THE INTEGRATED SECURITY SYSTEM OF THE SENATE OF THE ITALIAN REPUBLIC

G. CONTARDI[1], F. GARZIA[2] & R. CUSANI[2]
[1]Senate of the Italian Republic, Rome, Italy.
[2]Department of Information, Electronics and Telecommunication Engineering,
SAPIENZA - University of Rome, Italy.

ABSTRACT

The security of a complex site is strongly dependent on the use of integrated technological systems. Any weakness of the integrated system involves a weakness of the security of the site itself. For this reason it is necessary to design and realize highly integrated, efficient and reliable security systems. The authors illustrate the work made to design and realize the integrated security system of the Senate of the Italian Republic.

Keywords: communication system, control system, integrated security system.

1 INTRODUCTION

The Senate of the Republic represents one branch of the Italian Parliament (the other branch is the Chamber of Deputies). The site is composed of 13 historical buildings located in the center of Rome in Italy.

In such a complex contest, it was necessary to design and realize a strongly integrated security system that could ensure a high interaction between the different subsystems that compose it. The different subsystems are able to interact reciprocally in an efficient and coordinated way, showing a high degree of usability to let the security personnel receive, in real time, the different information required to manage not only security but also emergency situations.

The system is properly divided into six subsystems:

1. telecommunication;
2. video surveillance TV;
3. access control;
4. intrusion detection;
5. fire detection/extinguishing;
6. supervision and control.

Information management represents a very important factor for the functionality and efficiency of the integrated security systems. In fact, due to their intrinsic nature, these systems generate a considerable information flow inside them that must be correctly addressed, coordinated, and potentially stored on temporary or permanent memory supports to avoid overcharging or over dimensioning of communication channels and storing devices [1–10].

The system guarantees a high degree of integration between the different subsystems ensuring a correct and immediate control of all data and significant events for security management and control.

The system functionalities are really superior with respect to the functionalities of single subsystems. In Fig. 1 a picture of Madama palace is shown.

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://journals.witpress.com
DOI: 10.2495/SAFE-V1-N3-219-247

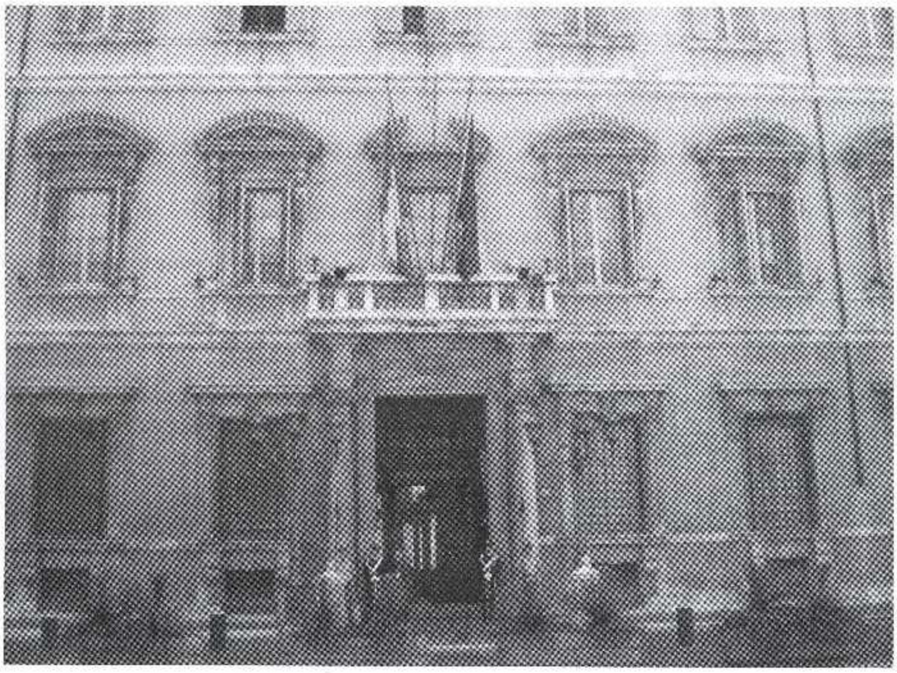


Figure 1: Picture of Madama palace, the main building where the assembly room of senators is located.

The system was designed and realized to reduce, as much as possible, the esthetical impact on the architecture of the senate buildings, providing its advanced functionalities without disturbing the artistic style of the buildings from any point of view.

The system operates thanks to an advanced telecommunication subsystem, characterized by a high reliability that is capable of working in the presence of any critical condition. The telecommunication system is based on both a fixed system and a mobile system.

The designed system is characterized by a high degree of modularity and expandability so that it is possible to add and integrate any other subsystem, device, or installation in any point of the senate buildings, guaranteeing the full control of any of the components.

Every component of the system is supplied by proper autonomous and backed-up electrical sources to allow for operation even in the absence of the main electrical supply.

The system is managed by a proper main control room and some secondary workstations that allow the total control of the system in case of malfunctioning or damage of the main control room. Therefore the full control of the whole system is always ensured. The system is also equipped with disaster recovery capabilities.

Special attention was reserved, in the design of the system, to the psychological and ergonomic aspects of the operators of the control room to avoid information overcharges that would induce stress and reduce attention levels, decreasing their performances.

For this reason, the information flow is processed to reduce its level in ordinary conditions and to properly increase it in emergency situations when the operators of the control room and other personnel must face and manage events that could become dangerous for people or goods. In Fig. 2 the scheme of the integrated security system is shown.

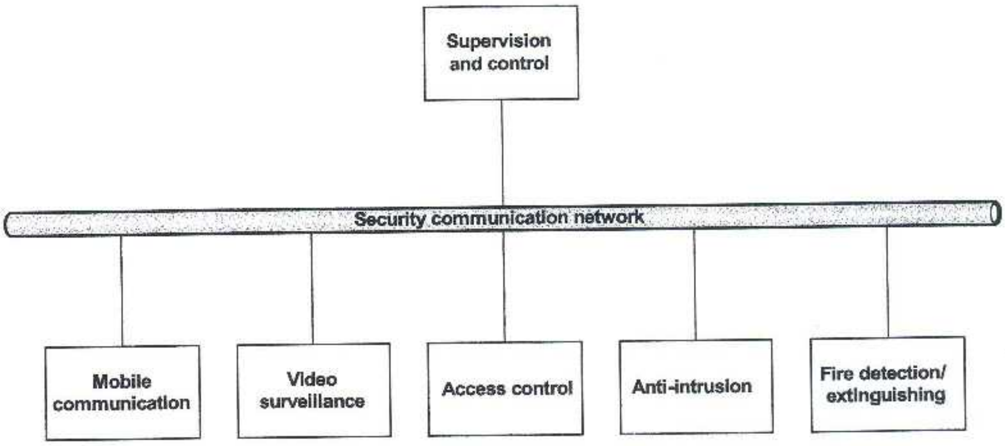


Figure 2: Scheme of the integrated security system.

The operators and personnel are properly and continuously trained to analyze and study the dangerous events, and to face them properly through functional and efficient procedures allowed by the high degree of integration of the system.

The realization of the powerful and versatile integrated security system described in this paper guarantees a high level of security services of the Italian Senate of the Republic.

2 THE TELECOMMUNICATION SUBSYSTEM

The telecommunication subsystem represents the backbone of the integrated security system (video surveillance CCTV, access control, intrusion detection, fire detection, etc.), ensuring advanced functionalities and performances [4–10].

In the following, only a synthesis of the main features is illustrated.

The telecommunication subsystem is composed by two strongly integrated subsystems: fixed infrastructure and mobile infrastructure.

The whole telecommunication subsystem is controlled by the main control room that checks the functionalities of any component of the integrated system, including the telecommunication subsystem. Any malfunctioning is immediately signaled to the operator that can activate the related procedures to guarantee the maximum functionality of the system.

The design of the telecommunication subsystem started with the analysis of security data flows that must be carried by the system.

The data flows of the integrated system are generated by video cameras, alarms, access control, voice communications, and control data.

Once the total flow that must be carried by the telecommunication system was known, it was possible to design it, dividing it into a fixed system and a mobile system. Each system has been designed according to the peculiar data flows that must be carried, following the criteria illustrated in the following.

The telecommunication subsystem is totally separated from the other telecommunication systems of the Senate, to avoid interferences that could weaken the system itself.

Further, it has been designed to guarantee a high reliability and availability using a high redundancy. In particular, it is equipped with a total autonomous electrical supply system.

The telecommunication subsystem is continuously and automatically checked so that any malfunction is immediately signaled and repaired. The control software examines any data flow to check any irregularity or overcharge of the system. Further, the system has been designed to guarantee a high quality of service (QoS) and class of service (CoS).

The telecommunication network has been designed as a function of the different environments to be served and of the different protocols to be carried to guarantee a high level of security and services.

The network has been designed and realized to:

1. reduce as much as possible the single points of failure
2. simplify the net management
3. simplify the different devices recognition
4. increase the reliability with the use of redundant devices
5. guarantee future expandability
6. be open toward to other kind of devices
7. guarantee the interoperability of different devices

To guarantee a high velocity of data transmission, redundant optical fibres have been used. All the connections are capable of reaching velocity of 10 Gbit/s.

The net architecture is based on dense grid connections, where two redundant centers are present and properly located into protected rooms. In this way, a damage of a center is immediately recovered by the other center. Each building is equipped with a proper redundant switch connected to the main backbone by means of four links: two toward the centers and two toward the switches of adjacent buildings. The two centers of the net are connected by means of a double optical fibre. Each connection of the net follows different physical paths so that the interruption of one link (voluntary or involuntary) is immediately recovered by the other links. This kind of architecture guarantees a high level of reliability. In Fig. 3 the network architecture schematization is shown.

