The security telecommunication system of the Vatican City State

Fabio Garzia, Roberto Cusani
INFOCOM Department
SAPIENZA – University of Rome
Rome, Italy
fabio.garzia@uniroma1.it

Enzo Sammarco
General Direction of Safety, Security and Civil Protection
Vatican City State

Abstract— **The security of a modern state is strongly related to the telecommunication system of the State itself. Any weakness of the system involves a weakness of the security of the State. For this reason it is necessary to design and realize highly integrated, efficient and reliable telecommunication systems. The authors illustrate the work made to design and realize the security telecommunication system of the Vatican City State.**

Keywords – telecommuncation system, integrated security system, control system.

I. INTRODUCTION

The Vatican City State extends over a surface of about 44 hectares in the heart of Rome in Italy. It is also composed by other detached zones such as the summer residence of the Pope, located in Castel Gandolfo, on the hills close to Rome, and others. The territory is also composed by some important detached Basilicas, such as S. John and Holy Mary.

Figure 1. View of S. Peter Basilica and of part of Vatican City State.

Even if the extension of the State is quite reduced, the Vatican State is characterized by the same security and telecommunication needs of any other State that are further amplified by the reduced dimensions of the State.

For this reason it has been designed and realized a security telecommunication system that is able of guaranteeing a high level of efficiency and security in ensuring the communication services of the State.

The scope of the paper is to illustrate the mentioned advanced telecommunication system, the difficulties found for its design and realization, and the results obtained, from its installation, in the normal and emergency situations.

Due to secrecy reasons, the telecommunication system is illustrated according to the general philosophy design, without illustrating specific details that could compromise the security of the system itself.

II. ROLES OF INFORMATION AND TELECOMMUNICATION SYSTEM IN SECURITY

Information plays a crucial roles in security, since it is vital in the typical offence, defence and dominance phase of any conflict [1, 2].

The general term of “information” encompasses three levels of abstraction, distinguished by information as both content and process, that are:

1) data: observations, measurement, and primitive messages;

2) information: organized set of data. The organizational process may include sorting, classifying, or indexing and linking data to place data elements in relational context for subsequent searching and analysis;

3) knowledge: information, once analysed and understood. Understanding of information provides a degree of comprehension of both static and dynamic relationships of objects of data and the ability to model structure and past and future behaviour of those objects. Knowledge includes both static content and dynamic processes. Sometimes it is also called intelligence.

The role of electronically collected and managed information at all levels has increased to become a major component of any security context.

The electronic transmission and processing of information content has expanded both the scope and speed of any security process: the greater the capability of managing information rapidly and the higher is the probability of ensuring an efficient defence to any kind of attack.

It is therefore clear that an efficient telecommunication system plays a crucial roles in the transmission of information: the more it is powerful and well designed and the more a security system (intended as integration of technologies, procedures and surveillance personnel) is efficient.

III. THE SECURITY TELECOMMUNICATION SYSTEM

The telecommunication must serve not only for voice but also for security data communication [3-9].

It is the backbone of the integrated security system (video surveillance CCTV, access control, intrusion detection, etc.), ensuring advanced functionalities and performances.

The telecommunication system is composed by two strongly integrated sub-system: fixed infrastructure and mobile infrastructure. Both of them are illustrated in the following.

The mobile infrastructure is also capable of using satellite connections which ensures the same security levels of the central State to the personnel that follows the Pope during His Pastoral travels all over the world. In this way, the connection with the central system is always guaranteed, realizing a flexible and reconfigurable system that can easily and efficiently extend in different parts of the world at the same time.

The whole telecommunication system is controlled by a security room that checks not only the security of the Vatican City State but also the functionalities of any component of the integrated system, including the telecommunication system. Any malfunctioning is immediately signaled to the operator that can activate the related procedures to guarantee the maximum functionality of the system.

IV. DESIGN OF TELECOMMUNICATION SYSTEM

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

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

The heavier security component, from the generated data rate point of view, is represented by video cameras, that produce a not neglect able output bit/rate. In fact, to obtain a good quality of the video, it is necessary to use almost 25 frame per second, at full PAL video system resolution. A non-compressed coding standard generates about 2 Mbit/s while a highly compressed standard can reduce the flow to about 128 Kbit/s (depending on the variability rate of the scene).

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

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

Further it has been design to guarantee a high reliability and availability using a high redundancy. In particular, it is endowed by a total autonomous electrical supply system, to increase its reliability. The electrical reliability has been tested on the field during the electrical black-out which took place in Rome and all over Italy on September 2003: the telecommunication system continued to work until the electrical supplied was recovered different hours later.

