THE INTEGRATED SECURITY SYSTEM OF THE VATICAN CITY STATE

F. GARZIA[1], E. SAMMARCO[2] & R. CUSANI[1]
[1]INFOCOM Department, SAPIENZA – University of Rome, Italy.
[2]General Direction of Safety, Security and Civil Protection, Vatican City State.

ABSTRACT
The security of a modern state is strongly dependent on the use of integrated technology systems. Any weakness of the integrated 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 security systems. The authors illustrate the work made to design and realize the integrated security system of the Vatican City State.
Keywords: integrated system, security system, telecommunication system.

1 INTRODUCTION

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

Even if the extension of the State is quite reduced, the Vatican State is characterized by the same security 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 an integrated security system, that is, able of guaranteeing a high level of efficiency of the security services of the State (Fig. 1).

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

Due to secrecy reasons, the integrated security system is described according to the general philosophy design, without describing specific details that could compromise the security of the system itself.

2 ROLES OF INFORMATION AND TELECOMMUNICATION SYSTEM IN SECURITY

Information plays a crucial role 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 analyzed 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 behavior of those objects. Knowledge includes both static content and dynamic processes. Sometimes it is also called intelligence.

ISSN: 2041-9031 (paper format), ISSN: 2041-904X (online), http://journals.witpress.com
DOI: 10.2495/SAFE-V1-N1-1-17

Figure 1: View of St. Peter Basilica and square, Bernini colonnade and part of Vatican City State.

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 integrated security system plays a crucial role in the transmission and management of information: the more it is powerful and well designed and the more the security system (intended as integration of technologies, procedures, and surveillance personnel) is efficient.

3 THE INTEGRATED SECURITY SYSTEM

In complex contest, such as the Vatican City State, it is necessary to design and realize a strongly integrated security system that ensures a high interaction between the different subsystems that compose it. In this way, the different subsystems are capable of interacting reciprocally in an efficient and coordinate way, showing, at the same time, a high degree of usability, to let the security personnel to receive, in real time, the different information necessary to manage not only security but also emergency situations.

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

The system is properly divided into subsystems that are described in Section 4.

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.

In this way, a system has been designed whose functionalities are really superior with respect to the functionalities of single subsystems.

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 described in Section 5.

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

The system is controlled by a proper main security room and some secondary security rooms that allow the total control of the system in case of malfunctioning or damaging of the main control room.

The realized integrated system has been designed considering also the psychological and ergonomic aspects of the operators of the control rooms, to avoid information overcharges that would induce stress and reduction of attention level, decreasing their performances.

For this reason, the information flow is processed and reduced in ordinary conditions and properly increased in emergency situations, when the operators of the control rooms and the other personnel must face and manage events directly that could become dangerous for people or goods.

The operators and the personnel are properly and continuously trained to make them able of analyzing and studying the dangerous events, to face them through proper functional and efficient procedures allowed by the high degree of integration of the system.

3.1 Design criteria of the system

To design the integrated system, it has been necessary to do a proper analysis of the risks that could menace the security of the State in normal and critical conditions.

Critical conditions verify generally during the great events, when hundreds of thousands of people go into St. Peter square in the presence of the Pope.

It must not be forgotten that, normally, some parts of Vatican City State such as St. Peter Basilica and Vatican Museums are visited by millions of people every year, posing severe requisites to the system by the safety and security point of view.

Once individuated the possible risks and the related countermeasures and procedures to manage and control them, it has been possible to design the whole system.

The system was designed according to high reliability standards, since it must work in any severe and critical condition even in the case of lost or damaging of part of it.

The system is therefore divided into autonomous subsystems for reliability reasons since in case of malfunctioning of any subsystem, or of parts of it, the other subsystems can continue to operate, ensuring their functionalities.

Any subsystem is characterized by a high reliability, being supplied from different electrical sources, properly backed-up, that allow them to operate even in the absence of the main electrical supply for a long time.

Any subsystem is also divided into subcomponents totally autonomous from the operative point of view, to increase the reliability of the subsystems themselves.

Any component of the system is constantly and automatically checked and monitored from the functionality point of view, so that any malfunctioning is immediately revealed; in this case, the necessary alarm signaling is sent to the maintenance personnel for a prompt repairing.

The system can anyway operate, even with reduced performances, with one or more than one damaged components, due to the severe operative conditions imposed by the security needs of the Vatican State.

The main subsystems are:

1. the telecommunication subsystem;
2. the video surveillance subsystem;
3. the access control subsystem;
4. the anti-intrusion subsystem.

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

The system is controlled by a main control room and by secondary control rooms.

The system is also endowed by disaster recovery capabilities, that is, the capabilities of transferring the partial or total control of the whole security system to secondary control rooms in case of malfunctioning or damaging of the main control room. In this way, the full control of the whole system is always ensured.