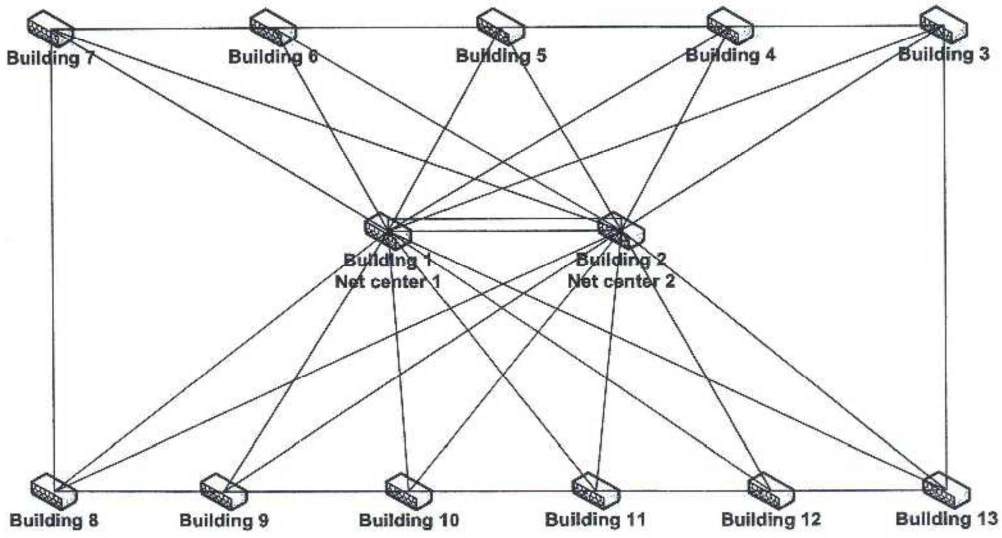


Figure 3: Network architecture schematization.

The fixed net infrastructure is designed and realized considering a three level hierarchic model:

1. access level
2. distribution level
3. core level

The access level is represented by the most external nodes of the net, also called leaves. The main functions of the nodes are:

1. introduction of the traffic inside the network
2. security management
3. band management (compression, traffic-shaping, etc.)
4. congestion management (priority management mechanisms)
5. proxy services (DHCP relay, etc.)

The distribution level represents a series of policing functionalities such as service access, management, and distribution of routing information and definition of the metric for the best paths choice. The main goals of this level are:

1. aggregation of the traffic coming from the nodes
2. hiding of the network details to the core by means of IP addresses aggregation
3. check of the dimensions of the routing tables by means of minimized core connections
4. congestion management by means of priority control mechanism and congestion avoidance
5. security management by means of access control list
6. band management by means of compression and traffic-shaping mechanism.

The core level makes the following functions:

1. high velocity switching of IP traffic
2. optimized management of net resources, bandwidth, CPU, etc.
3. traffic distribution through paths of the same weight
4. use of advanced techniques of QoS for policing, congestion avoidance, and prioritization.

All the servers related to the management of the network are grouped in a proper server farm. It is composed by two redundant servers connected by means of a double link. These servers are connected to the two centers of the network by means of a double link so that full redundancy is always ensured.

Even if all the connections are realized in a secure way and all the devices are properly placed in secure rooms, due to the extension of the net, to increase the security level of the system, all the links are properly ciphered by means of proper devices that allow the creation of Virtual Private LANs.

A series of Virtual LANs (VLAN) are defined for every switch of the building and for the two centers of the network. These VLANs are used for the connection of the different devices of the system and for the connection of the switches of the building with the other components of the net infrastructure.

All the installations connected to the system exchange information reciprocally and with the consoles of the supervision system. For this reason it has become necessary to implement proper security procedures to protect the server farm from possible attacks such as:

1. unauthorized access
2. denial of service
3. network reconnaissance
4. virus and worms
5. IP spoofing
6. layer 2 attacks

The security procedures are designed to avoid reducing the network performances.

To increase the security level of the network an access control through authentication of users and devices is present.

The network infrastructure is equipped with a management and monitoring system based on SNMP protocol that ensures the following functionalities:

1. periodical verification of the correct working status of devices
2. statistics of the devices such as network loads, errors, CPU loads, etc
3. reception of alarms and events
4. network discovery and automatic individuation of the features of found devices
5. remote configuration of devices (ports, VLAN, spanning tree, security, traffic management, routing, filtering, etc.)
6. firmware automated and centralized updating
7. automatic storing of the configuration of every network device.

The mobile communication subsystem is designed to allow a prompt diffusion of security information and a rapid response of personnel involved in any emergency situation. It is strongly integrated with the other components of the telecommunication subsystem.

The mobile subsystem is based on TETRA standard, a technology expressly developed in EU for security and safety communications.

Due to the variety of problems involved, a collective access radio system has been designed and realized. It is capable of satisfying all the security communication needs of the Senate. The mobile system is composed by a series of base stations (such as ordinary GSM or UMTS mobile communication system) connected to a central unit that manages and controls the service of radio units of the users.

The mobile communication system is composed by a control center, called master site (MS) and from a variable number of base stations (BSs) positioned on the territory.

Every BS can support four radio channels per transmitted carrier and can operate simultaneously on different carriers.

The MS is located in a protected zone inside the main control room. The main operator console is connected directly to the MS where it is possible to operate and program the database and the user's profiles directly on the mobile system.

The MS is connected directly to the PBX to interface with the internal and external telephone lines.

The radio units are characterized by reduced dimensions and weight and by controllable emitted powers, always ensuring better communication quality between the radio units and the nearest BS. It also includes a GPS receiver for positioning services and a

Bluetooth interface to connect to an external terminal, where it is possible to receive and control alarms and signals (data, picture, or video) coming from the supervision system.

The number and the positions of the BSs have been calculated by means of a proper and complex simulation and study of electromagnetic propagation (using Genetic Algorithms optimization). It ensures a full coverage of the buildings and of the related interiors, respecting the severe environmental electromagnetic emissions limitations imposed by the Italian law.

The dimensioned mobile system allows to serve, at the same time, the planned number of:

1. users
2. definable groups
3. contemporary calls
4. contemporary telephone calls

The frequencies used are between the interval of 380–400 MHz to ensure a greater propagation inside the buildings and the narrow streets around them, guaranteeing an optimal coverage of the area.

In a collective access radio system, the frequencies are dynamically assigned to the users, according to their needs, allowing an efficient and dynamic management of the system.

The mobile system allows the interconnection with the internal and the external telephone net, guaranteeing a high level of connectivity. In Fig. 4 the logical fluxes of network security are shown.

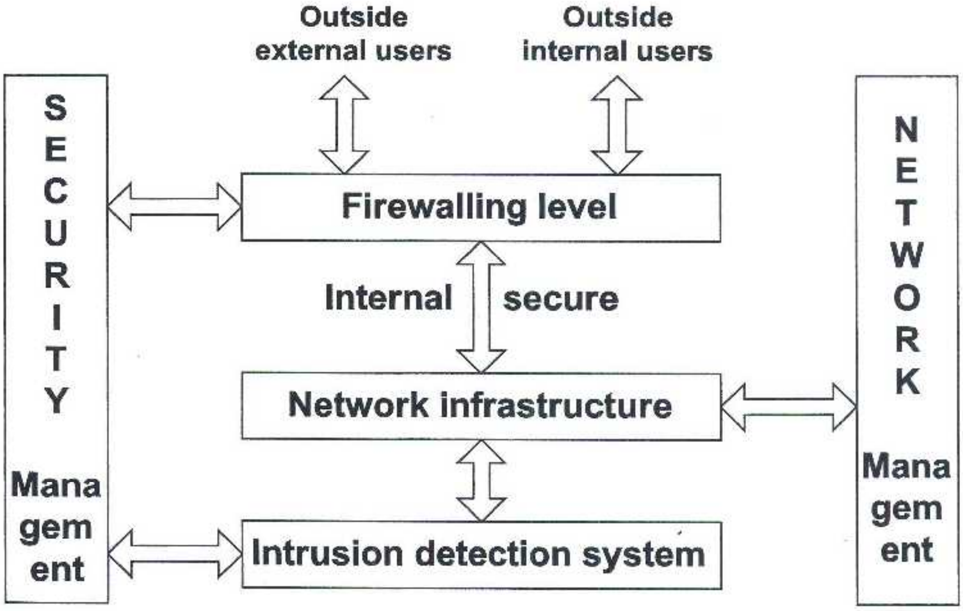


Figure 4: Logical fluxes of network security.

The used digital technology is characterized by the following advantages:

1. better quality of vocal messages
2. higher transmission and.reception velocity
3. lower dependence from signal reception level
4. higher security of conversation thanks to the used cryptographic algorithm
5. capabilities of using the mobile units not only as phones but also as data terminals to transmit and receive any kind of information
6. localization of mobile terminals by means of integrated GPS units.

Every used radio link can be divided in four different channels that are used singularly or together as a function of the necessary transmission band.

The mobile subsystem checks continuously the coding/decoding quality of the voice, allowing an optimal communication service even in the presence of noises.

The system allows a multilevel user authentication (user–mobile system, mobile system–fixed net, network–network, user–user), using high security cryptographic algorithms. It also supports a multi-traffic profile that allows voice and data service with the same terminal at the same time. The voice traffic is based on a TDMA (Time Division Multiplexing Access) transmission technology while the data traffic is based on a PDO (Packet Data Optimized) transmission technology. The PDO technology also allows a full compatibility with TCP/IP protocol and all the related facilities.

Thanks to the GPS receivers integrated inside the mobile terminals, it is possible to see the position of users on proper maps in the control room greatly improving the quality of security and emergency services and procedures. In Fig. 5 the main functionalities of the mobile communication system are shown.