The telecommunication system is checked continuously and automatically so that any malfunctioning 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 design to guarantee a high quality of service (QoS) and class of service (CoS).

The two telecommunication subsystems have been designed using advanced optimization techniques such as the one offered by Genetic Algorithms (GAs), as it is explained in the following.

V. THE FIXED TELECOMMUNICATION SYSTEM

The fixed telecommunication system is composed by an optical loop backbone based on ATM technology and by secondary branches based on different technologies (Ethernet, etc.).

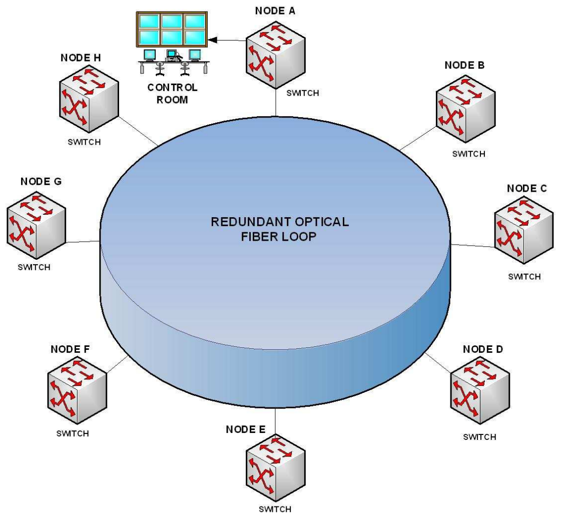

Figure 2. Scheme of the fixed telecommunication system where the add/drop nodes are visible.

The optical backbone is characterized by a high redundancy using two loops, so that an interruption of a part or of a whole loop is properly recovered, generating a new path, using the other loop. In this way the main loop is capable of guaranteeing a high reliability and availability. The two loops composing the high redundancy loop do not follow the same path, since any voluntary or not voluntary cut of one loop cable of the net does not interrupt the other cable of the net.

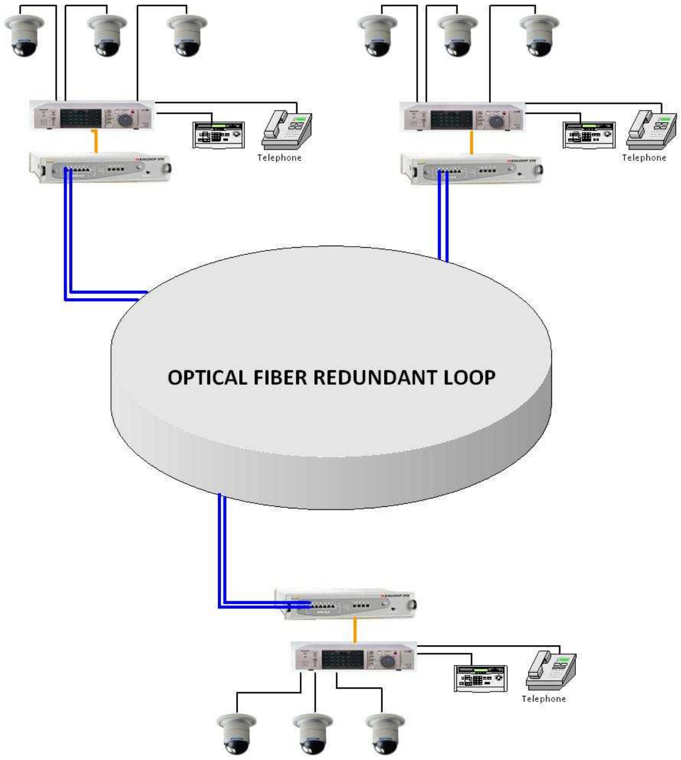

Figure 3. Scheme of the fixed telecommunication system where the add/drop multiplexers that serve video cameras, phone and other data flows are visible.

In a territory subjected to architectural restrictions such as the Vatican City State, it is very difficult to find not only proper paths where install the two optical fibers loops of the main backbone of the net but also find the minimum number of Add/Drop Mux and their fixed positions imposed by the mentioned restrictions to reach all the secondary nets.

In fact the Add/Drop Mux cannot be installed in every desired position and every secondary nets cannot be linked to the nearest Mux, due to the same restriction. This kind of problem, typical of prestigious artistic and architectural environment, has already be studied [4] and it has been applied, in a proper adapted version, even in the considered situation, guaranteeing excellent results.

VI. THE MOBILE COMMUNICATION SYSTEM

The mobile communication system 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 system.

Due to the variety of problem involved, a collective access radio system, based on TETRA standard, has been designed and realized which is capable of satisfying all the security communication needs of the State. 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.