Once individuated the number of components and devices to be installed on the field, it has been possible to design the functional architecture of the subsystems and to calculate the generated data flows that must be transmitted inside and outside the system. This allows to design the telecommunication system that represents the backbone of the whole security system.

A scheme of the integrated system is shown in Fig. 2.

4 THE TELECOMMUNICATION SUBSYSTEM

The telecommunication subsystem is used not only for voice but also for security data communication [3–9].

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

In the following, only a synthesis of the main features of the telecommunication subsystem is described.

The telecommunication subsystem is composed of two strongly integrated subsystems: fixed infrastructure and mobile infrastructure. Both of them are described in Section 6.

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 subsystem is controlled by the security rooms that check not only the security of the Vatican City State but also 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.

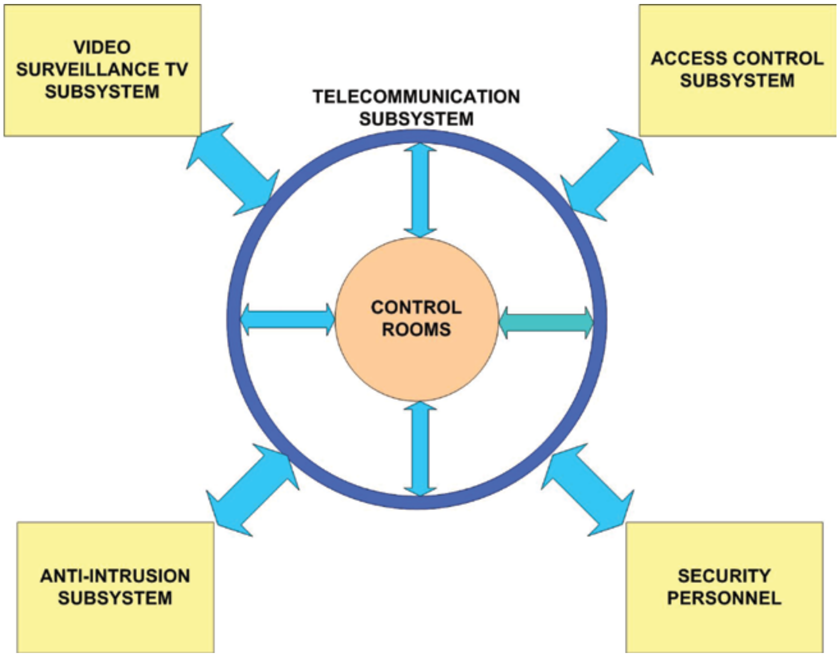

Figure 2: Scheme of integrated security system.

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

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

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 system has been designed according to the peculiar data flows that must be carried following the criteria described in the next paragraphs.

The telecommunication subsystem is totally separated from the other telecommunication systems of the State, 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 endowed with a total autonomous electrical supply system.

The telecommunication subsystem is continuously and automatically checked 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 designed to guarantee a high quality of service (QoS) and class of service (CoS).

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

The main data flow moves on the optical loop backbone where it is diverted towards the desired point, exiting or entering through proper Add/Drop Multiplexer (Add/Drop Mux) nodes that spill in or out the traffic from the main high velocity loop towards the secondary reduced velocity net.

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.

A scheme of the fixed telecommunication subsystem is shown in Fig. 3, where it is possible to see the redundant optical fiber loop and the different ATM switch nodes to insert/extract information flows from the main loop.

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.

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 State. The mobile system is composed of 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 is 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.

The used digital technology is characterized by a series of advantages indicated in Table 1.

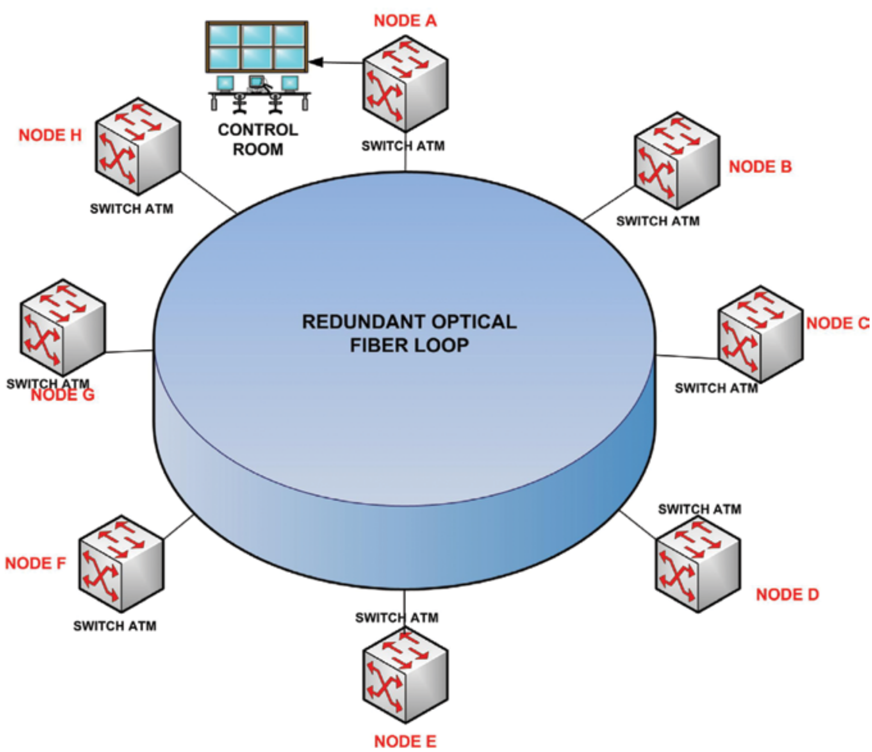

Figure 3: Scheme of the fixed telecommunication system.