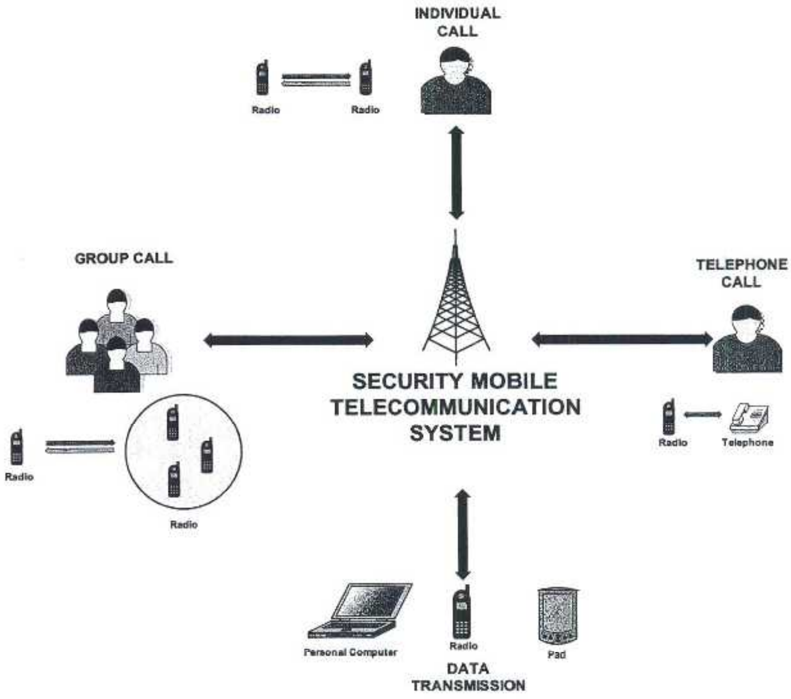


Figure 5: Main functionalities of the mobile communication system.

The mobile system uses two kinds of logical channels:

1. control channels
2. traffic channels

The control channels carry the signalling information. The radio terminals, when not busy in a call, listen continuously to the control channels when they receive information regarding the net (available close cell, available services, channel status, etc.) and can make the request to start a particular service.

The traffic channels carry the voice or data information. The traffic channels (from one to four for every used frequency according to the requested service) are assigned to the mobile terminals from the system and released from the terminal or from the net when the service is terminated.

The mobile subsystem offers the following vocal services:

1. Individual call: this service is equivalent to the communication through a cellular phone (i.e. a user calls another user).
2. Group call: a user calls a defined group. Every member of the group can listen and talk to everybody. The group is defined in a flexible way, i.e. each user can be added to the group or deleted from the group at any time.
3. Direct call: two or more radio units communicate directly without the support of the base station.
4. Broadcast call: that is a unidirectional point–multipoint call in a certain zone. The zone and the users can be dynamically defined.
5. Emergency call: that allows to make a high priority call pressing an emergency button on the radio unit.
6. Include call: that allows calling or inserting in a call one or more supplementary users.
7. Open channel: a group of users can talk on a certain radio channel and all the users can listen and talk at any time.

The mobile system offers the following data services:

1. Status transmission: that allows to broadcast short and predefined messages from the dispatcher to the radio units and vice versa.
2. Short data service: that allows to send predefined messages to single users or group of users.
3. Data transmission using a circuit commutation mode.
4. Data transmission using a packet commutation mode (X25, TCP/IP).

Further, the mobile subsystem is characterized by a high security level through:

1. Use of mutual authentication (radio unit–base station and vice versa)
2. Cryptographic communications using both static and dynamic keys
3. Support of end to end cryptographic communications
4. Disabling capabilities of stolen or lost radio units
5. Management of data directly through IP network using ciphered protocol

2.1 The genetic algorithms–based design of the mobile communication subsystem

The design of the mobile communication subsystem is a typical non-linear optimization problem where a goal must be reached (full coverage of the given area, contemporary number of users, contemporary number of group of users) respecting some restrictions (limited number of installation places available for the base station antennas, maximum emission of electromagnetic power, etc.).

This problem can be solved using genetic algorithms (GAs) [11–19].

In our problem we deal with peculiar restrictions such as the possibility of installing the BSs only on the terraces of the buildings.

Further, we need a full redundancy of the whole coverage area: that is, each point of the interested zones must be covered by almost two BSs so that a malfunction of one BS is immediately recovered by the other BS.

Further, it is necessary to consider the background noise that could be present in the area and that could reduce the coverage area of each BSs and the related transmission velocity. The background noise has been measured and evaluated preliminary.

In the following we describe how this peculiar problem is coded and solved in terms of GAs, that allow to solve it rapidly and in an efficient way, without illustrating particular details (such as final position of BSs, number of contemporary users, number of contemporary group of users, etc.) for secrecy reasons.

Genetic algorithms are considered wide range numerical optimization methods that use the natural processes of evolution and genetic recombination [11–17]. Thanks to their versatility, they can be used in different fields and they also find a lot of applications in wireless network optimization problems [18, 19].

GAs are particularly useful when the goal is to find an approximate global minimum in a high-dimension, multi-modal function domain, in a near-optimal manner. Unlike the most optimization methods, they can easily handle discontinuous and non-differentiable functions.

The algorithms encode each parameter of the problem to be optimized into a proper sequence (where the alphabet used is generally binary), called a gene, and combine the different genes to constitute a chromosome. A proper set of chromosomes, called a population, undergoes the Darwinian processes of natural selection, mating, and mutation, creating new generations, until it reaches the final optimal solution under the selective pressure of the desired fitness function.

GA optimizers, therefore, operate according to the following nine points:

1. encoding the solution parameters as genes
2. creation of chromosomes as strings of genes
3. initialization of a starting population
4. evaluation and assignment of fitness values to the individuals of the population
5. reproduction by means of fitness-weighted selection of individuals belonging to the population
6. recombination to produce recombined members
7. mutation on the recombined members to produce the members of the next generation
8. evaluation and assignment of fitness values to the individuals of the next generation
9. convergence check

The flow chart of GAs operative process is schematized in Fig. 6. In Fig. 6 the flow chart of GAs operative process is shown. In Fig. 7 the scheme of coding of problem parameters into chromosomes is shown.

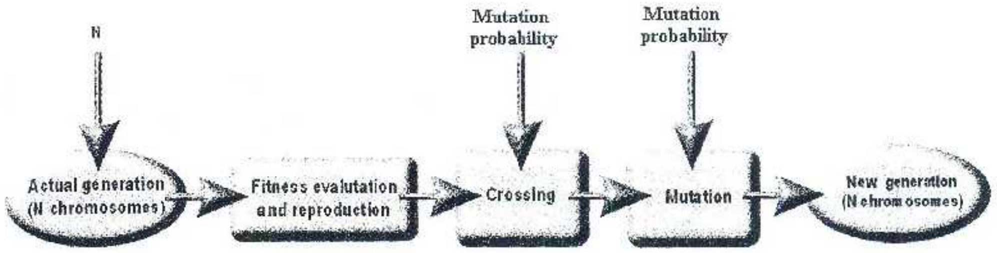

N
Mutation probability
Mutation probability
Actual generation (N chromosomes)
Fitness evalutation and reproduction
Crossing
Mutation
New generation (N chromosomes)

Figure 6: Flow chart of GAs operative process.

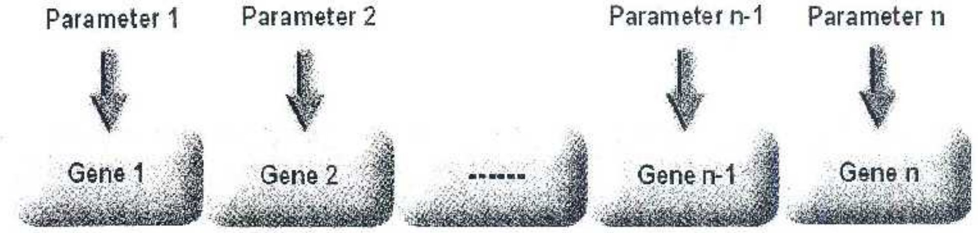


Figure 7: Scheme of coding of problem parameters into chromosomes.

The coding is a mapping from the parameter space to the chromosome space that transforms the set of parameters, which is generally composed of real numbers, in a string characterized by a finite length. The parameters are coded into genes of the chromosome that allows the GA to evolve independently from the parameters themselves and therefore from the solution space.

The parameters can be discrete or continuous. If they are continuous, it is generally necessary to fix some limits on them or to restrict the values that they can assume in a handful of possible range. In both cases a binary representation is generally used since it can be shown that coding has an underlying relevance in producing improved results and that it is better to use the shortest possible useful alphabet.

If g_i is the i-th coded gene representing the i-th parameter of the N solution parameters, encoded by means of M_i bits b, its structure is:

$$g_i = [b_1\ b_2\ b_3 \ldots\ldots. b_{Mi-1} b_{Mi}] \tag{1}$$

and the general chromosome c shows the following structure:

$$c = [g_1\ g_2\ g_3 \ldots\ldots. g_{N-1} g_N] = [b_1\ b_2\ b_3 \ldots\ldots. b_{M-1} b_M] \tag{2}$$

M being the sum of the bits that compose each gene; that is, $M = M_1 + M_2 + \cdots + M_{N-1} + M_N$.

The greater the number of bits used to represent a certain parameter the greater is the accuracy (but the slower is the convergence). The correct number of bits must therefore result as a compromise between the real precision required and the velocity of convergence.

Once created, it is necessary to choose the number of chromosomes that compose the initial population. This number strongly influences the efficiency of the algorithm in finding the optimal solution. A high number provides a better sampling of the solution space but slows the convergence. A good compromise consists in choosing a number of chromosomes varying between five and ten times the number of bits in chromosomes even if in most situations it is sufficient to use a population of 40 to 100 chromosomes which do not depend of the length of the chromosome itself. The initial population can be chosen at random or it can be properly biased according to specific features of the considered problem.