In a collective access radio system the frequency are dynamically assigned to the users, according to the 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.

The used digital technology shows 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.

Every used radio link can be divided in 4 different channels, that are used singularly or together as a function of the necessary transmission band.

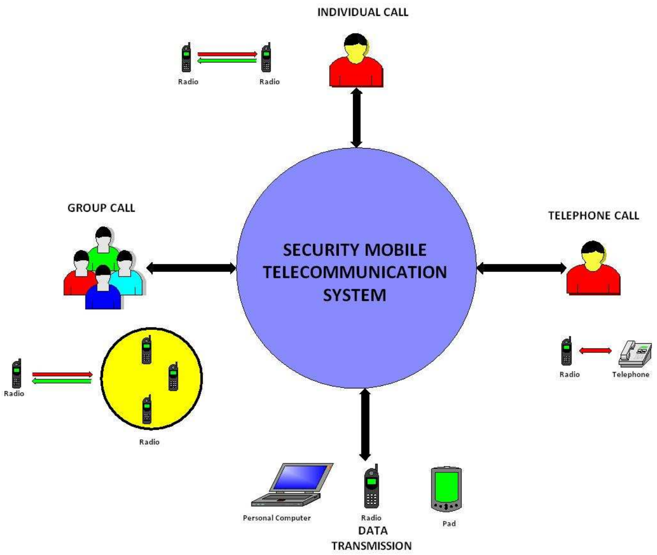

Figure 4. Mail functionalities of the mobile communication system.

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

The system allows a multi-level 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 which 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 used PDO technology also allows a full compatibility with TCP/IP protocol and all the related facilities.

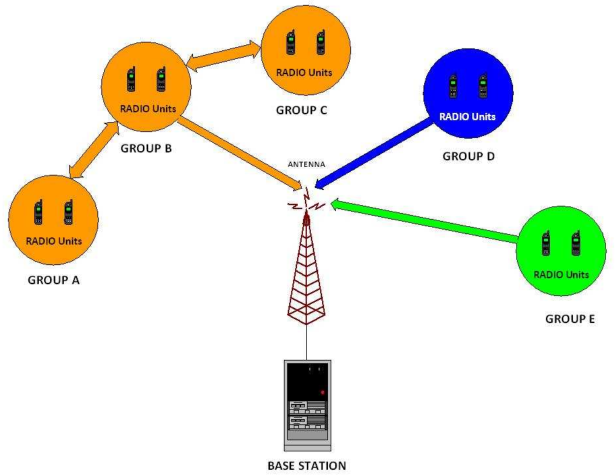

Figure 5. Scheme of mail vocal services.

The mobile system ensures the following functionalities:

1) full-duplex communications;

2) capabilities of defining user groups whom assign homogeneous communications services;

3) use of only one radio base temporal slot for the communication of user belonging to the same group;

4) simultaneous delivery of information to the users of the same group;

5) communication channel assignment in less than 500 ms;

6) direct communication between different radio units without using the main infrastructure;

7) dynamic management of the queued calls (absence of lost calls).

Further, the mobile system 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.

The mobile system 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 everybody. The group is defined in a flexible way, that is 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 of 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).

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

Every BS can support 4 radio channels per transmitted carrier and can operate simultaneously on different carriers. The emitted power per carrier is of about 25 W ERP.

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 directly on the mobile system, programming the database and the users profiles.

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 emitted powers varying between 1 W and 10 W, always ensuring the better communication quality between the radio units and the closer BS.

The positioning of base stations in a territory with urban and environmental restrictions, such as Vatican City State, is not so simple and immediate, since it is necessary to ensure an optimal radio coverage placing the BSs and the related antennas in fixed zones and the related emitted power cannot exceed a certain level to avoid of reaching human health limits. This optimization problem has been successfully solved using genetic algorithms [10], properly adapted to the considered problem.

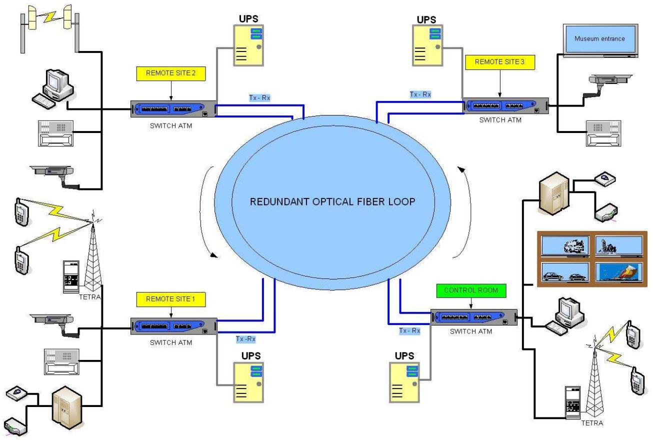

Figure 6. Scheme of complete network.

