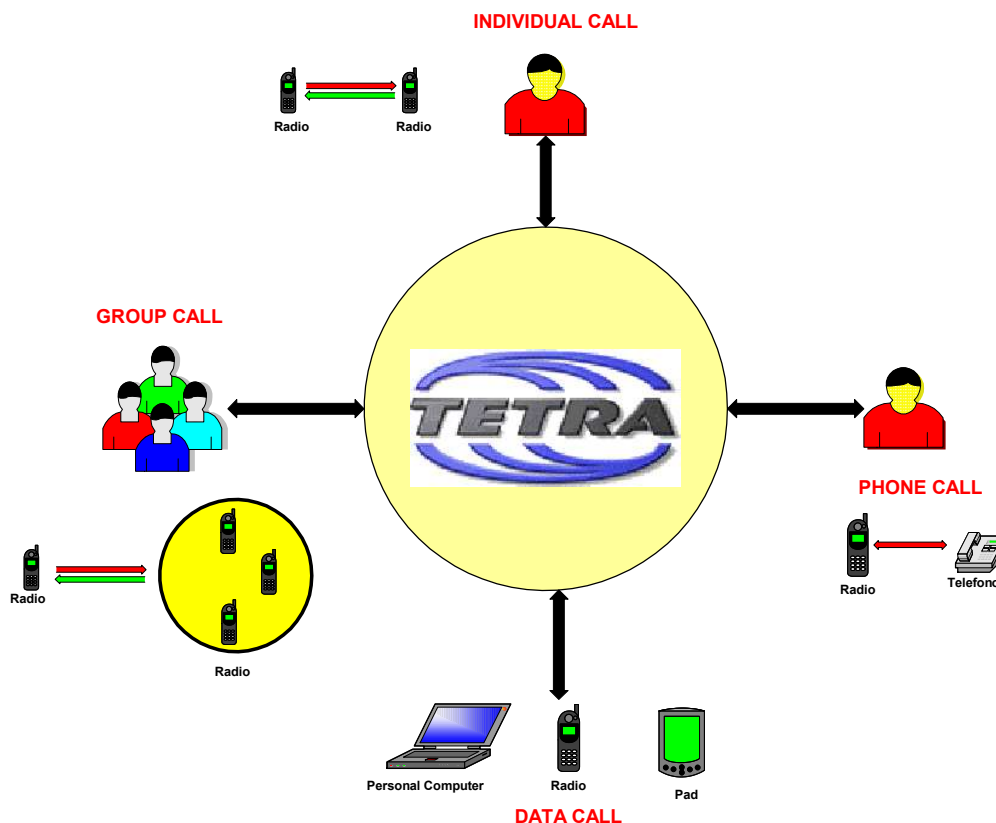


Fig.3 Schematizzazione del sistema di radiocomunicazione TETRA

I sistemi ad accesso multiplo permettono di avere a disposizione i seguenti servizi:

- *Individual Call (chiamata individuale):* questo servizio corrisponde al collegamento mediante un sistema pubblico di radiocomunicazione mobile (GSM, UMTS). L'utente chiama un altro utente e viene collegato con quest'ultimo.
- *Group Call (chiamata di gruppo):* un determinato utente chiama un gruppo prestabilito. Ogni membro del gruppo può ascoltare e parlare con tutti. La chiamata di gruppo può essere organizzata in modo tale che ogni singolo partecipante debba confermare o meno la propria comunicazione. Il gruppo può essere modificato in modo flessibile, potendo aggiungere o ridurre partecipanti durante lo svolgimento.
- *Direct Mode:* con il direct mode due o più stazioni mobili comunicano direttamente tra di esse, senza l'intervento della stazione di base (walky-talky).
- *Broadcast Call:* si tratta di una comunicazione unidirezionale punto-multipunto in una determinata zona. La zona e gli utenti sono predefiniti. I singoli partecipanti non devono confermare la chiamata e quindi il chiamante non può controllare se effettivamente il chiamato o i chiamanti hanno ricevuto la comunicazione.
- *Emergency Call (chiamata d'emergenza):* che permette di chiamare con la massima priorità un dispatcher o un gruppo d'utenti predefinito utilizzando un tasto di emergenza.
- *Include Call:* che permette di chiamare e di inserire in una conversazione uno o più utenti supplementari.

- *Status Transmission*: che permette la trasmissione dal dispatcher verso le stazioni mobili e viceversa oppure tra le stazioni mobili, di messaggi molto brevi e predefiniti.

I sistemi ad accesso multiplo di tipo digitale consentono inoltre i seguenti servizi:

- *Short Data Service*: che permette di inviare messaggi predefiniti a singoli utenti o ad un gruppo.
- *Servizi di trasmissione dati a commutazione di circuito*: caratterizzati dalle seguenti caratteristiche:
 - Trasmissione dati non protetta: $n \times 7,2 \text{ kBit/s}$ ($n = 1, 2, 3 \text{ o } 4$)
 - Trasmissione dati protetta: $n \times 4,8 \text{ kBit/s}$ ($n = 1, 2, 3 \text{ o } 4$)
 - Trasmissione dati altamente protetta: $n \times 2,4 \text{ kBit/s}$ ($n = 1, 2, 3 \text{ o } 4$) (n = numero degli intervalli di tempo utilizzati su una frequenza portante).