Fitness function (or cost function or object function) provides a measure of how good a given chromosome is and therefore, how good an individual within a population is. Since the fitness function acts on the parameters themselves, it is necessary to decode the genes composing a given chromosome to calculate the fitness function of a certain individual of the population. The fitness function is the only connection between the physical problem being optimized and the genetic algorithm. The only constraints on the form and content of the fitness function, imposed by GAs, are that the fitness value returned by the fitness function is in some manner proportional to how good a given trial solution is and that the fitness value is positive (even if a positive value is not always required).

The reproduction takes place utilizing a proper selection strategy which uses the fitness function to choose a certain number of good candidates. The selection process cannot be based only on choosing the best individuals, since they cannot be very close to the optimal solution. For this reason, there must be some chances that some unfit individuals are preserved to be sure that the genes carried by them are not lost prematurely from the population. A very common selection strategy is represented by the proportionate selection, where individuals compete on the basis of their fitness. The individuals are assigned a space of a roulette wheel that is proportional to the fitness. The higher the fitness, the larger is the space assigned on the wheel and the higher the probability to be selected at every wheel tournament. The tournament process is repeated until a reproduced population of N individuals is formed.

The recombination process selects two individuals of the reproduced population at random, called parents, crossing them to generate two new individuals, called children. The simplest technique is represented by the single-point crossover where, if the crossover probability overcome a fixed threshold, a random location in the parent's chromosome is selected and the portion of the chromosome preceding the selected point is copied from parent A to child A and from parent B to child B, while the portion of chromosome of parent A following the random selected point is placed in the corresponding positions in child B and vice versa for the remaining portion of parent B chromosome. If we point out with c_p^A and c_p^B the chromosomes of parents A and B respectively, and if R is the random location:

$$c_p^A = [b_1^A\, b_2^A\, b_3^A \ldots b_{R-1}^A \,|\, b_R^A \ldots . b_{M-1}^A b_M^A] \tag{3a}$$

$$c_p^B = [b_1^B\, b_2^B\, b_3^B \ldots b_{R-1}^B \,|\, b_R^B \ldots . b_{M-1}^B b_M^B] \tag{3a}$$

their children c_c^A and c_c^B, generated by the crossover, are:

$$c_c^A = [b_1^A\, b_2^A\, b_3^A \ldots b_{R-1}^A \,|\, b_R^B \ldots . b_{M-1}^B b_M^B] \tag{4a}$$

$$c_c^B = [b_1^B\, b_2^B\, b_3^B \ldots b_{R-1}^B \,|\, b_R^A \ldots . b_{M-1}^A b_M^A] \tag{4a}$$

If the crossover probability is below a fixed threshold, the whole chromosome of parent A is copied into child A and the same happens for parent B and child B. The crossover is useful to rearrange genes to produce better combinations of them and therefore more fitting individuals. The recombination process has shown to be very important and it has been found that it should be applied with a probability varying between 0.6 and 0.8 to obtain the best results.

The mutation is used to survey parts of the solution space that are not represented by the current population. If the mutation probability overcomes a fixed threshold, an element in the string composing the chromosome is chosen at random and it is changed from one to zero or vice versa, depending on its initial value. To obtain good results, it has been shown that mutations must occur with a low probability varying between 0.01 and 0.1.

The converge check can use different criteria such as the absence of further improvements, the reaching of the desired goal or the reaching of a fixed maximum number of generations.

After the above overview on GAs, we illustrate the implementation of the considered problem.

Once the area to be covered is calculated, whose value is A_T, and once given the maximum coverage distance R_{BS} of a BS (which is the circular diagram that indicates where the emitted signal is above a minimum receivable threshold and that is obviously related to the irradiation diagram and the emitted power), whose area is $A_{BS} = \pi R_{BS}^2$, the minimum number $N^{BS}{}_{min}$ of BSs is equal to:

$$N_{min}^{BS} = 2 \cdot \text{round}\left(\frac{A_{SENATE}}{\pi R_{BS}^2}\right) \quad (5)$$

where the rounding operation is made toward the nearest integer equal or greater than the argument of the operation. The coefficient 2 is present since we desire a double coverage (full redundancy) of the Senate area.

The number obtained from equation (5) is obviously ideal since it can be reached if all the Senate area is available for BSs placement and if the coverage diagram is characterized by a regular shape (i.e. square, etc.) that allows to ensure a perfect matching between the coverage of nearby BSs. It is evident that in real conditions, the minimum number of BSs necessary that ensures the complete coverage of the Senate buildings area with the desired redundancy is obviously greater than the value calculated by means of equation (5), due to the not-perfect matching of the coverage diagram of near BSs and due to the limitation of places for BSs installation.

For this reason, given the interested area, it is considered an initial number, $n*N^{BS}{}_{min}$, of BSs (where n is a parameter, > 1, to choose at will) greater than the minimum number $N^{BS}{}_{min}$, leaving the GA to optimize and reduce their number, according to the availability of installation places, reaching eventually the value of $N^{BS}{}_{min}$ in ideal conditions.

Once defined the initial number $n*N^{BS}{}_{min}$of BSs, it is necessary to define the parameter to be optimized for each BS, represented by its coordinates. To increase the optimization capability of used GA, it is also considered the control of emitted power of each BS that allows to reduce linearly the maximum radius of coverage R_{BS} up to zero so that the GA is capable of a fine matching of coverage diagram of near BSs.

Since not all the initial BSs are used to perfectly cover the considered territory, it is necessary to add, for each BS, information that indicates if the BS is active or not.

Further, since the number of contemporary users and the number of contemporary group of users depends on the number of frequency of each BS, it is necessary to add this information to each candidate solution of BSs.

These considerations lead to five solution parameters, for each BS, that are:

1. *x*-coordinate
2. *y*-coordinate
3. activity of the BS
4. reduction of maximum coverage distance R_{BS}
5. number of frequencies

Let's discuss now the variability range of the parameters indicated above and the relative accuracy necessary to represent them in term of binary strings.

Concerning the x and y coordinates, if we choose a 1 m resolution, and we consider the maximum extension of the zone interested by the buildings of the Senate ($\approx$ 2 km), 10 bits are enough to represent the distance between 1 m and 2.048 m (i.e. $\approx$ 2 km).

The activity of each BS is coded using a single bit, where a binary 1 indicates that the BS is active while a binary 0 indicates that the BS is not active, even if it is located in a given (x, y) position.

The reduction of maximum coverage distance can vary between 0% and 100%. We choose to use 7 bits that allow representation of 127 numbers. Since the necessary numbers to code the percentage with a resolution equal to 1% are only 100, the remaining 27 values are used to represent the corresponding percentage values between 0% and 27%, maintaining them active in the evolution process. A 6 bit encoding is not possible since it allows to represent only 64 numbers with a resolution of 1 unit that is not enough for our purposes.

The number of frequencies has been chosen to be variable between 1 and 8 and therefore has been coded with 3 bits.

5 genes are therefore used to encode the parameters of each BS whose total length is equal to 29 bits. The genes features are summarized in Table 1.

Each chromosome, or individual, representing a solution of the problem, is composed by a string representing all the $n^*N^{BS}{}_{min}$ BSs and the related five parameters (whose total length is equal to 29 bits). The total length of each chromosome is therefore equal to $29^*\ n^*N^{BS}{}_{min}$ bits.

It is now necessary to define the fitness function f. This function must consider all the desired optimization goals, which are:

1. integral coverage of the Senate area with the minimum number of BSs
2. overlapping of coverage diagram by means of almost 2 BSs, to increase the communication reliability as much as possible
3. placement of BSs only in the allowed zones (Senate palace terraces)
4. number of contemporary users
5. number of contemporary group of users
6. maximum emitted power

The first two points are synthesized with a proper function while the third point is considered using a proper territorial array.

Table 1: Features of the 5 genes used to identify a BS.

Base station parameters			
Gene	Feature	Number of bits	Range
1	x coordinate	9	0 ÷ 2.047 meters
2	y coordinate	9	0 ÷ 2.047 meters
3	Activity of BS	1	0 ÷ 1
4	Reduction of maximum coverage distance R_{AP} of AP	7	0 ÷ 100 %
5	Number of frequencies	3	1 ÷ 8

The considered fitness function of the generic chromosome C can be expressed as:

$$f(C)=\frac{\dfrac{\text{coverage area}(C)}{\text{total coverage area}}\cdot\dfrac{\text{redundant overlapped area}(C)}{\text{total coverage area}}}{\dfrac{N^{BS}(C)-N^{BS}_{\min}}{N^{BS}_{\min}}+1} \tag{6}$$

where 'coverage area (C)' is the area covered by the BSs distribution related to the chromosome C, or individual I, $N^{BS}(C)$ is the number of active BSs related to the chromosome C and 'redundant overlapped area (C)' is the total area of redundant overlapping of the different coverage diagrams of APs to increase the reliability of the coverage field.

The mentioned function keeps into consideration the performances of the chromosome C (BSs distribution) in terms of coverage area (first term of numerator), in terms of respecting of redundant overlapping (second term of numerator) and in terms of reduced number of BSs (denominator). The number one that has been added as second term of the denominator is necessary to avoid divergence toward infinity when the fitness function is used to evaluate a chromosome C that uses a minimum number $N^{BS}{}_{min}$, of BSs.

The information relative to the allowed zones for BSs placement is stored in a proper binary array, characterized by the same dimensions and resolution of *(x, y)* coordinates of BSs. Each element of the array (representing a cell of the Senate area whose dimensions are 1 m × 1 m) that can be used for BSs placement is marked with a binary zero and each element of the array that cannot be used for BSs placement is marked with a binary 1. Practically inside the mentioned array, the profile of the Senate area (terraces of buildings) is stored.