VII. THE SATELLITE COMMUNICATION SYSTEM

The mobile communication system has been designed to be capable of using satellite connections so that it is possible to ensure the telecommunication service all over the world, following the Pastoral travels of the Pope.

To ensure this kind of service it has been designed and realized a mobile unit, capable of guaranteeing the mobile communications inside its coverage area and of exchanging data with the central control room of the Vatican City State using satellite connections.

Different kind of satellite connections have been realized. In particular two specific connections, that have been tested for the first time in July 2002, are used. They use Eutelsat and Inmarsat satellite system.

The Eutelsat satellite connection operates in the Ku frequency band (11-14 GHz), working as a transponder, that is signals transmitted by a earth unit are received, amplified and transmitted by the satellite towards the other earth unit and vice versa.

The remote mobile unit transmits directly towards the satellite that transponds the signal towards the receiver located in the Vatican City State which is connected to the central mobile communication unit by means of a X21 modem.

The difficulties of the connection is represented by the need of ensuring a reduced communication delay to avoid that the security protocol of the mobile communications unit could interrupt the communication since it doesn't respect the security standards.

The Inmarsat (International Maritime Satellite Organization) is the owner of a satellite communication system that operates in 84 countries all over the world. It's infrastructure is composed by 8 satellites located in a geostationary orbit capable of covering any area of the world, with the exception of poles.

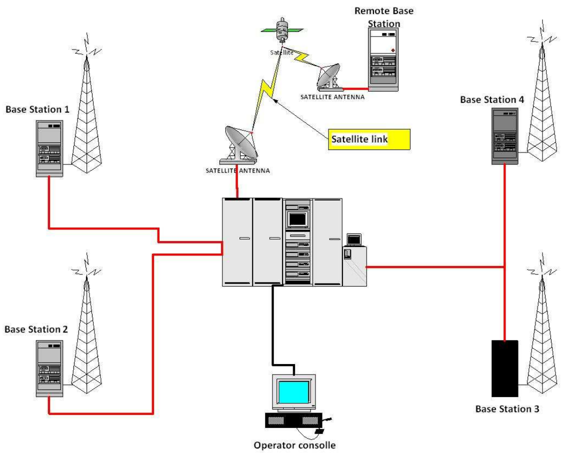

Figure 7. Scheme of the satellite connection.

The Inmarsat system allows of realizing voice or data call using proper terminals that can be terrestrial, maritime or mobile. All the terminals are equipped with special parabolic antennas characterized by different sizes.

The connection between the remote mobile unit and the Inmarsat unit and between the Inmarsat unit and the control room of Vatican City State is realized using an ISDN modem: in this way the satellite connection transfer all the information (voice and data), handling them as an ISDN telephone call.

Even in this case the communication channel has been optimize to reduce as more as possible the delay and the noise to avoid rejection of the communication due to security protocols of the system.

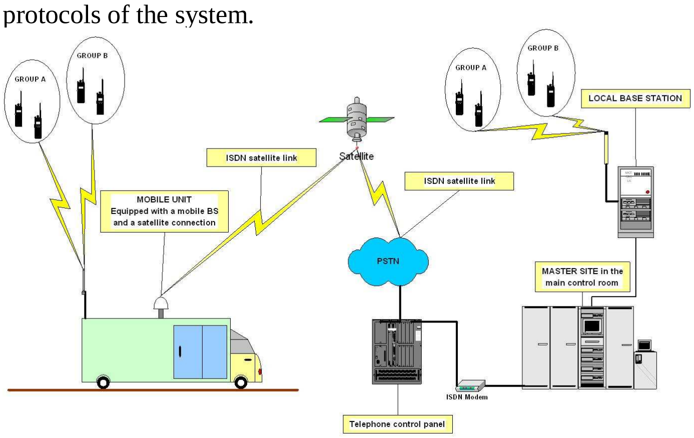

Figure 8. Scheme of the satellite connection including the mobile unit.

VIII. FURTHER DEVELOPMENT OF THE MOBILE COMMUNICATION SYSTEM

The mobile communication system has furtherly been improved using a new digital technology named Digital Mobile Radio (DMR) that is standardized by European Telecommunications Stantards Institute (ETSI).

The DMR is based on the Time Domain Multiplexing Access (TDMA) as TETRA technology but it uses only two temporal slots instead of four.

In fact, instead of using four temporal slots whose bandwidth is of 25 kHz, it uses only two temporal slots whose bandwidth is of 12.6 kHz.