Rispetto ai sistemi pubblici di radiocomunicazione mobile come il GSM o l'UMTS, i sistemi di radiocomunicazione ad accesso multiplo PMR vengono utilizzati per servire un numero ridotto di utenti, con tempi di conversazione brevi. Ciò comporta un flusso di traffico ridotto e in generale la possibilità di costruire celle di estensione significativa. La potenza emessa per frequenza portante della stazione di base è dell'ordine di grandezza di 25 W ERP.

Una considerazione a parte deve essere riservata ai sistemi ad accesso multiplo digitali comunemente facenti parte del protocollo TETRA. Infatti tali sistemi, ai normali vantaggi dei sistemi ad accesso multiplo di tipo analogico le reti digitali, aggiungono una efficiente gestione dello spettro della frequenza radio in quanto utilizzano un accesso ai canali mediante la tecnica **TDMA** (Time Division Multiple Access).

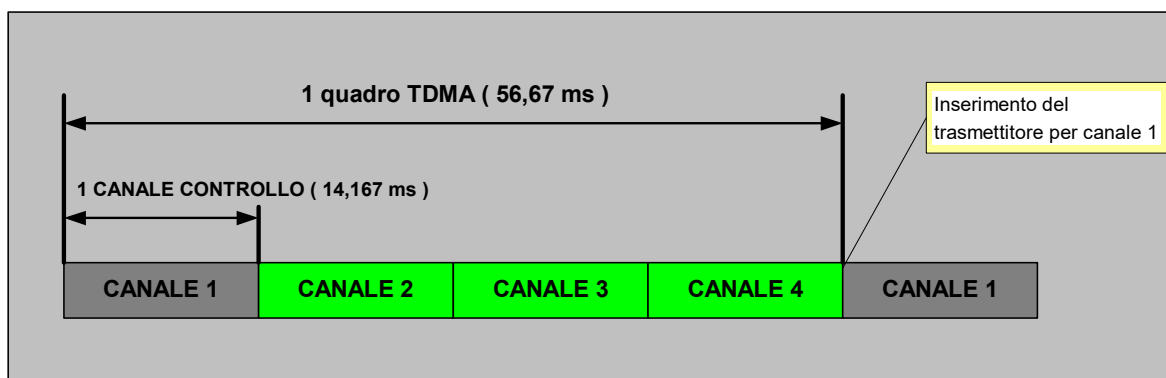


Fig.4 Suddivisione dei canali nel sistema TETRA

I sistemi TETRA forniscono quattro canali di comunicazione indipendenti all'interno di un canale di radiocomunicazione di 25 kHz. Uno solo di essi (slot) viene occupato per un quarto del tempo, per la durata di un intervallo di tempo base del sistema (quadro TDMA). Per il resto del tempo, il canale di radiocomunicazione può essere utilizzato da altri utenti. Il trasmettitore viene perciò inserito e disinserito circa 18 volte al secondo durante una comunicazione. Se tuttavia occorre una grande capacità di trasmissione, un utente può occupare anche più di un intervallo di tempo (fino a quattro). Il singolo utente può trasmettere contemporaneamente sia la voce sia i dati.

Con le reti digitali TETRA, in una cella vengono solitamente installate 3 - 4 frequenze, che permettono, rispettivamente, l'utilizzo di 12- 16 canali logici per stazione Base.

I diversi sistemi PMR si differenziano molto gli uni dagli altri per quanto concerne il numero di utenti, la zona di copertura, il flusso di traffico supportabile e i servizi offerti. Alcuni sistemi sono limitati dal rumore (i limiti del sistema sono determinati dal rumore del ricevitore) oppure limitati dalle interferenze (presenza di forti interferenze nello stesso canale causate da celle vicine). L'efficienza dello spettro dipende fortemente da questi parametri.

Il sistema di radiocomunicazione utilizzato ha permesso di creare una reale sinergia tra gli operatori sul campo, sviluppando una reale interazione con il territorio in modo da gestire efficientemente il personale operante.

6. CONCLUSIONI

La gestione della sicurezza in contesti specifici, complessi ed articolati, quali quelli dello Stato Città del Vaticano, richiede inevitabilmente un'analisi meticolosa dei rischi e dei pericoli da fronteggiare, nonché un attento studio e una corretta progettazione, al fine di integrare fortemente tutte le componenti del sistema e di garantire la massima interazione reciproca, con particolare attenzione alla gestione dei flussi di informazione.

In tal modo è stato possibile realizzare un sistema integrato estremamente efficace ed efficiente per la gestione della sicurezza dello Stato Città del Vaticano.

Bibliografia

- [1] F.Garzia: "Impianti e Sistemi di Sicurezza", Carocci Editore, Roma, 2001.
- [2] F.Garzia: "The integrated safety/security system of the Accademia Nazionale dei Lincei at Corsini Palace in Rome", Proceedings of International Conference on Integrating Historic Preservation with Security, Fire Protection, Life Safety and Building Management Systems, Ministero dell'Interno - Dipartimento dei Vigili del Fuoco, del Soccorso Pubblico e della Difesa Civile & NFPA (National Fire Protection Association), pp.77-99, Roma 2003.
- [3] F.Garzia, "I sistemi integrati di sicurezza per la protezione dei beni culturali, Ambiente&Sicurezza, IL SOLE 24 ORE, pp.18-23, 8 luglio 2003.
- [4] 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 (Boston), pp.287-293, 2002.
- [5] 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 (Boston), pp.853-861, 2002.
- [6] T.Bucciarelli, F.Garzia, G.M.Poscetti: "Manuale di Sicurezza delle Comunicazioni", IL SOLE 24 ORE (in preparazione).