The control about the BSs placement in not-allowed zones is made at any genetic operation (reproduction, crossing, mutation), checking in the proper array if the coordinate of the BSs of the actual chromosome C, or individual I, are marked with a binary 1 if this happens, the related chromosome is deleted.

The control about the number of users and number of group of users is made at any genetic operation (reproduction, crossing, mutation), checking if the total number of frequencies of the BSs of the actual chromosome C, or individual I, allows to reach the requested goal. If this doesn't happen, the related chromosome is deleted.

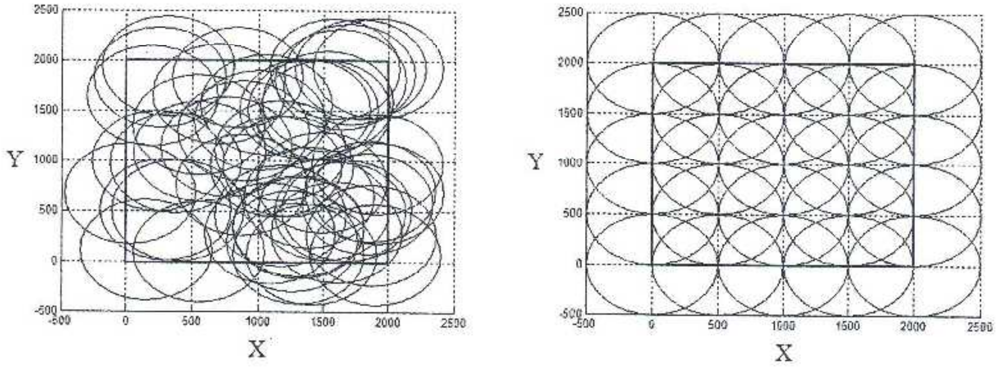
The same considerations are valid for the maximum emitted power.

Once the initial population is generated at random, the individuals characterized by BSs not-allowed placement are eliminated and the selection is operated only on the remaining individuals until a reproduced population characterized by the same number of individuals of the initial population is attained.

Since the initial population is initialized at random, there is generally a portion of it that is eliminated at the beginning. But after the first iterations, more fitting individuals are generated and it is not necessary to eliminate any of them.

Once the population is recombined and mutated, the fitness function of the population is again calculated with the same criteria illustrated above, considering only fitting individuals. The converge test is made controlling if the difference between the mean value of fitness functions of the valid individuals belonging to the actual generation and the mean values of the last N_G generations is lesser than a certain percentage value p_{stop}.

Good results and rapid converge are obtained with population composed of 50 to 60 individuals, with converge test parameters N_G and p_{stop} equal to 25 and 0.08 respectively. In Fig. 8 an example of initial random distribution on BSs (a) and final distribution (b) without restrictions on BSs placement is shown.



(a)

(b)

Figure 8: Example of initial random distribution on BSs (a) and final distribution (b) without restrictions on BSs placement. n parameter is equal to 2. The distance R of coverage is 500 m for every BS.

The proposed GA has demonstrated to be extremely versatile in BSs optimal placement in areas, such as the one of Senate, where a plenty of restrictions are present. The optimal solutions are generally obtained after a limited number of generations that rarely overcomes 150 iterations.

The computation time strictly depends of the number of BSs considered since each of them adds 29 bits to each chromosome and therefore 29 bits of information to be handled by the GA. The number of BSs grows with the reduction of maximum coverage R_{BS} of BSs. The longer this distance and the lesser the number of BSs and therefore the time necessary to reach the final optimal solution increases.

An example of BSs placement without restrictions on BSs placement zones, number of users, number of groups, and fixed coverage radius (same emitting power) is shown in the next figure. It is possible to see that the BSs are placed regularly to guarantee a double coverage of each point and that the number of BSs is reduced of about 50% with respect to the initial random distribution.

Since the proposed design technique must be independent from any particular commercial devices, different optimizations were made considering variable values of maximum reachable distance R_{BS} of BSs to know for which values the maximum reduction of initial number of BSs is obtained for a given number of contemporary users and contemporary groups of users. The n parameter to be multiplied for $N^{BS}{}_{min}$ was chosen to be equal to 2. The results are shown in Fig. 9.

It is possible to see that the maximum reduction of number of BSs is obtained if devices that ensure a maximum coverage distance more than 1.250 m are used. This can explain the position of the buildings and the number of contemporary users. In fact, due to the maximum number of frequencies allowed, a short-medium range coverage of BSs is preferable (with respect to a long coverage or a short coverage) due to the possibility of GA of optimizing their position with respect to the restrictive design condition imposed. Even if long range BSs are used, since the GA can also control the coverage range, the BSs are always placed in the same position, reducing properly their coverage distance to guarantee the maximum number of contemporary users. This also implies that it is not necessary to choose more expensive long range

BSs, since a coverage of only 1.250 m ensures optimal results in terms of reduction of number of BSs and therefore in terms of increasing the reliability of the mobile communication network. On the contrary, when short range BSs are used, it is necessary to use a higher number of them to guarantee reaching the desired number of users and groups of users, and therefore the reduction of initial amount of BSs is lesser, as it is possible to see from above figure.

It is obvious that different design solutions were obtained, each of them characterized by a different placement of BSs in the Senate area and all respecting the design conditions. They are not shown in figure above for brevity.

We have therefore studied an efficient technique that uses GAs for BSs placement in areas with different kind of restrictions, such as the Senate buildings. It is capable of operating on any kind of real situation, reaching optimal results.

It has been used in the initial planning of mobile communication network, adding later further restrictions, which have been identified, to improve the found solutions.

It gives not only different optimal solutions for base stations placement on the terraces of Senate buildings but also the maximum coverage requested (emitted power) for the BSs to reach the minimum cost of installation.

The use of GA techniques on this kind of problem ensures to find, always and efficiently, quasi-optimal solutions that would otherwise be impossible to find due to the considerable numbers of parameters involved in the optimization problem and due to the numerous restrictions to be considered in the resolution of the problem. In Fig. 9 the reduction [%] of the initial number of BSs as a function of the maximum coverage.

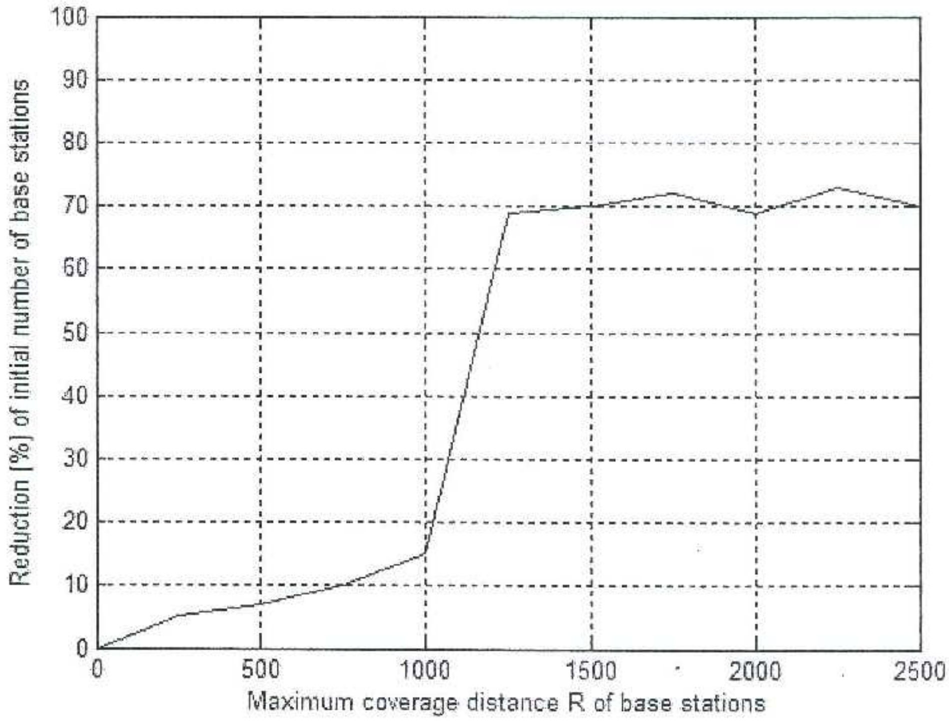


Figure 9: Reduction [%] of the initial number of BSs as a function of the maximum coverage distance R_{BS} (emitted power) of BSs to be installed.

distance RBS (emitted power) of BSs to be installed is shown.

3 THE VIDEO SURVEILLANCE SUBSYSTEM

The video surveillance subsystem (VSS) is designed to allow the operators to control any zone of the buildings and to reconstruct, in a second's time, any kind of event thanks to the high storing capabilities of the subsystem. It also integrates the alarms coming from the other subsystems, providing a visual access to the area of the signaled events.

The integration with the other subsystems is realized by means of:

1. supervision system that represents the central element for the management of the whole security system.
2. direct integration, obtained through the direct connection of the different components of other subsystems.

The VSS uses the communication services offered by the security network described above to transmit images, both in real time and recorded, to the interested operators. The access to the stored images is properly restricted to comply with Italian privacy laws.

The VSS is capable of individuating any intrusion attempts through the external perimeters of the buildings. For this reason it is necessary to transmit, in real time, all the images necessary to evaluate the events or to send them to proper automatic devices that analyze the scenes and generate an alarm to the operator only in dangerous situations.

Image acquisition is made through an optimal visualization of the controlled areas, using both wide angle and narrow angle camera objectives, according to the characteristic of the zones.

The VSS is also equipped with high storage capabilities and it is able to:

1. record the images coming from all the cameras.
2. allow easy access to the images archive to analyze, in a second's time, any critical event.

The VSS has been designed and realized to guarantee high standard of efficiency, quality, scalability, opening, operative flexibility, reliability, and security, according to the respect of privacy imposed by Italian privacy laws. In Fig. 10 the scheme of the video surveillance subsystem is shown. In Fig. 11 the logical architecture of the video surveillance subsystem is shown.