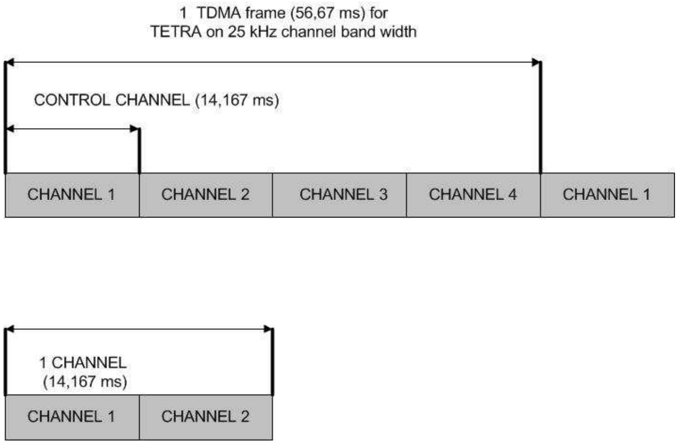
1 TDMA frame (56,67 ms) for
TETRA on 25 kHz channel band width
CONTROL CHANNEL (14,167 ms)
CHANNEL 1
CHANNEL 2
CHANNEL 3
CHANNEL 4
CHANNEL 1
1 CHANNEL
(14,167 ms)
CHANNEL 1
CHANNEL 2

Figure 9. Comparison between TETRA and DMR slot standards.

The DMR allows to create a simulcast network on the desidered territory using the first channel for the general communications over all the base stations and the second channel for the communication related to a specific territory covered by the single base stations.

The security of communications of DMR is properly ensured by native chryptographic algorithms for vocal and data services.

The DMR uses a master site and secondary slave sites.

The different sites are connected by means of TCP/IP protocol using optical fibers or broadband wireless connections that are capable of reaching distances up to 40 km.

Thanks to the use of TCP/IP protocol it is possible to create VPN connections through internet to connect remote sites. This last solution is generally used during the Pope’s holiday period on the mountains of north of Italy to keep a constant contact with the telecommunication system located in Vatican City State in Rome, about 600 km far away.

The DMR system, as TETRA system, is capable of supporting data services, so that it is possible to send on the mobile terminals all the information related to the security and to the operative alarms.

The mobile terminals are equipped with a GPS recevier so that it is possible to know exactly the position of security personnel to manage properly dangerous and emergency situations.

The DMR communication system is used to ensure greater reliability and redundancy to the TETRA communication system.

The introduction of DMR technology has greatly improved the security level of communications of the Vatican City State.

IX. CONCLUSION

The security management in complex contests such as the Vatican State needs a detailed risk analysis of menaces and dangers that must be faced and a correct study, design and realization of an efficient telecommunication system that is capable of integrating the different security systems, ensuring the maximum reciprocal integration of the different sub-systems involved.

In this way it has been possible to realize a powerful and versatile telecommunication system that guarantees a high level of security services of the State.

REFERENCES

[1] E. Waltz, “Information Warfare – Principles and operations”, Artech House Publisher, Boston (USA), 1998.

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

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

[4] F. Garzia, “The integrated safety/security system of the Accademia Nazionale dei Lincei at Corsini Palace in Rome”, Integrating Historic Preservation with Security, Fire Protection, Life Safety and Building Management Systems, Rome (Italy), pp.77-99, 2003.

[5] F. Garzia, and G. M. Veca, “Integrated security systems for hazard prevention, management and control in the Italian high speed train line”, Risk Analysis III, WIT Press, Southampton (UK), pp.287-293, 2002.

[6] E. Antonucci, F. Garzia, and G. M. Veca, “The automatic vehicles access control system of the historical centre of Rome”, Sustainable City II, WIT Press, Southampton (UK), pp.853-861, 2002.

[7] F.Garzia, “The integrated supervision and control system of the Gran Sasso mountain”, Safety & Security Engineering, WIT Press, Southampton (Boston), pp.699-711, 2005

[8] F. Garzia, E. Sammarco, and R. Cusani, “Integrated access control system for ports”, Safety & Security Engineering III, WIT Press, Southampton (UK), pp.313-323, 2009.

[9] G. Contardi, F.Garzia, R.Cusani, “The integrated security system of the Senate of the Italian Republic”, Proc. of IEEE International Carnahan Conference on Security Technologies, Zurigo, pp.111-118, 2009.

[10] F.Garzia, C. Perna, R. Cusani, "Optimization of UMTS network planning using genetic algorithms", (in print), Int. J. Communication, Network and System Sciences, 2010