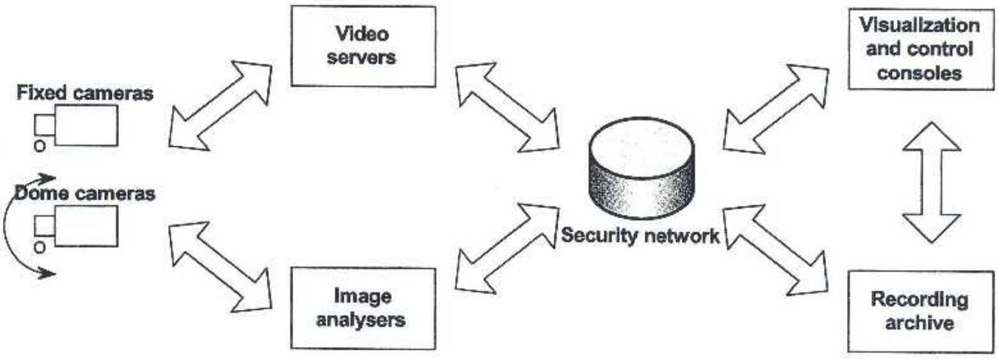


Figure 10: Scheme of the video surveillance subsystem.

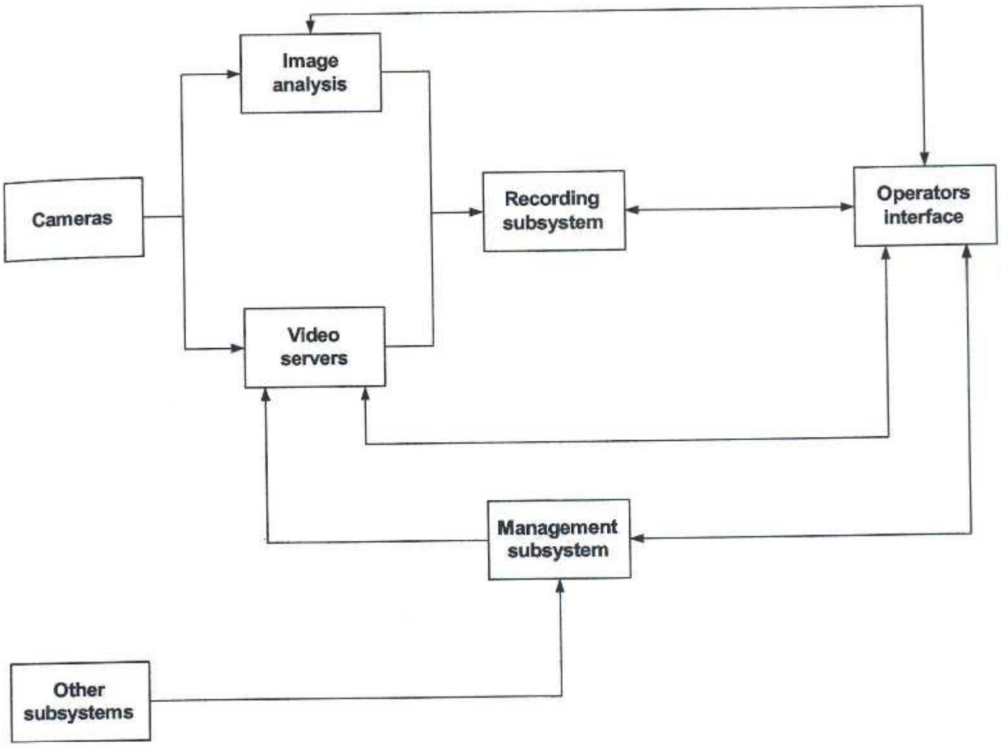


Figure 11: Logical architecture of the video surveillance subsystem.

The VSS is based on a mixed analogue/digital architecture. All the cameras are analogue, to guarantee a high quality images to be locally analyzed by proper analysis devices. The images are locally converted in digital format, by a proper local video server, to be sent toward the control room and toward the distributed consoles which need that image using a TCP/IP protocol. The VSS is composed by the following main components:

1. Cameras: two different kind of cameras are used – fixed, to control the entrances of the buildings and dome, to control the external areas
2. Video servers: convert the analogue signal coming from cameras into a digital signal to be sent through the dedicated security network
3. Images analyzers: analyze the images coming from the cameras through advanced techniques and algorithms to automatically reveal critical situations. The related alarms are sent to the related operators through the telecommunication network
4. Control and visualization consoles: the consoles are present in the main control room and entrance gate houses of the palaces
5. Recording system: stores all the images coming from the cameras through the network, located in the main control room. Access to the image archive is properly protected to comply with the Italian privacy laws
6. Telecommunication network: represents the backbone of the whole security system (this has already been described before). It allows the communication between all the components of the video surveillance subsystem. In Fig. 12 the physical architecture of the video surveillance subsystem is shown.

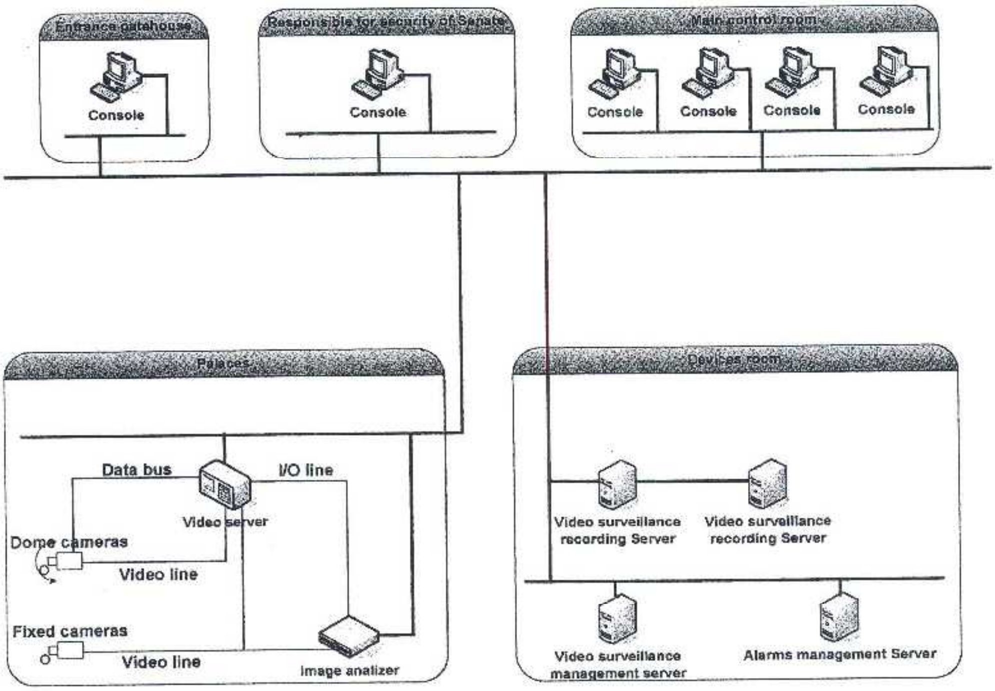


Figure 12: Physical architecture of the video surveillance subsystem.

The VSS is composed by the following logical elements:

1. field devices (cameras)
2. digitalization devices
3. image analysis devices
4. recording devices
5. management devices
6. operator interfaces

The VSS can be divided into three typology of elements:

1. Peripheral: composed by the cameras (fixed and dome with automatic commutation day/night), infrared illuminators, image analysis devices, video servers.
2. Access points: represented by the consoles located in the control room and the entrances. They allow a full access (according to their functionalities) to the real time images. Access to the recorded images is restricted to specific users. In the control room, LCD colour displays and wide screen plasma displays are used to view the images of particular interest. Particular care was taken in designing the human–system interface from the control room point of view. All the controls are made by means of simplified interfaces such as guided menus, keyboards, and joysticks, reducing the complexity as much as possible and making them extremely user-friendly. In this way,

the stress of the operators is reduced, letting them face any critical events with the necessary concentration.

3. Control center: represented by all the devices dedicated to the management and control of the whole subsystem (servers, recorder, etc.)

4 THE ACCESS CONTROL SUBSYSTEM

The access control subsystem (ACS) controls all the entrances of the buildings and the technological installation rooms.

It is characterized by a high modularity so that it is possible to add further entrances without any problems.

The ACS uses hands-free radiofrequency badges together with biometric face recognition and all the events are properly visualized and recorded by means of the video surveillance subsystem. Locally, a display shows the face of the entering person and the image is recorded into the database for an immediate visual recognition and control to be made by the entrance security personnel. In Fig. 13 the physical architecture of the access control subsystem is shown.

The ACS allows:

1. the identification of the persons
2. the management of the internal areas as a function of the requested security level
3. a high degree of security of the working environments
4. a greater goods protection

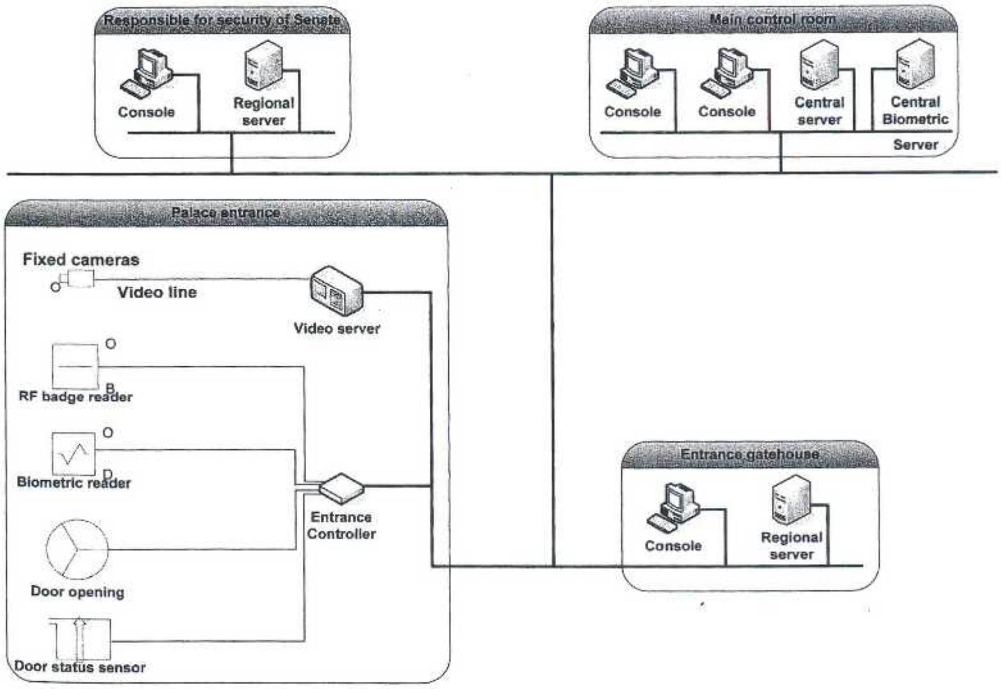


Figure 13: Physical architecture of the access control subsystem.

5. a reduction of costs due to a more rational use of human resources
6. a double level of protection (people and goods)
7. a high safety level, since it is possible to know, in an emergency situation, the exact number of persons present inside each building
8. a proper integration with the security system to obtain advanced functionalities.

The ACS is based on a distributed architecture with central database and regional databases. In this way, in case of temporary loss of the network, the subsystem is capable of working without any problems, updating the central database when the communication is restored.

The ACS is composed of the following main components:

1. central server
2. biometric central server
3. regional servers
4. entrance controllers
5. entrance consoles

The central server stores the user profiles, the installations configuration, and the history of alarms and events. It duplicates this information on the regional servers.

The biometric server stores the face pictures of users, importing the related information and profiles from the central server. It duplicates this information on the regional servers.

The regional servers store all the information related to the users and all the history of alarms and events that are verified in the controlled entrance. It communicates with the central server and with the biometric central server to keep the central database updated.

The entrance controllers work as an interface between the regional servers and the badge readers, sensors, and electrical lockers of the automatic entrances.

The entrance consoles are located close to the entrances and are used by the security personnel. They allow security personnel to:

1. visualize the transits and the face of entering people
2. manage the alarms
3. manage the entrances
4. check the state of every entrance devices (sensors, actuators, badge readers, etc.)
5. configure the local ACS components

Every operation made by the operators is properly recorded into the ACS and it is available to be controlled in a second's time.

The radiofrequency badge readers comply with all the international laws concerning human exposure to electromagnetic fields and are characterized by a reduced emission level.

The badges are to be used with all the internal operative services of the Senate and are composed by three sections:

1. radiofrequency
2. magnetic strips
3. microchip

In case of the malfunctioning of one modality (radiofrequency badge or face recognition), the entrances can be enabled to work in a single modality instead of double modality to guarantee access to the people. In this way, the security personnel are aided by the real image of the person compared on the display with the image stored into the database.

Proper consoles are located in the office dedicated to the generation and printing of badges for face enrolment and storage into the database.

5 THE ANTI-INTRUSION SUBSYSTEM

The anti-intrusion subsystem (AIS) is dedicated to the perimeter control of the buildings and to the acquisition of internal alarms activated by means of proper buttons. It uses proper input/output (I/O) modules to read the field sensors information and to send them, through the network, to the consoles of the control rooms. It allows:

1. concentration of the alarms toward the dedicated consoles
2. control of the field devices to inform in real time the central system of eventual anomalies and malfunctioning to request proper repairing procedures
3. interfacing with the other subsystems, in particular the video surveillance, to activate joint procedures in case of alarm (such as activation of the nearest cameras to view directly the alarmed zones)

The AIS, like the other subsystems, is totally autonomous and self-consistent so that it is capable of working even in the absence of control by the supervision subsystem.

The field sensors are represented by:

1. perimeter barriers on the terraces
2. magnetic contacts on door and windows
3. anti-aggression button
4. mobile radiofrequency alarm button devices

The AIS is characterized by a high modularity so that it is possible to add further I/O modules, thanks to the capillary presence of the security network in any building, and further field sensors.

The I/O modules can connect to the field sensor by means of direct connection or by means of serial bus connection. They can be programmed to interface with any kind of device and communication protocol.

All the alarms and events are displayed on the consoles of the control rooms.

6 THE FIRE DETECTION/EXTINGUISHING SUBSYSTEM

The fire detection/extinguishing subsystem (FDES) is capable of monitoring any part of the buildings, allowing the security personnel, thanks to the proper consoles, to be informed immediately in case of fire.

It is composed by different control panels (one or more control panels per building), located in the entrances gatehouse of the building where the security personnel is always present. The control panels are interfaced with a console where the alarmed zones are shown through proper maps to allow an immediate localization of the fire events. It also allows a direct vision of the alarmed building by means of the nearest camera of the video surveillance subsystem. The control panels are further more interfaced with the central supervision and control system to let the fire events be signaled in the control rooms.

The FDES is also complemented by a public address message diffusion system (PAMDS). Each local console is interfaced with the local PAMDS to allow an immediate local diffusion of the alarm messages. Each PAMDS is interfaced with the central supervision and control system, through the security network, so that it is possible to send vocal messages to the different zones of the buildings from the control room.

The PAMDS is equipped with different audio channels and it is capable of handling both pre-recorded message and operators real-time messages.

The division of the FDES in different independent modules (local control panels) ensures a high reliability and a capability of working even in case of malfunctioning of upper level components (local consoles, network, and control room).

Different kinds of sensors have been used as a function of the controlled environments. They are:

1. interactive
2. analogical
3. collective
4. addressable
5. linear barrier
6. wireless

All the sensors have been installed according to the Italian and European laws. In Fig. 14 the physical architecture of the fire detection subsystem is shown.

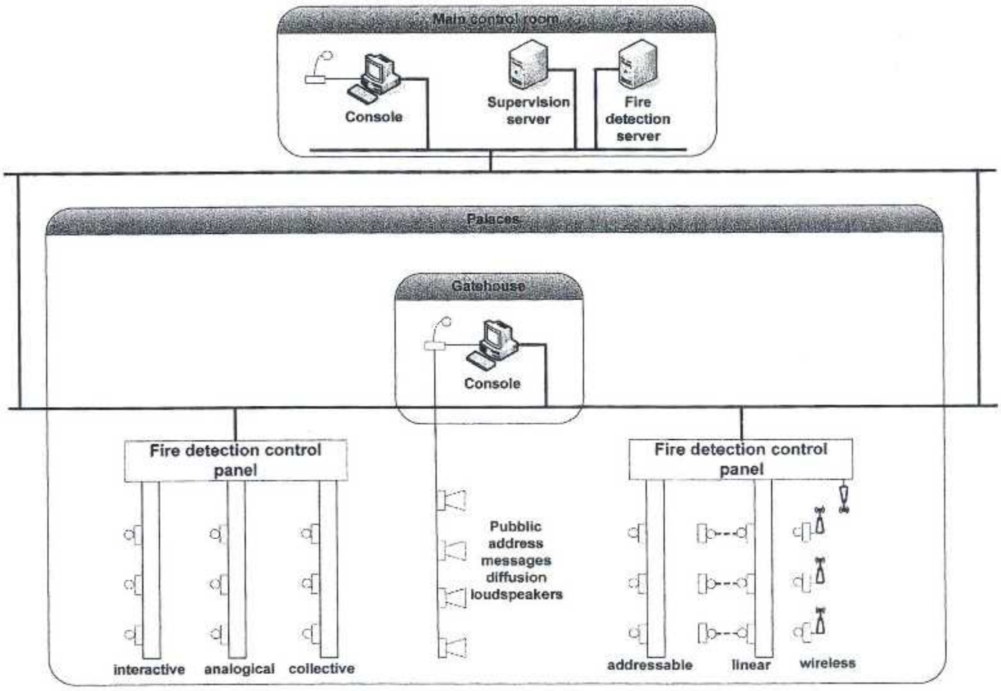


Figure 14: Physical architecture of the fire detection subsystem.

Gas detection sensors (carbon dioxide, methane, hydrogen, etc.) are installed and controlled in the technological rooms.

The local control panels are also connected to:

1. fire alarm signaling buttons
2. fire signaling flashing panels
3. fire-proof doors opening electromagnets
4. fire extinguishing installations.

All the air-conditioning ducts are properly controlled by air analysis units.

A proper integration server is installed in the control room. It is used to interface all the fire detection control panels with the supervision and control system.

7 THE SUPERVISION AND CONTROL SUBSYSTEM

The supervision and control subsystem (SCS) is the integrating element of the different subsystems (even if these last ones are also connected at a lower lever in some cases), offering superior functionality with respect to the functionalities offered by the separated subsystems.

It allows an optimization of the management and control procedures, reporting all the signaling and alarms on the consoles of the control room.

The SCS uses an open software platform which is extremely flexible and programmable so that it is very easy to be used and to be expanded to add new components in a second's time.

The SCS uses the dedicated security network to exchange information with the different subsystems to control them even if they are totally autonomous from the SCS, being able to operate even in the absence of coordination.

The advanced functionalities of the SCS are available on the consoles of the control room even if any console can be added in any place of the Senate for particular and momentary needs, thanks to the capillarity diffusion of the security network.

All the information is shown on proper maps, allowing a clear and immediate view and management of the events through appropriate software buttons present on the maps themselves.

All the alarms, the signaling, and the operator actions are stored into the historical database of the SCS. In Fig. 15 the logical architecture of the supervision and control system is shown. In Fig. 16 the logical architecture of the control module is shown.

The SCS is characterized by:

1. integration with other subsystems
2. autonomy from the other subsystems
3. expandability
4. scalability
5. operative flexibility
6. reliability
7. high security level

It can control:

1. single sensors and cameras
2. whole installations
3. any other element and device in the field

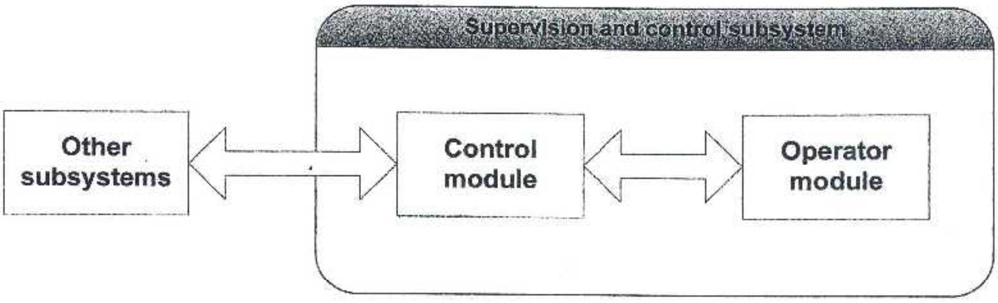


Figure 15: Logical architecture of the supervision and control system.

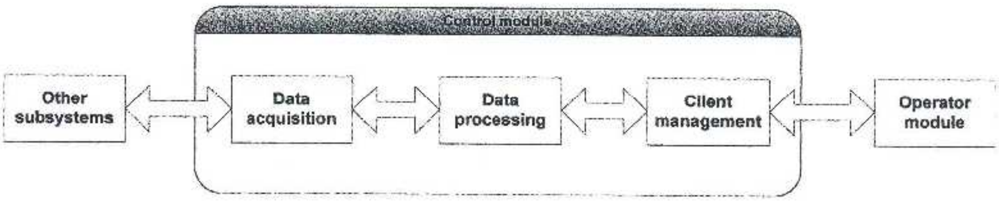


Figure 16: Logical architecture of the control module.

It is composed by:

1. central redundant servers
2. consoles
3. security telecommunications network

The logical architecture of the SCS can be divided it into two functional modules:

1. control module
2. operator module

The control module is constituted by three different sub-modules:

1. data acquisition
2. data processing
3. client management

The data acquisition sub-module takes care of interfacing with other subsystems, managing all the problems related to the connection with other plants and related to the coding/ decoding of messages (communication protocols). It mainly adapts the data received from the field sensors and installations in the standard format useful for the control module.

The data processing sub-module is the core of the subsystem and it takes care of controlling the data, generating alarms, and actuating the actions associated with the alarms. It can work under the supervision of the operator or automatically, according to pre-defined procedures. The automatic actions can be:

1. storing of the state variation into the historical database
2. alarm generation and notification to the interested operator consoles
3. storing of the alarms in the historical database
4. activation, without operator action, of a pre-defined command after proper signaling
5. reproduction of an audio file, on the interested operator consoles, to signal a particular event
6. automatic opening of a video windows, on the interested operator consoles, to show the image related to a particular event
7. automatic opening of a synoptic map, on the interested operator consoles, to show a particular event.

The client management sub-module manages the information exchange with the operators, answering to the interface requests and sending it all the data.

The operator module represents the element of SCS that interacts with the operators. In Fig. 17 the logical architecture of the operator module is shown

The operator module is constituted by two different sub-modules:

1. supervision and control
2. configuration and management

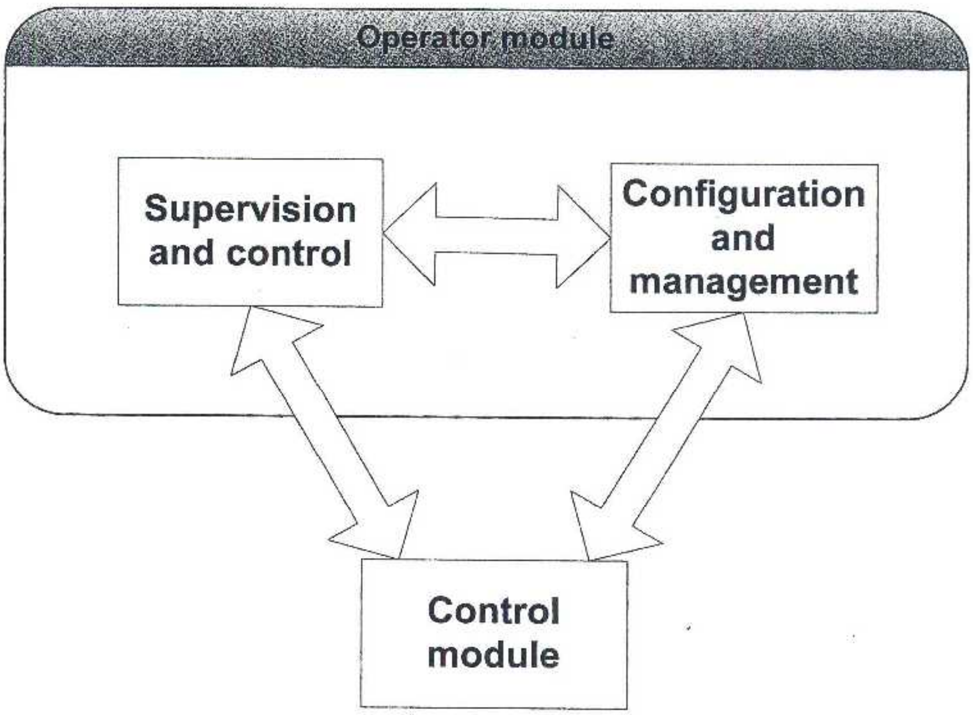


Figure 17: Logical architecture of the operator module.

The supervision and control subsystem takes care of interfacing with the operators to allow full control of the subsystems.

The configuration and management sub-module allows specialized personnel to configure and manage the whole system. It is controllable through a proper dedicated console, whose access is properly protected.

Both the sub-modules communicate with the control module, in particular with the client sub-module, to:

1. receive the events signals coming from the controlled subsystems and send them the action to be executed
2. send the configuration information.

8 CONCLUSIONS

The security management in complex contests such as the Italian Senate of the Republic needs a detailed risk analysis and a correct study, design, and realization of an efficient telecommunication subsystem that is capable of integrating different security subsystems, thanks to the aid of a supervision and control subsystem, ensuring the maximum reciprocal interaction of the different subsystems involved.

In this way, it has been possible to realize a powerful and versatile integrated security system that guarantees a high level of security services of the Italian Senate of the Republic.

REFERENCES

[1] Waltz, E., *Information Warfare – Principles and Operations*, Artech House Publisher: Boston (USA), 1998.

[2] Denning, D.E., *Information Warfare and Security*, Addison-Wesley: Boston (USA), 1999.

[3] Nichols, R.K. & Lekkas, P.C., *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill: New York (USA), 2002.

[4] Garzia, F., The integrated safety/security system of the AccademiaNazionaledeiLincei at CorsiniPalace 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] Garzia, F. & Veca, G.M., 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] Antonucci, E., Garzia, F. & Veca, G.M., The automatic vehicles access control system of the historical centre of Rome, *Sustainable City II*, WIT Press: Southampton (UK), pp. 853–861, 2002.

[7] Garzia, F., Sammarco, E. & De Lucia, M., The security telecommunication system of the Vatican CityState, *Risk Analysis IV*, WIT Press: Southampton (UK), pp. 773–782, 2004.

[8] Garzia, F., Sammarco, E. & Cusani, R., The integrated access control system of the Vatican CityState, *SAFE 2007*, WIT Press: Southampton (UK), pp. 431–440, 2007.

[9] Garzia, F., Sammarco, E. & Cusani, R., Integrated access control system for ports, *SAFE 2009*, WIT Press: Southampton (UK), pp. 313–323, 2009.

[10] Garzia, F., Sammarco, E. & Cusani, R., The integrated security system of the Vatican CityState, *International Journal of Safety & Security Engineering*, **1(1)**, pp. 1–17, 2011.

[11] Davis, L., *Genetic Algorithms and Simulated Annealing*, Morgan Kaufmann Publishers, Inc.: Los Altos, CA, 1987.

[12] Davis, L., *Handbook of Genetic Algorithm*, Van Nostrand Reinhold: New York, 1991.

[13] Diaz, A.H.F. & de Vasconcelos, J.A., Multiobjective Genetic Algorithms Applied to Solve Optimization Problems. *IEEE Transactions of Magnetics*, **38(2)**, pp. 1133–1136, 2002.

[14] Goldberg, D.E., *Genetic Algorithms in Search, Optimisation and Machine Learning*, Addison-Wesley: New York, 1989.

[15] Goldberg, D.E. & Deb, K., *Foundations of Genetic Algorithms*, Morgan Kaufmann: New York, 1991.

[16] Holland, J.H, Genetic algorithms. *Scientific American*, pp. 66–72, 1992.

[17] Winter, G., Periaux, J., Galan, M. & Cuesta, P., *Genetic Algorithms in Engineering and Computer Science*, John Wiley & Sons, Inc.: New York, 1995.

[18] Garzia, F. & Cusani, R., Optimisation of cellular base stations distribution in territory with urban and environmental restrictions by means of genetic algorithms, *Proceedings of EETI 2004 Energy, Environment and Technological Innovation*, Rio de Janeiro (Brazil), 2004.

[19] Garzia, F., Perna, C. & Cusani, R., UMTS network planning using genetic algorithms, *International Journal of Communications and Network*, **2(3)**, pp. 193–199, 2010.