Table 1: Advantages of the used digital technology.

Better quality of vocal messages
Higher transmission and reception velocity
Lower dependence from signal reception level
Higher security of conversation thanks to the used cryptographic algorithm
Capabilities of using the mobile units not only as phones but also as data terminals to transmit and receive any kind of information

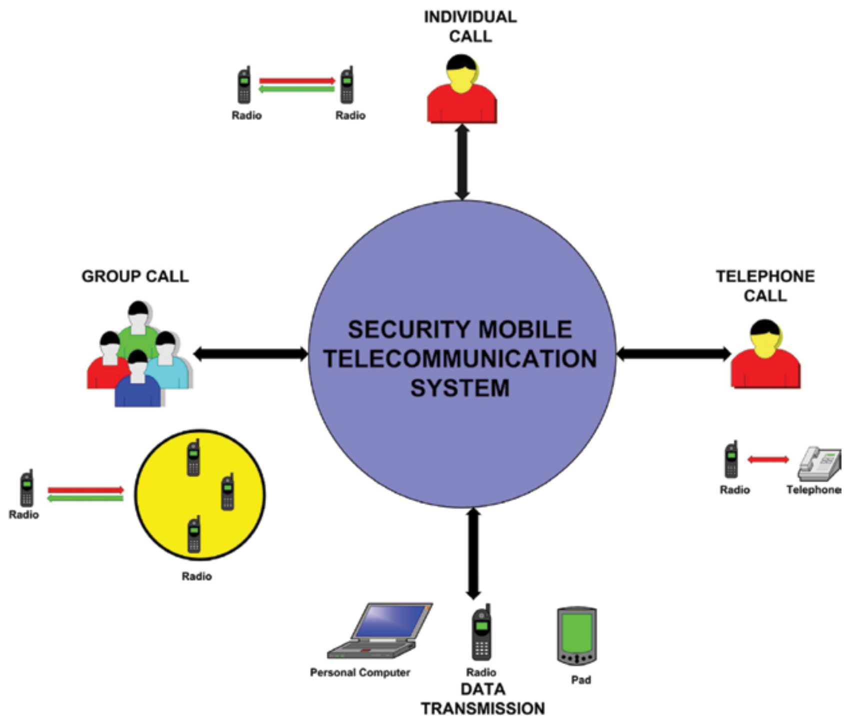

Figure 4: Main functionalities of the mobile communication system.

A scheme of the main functionalities of the mobile communication subsystem is shown in Fig. 4.

Every used radio link can be divided into 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 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 time division multiplexing access (TDMA) transmission technology, whereas the data traffic is based on a packet data optimized (PDO) transmission technology. The used PDO technology also allows a full compatibility with TCP/IP protocol and all the related facilities.

The functionalities of the mobile subsystem are indicated in Table 2.

Further, the mobile subsystem is characterized by a high security level according to the functionalities indicated in Table 3.

The mobile subsystem offers the vocal services indicated in Table 4.

The mobile system also offers the data services indicated in Table 5.

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

Table 2: Functionalities of the mobile subsystem.

Full-duplex communications
Capabilities of defining user groups whom assign homogeneous communications services
Use of only one radio base temporal slot for the communication of user belonging to the same group
Simultaneous delivery of information to the users of the same group
Communication channel assignment in <500 ms
Direct communication between different radio units without using the main infrastructure
Dynamic management of the queued calls (absence of lost calls)

Table 3: Security functionalities of the mobile communication subsystem.

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

Table 4: Vocal services offered by the mobile communication subsystem.

Name of service	Description
Individual call	This service is equivalent to the communication through a cellular phone (i.e. a user calls another user)
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
Direct call	Two or more radio units communicate directly without the support of the base station
Broadcast call	It is a unidirectional point–multipoint call in a certain zone. The zone and the users can be dynamically defined
Emergency call	It allows to make a high priority call pressing an emergency button on the radio unit
Include call	It allows of calling or inserting in a call one or more supplementary users
Open channel	A group of users can talk on a certain radio channel and all the users can listen and talk at any time

Table 5: Data services offered by the mobile communication subsystem.

Name of service	Description
Status transmission	Allows to broadcast short and predefined messages from the dispatcher to the radio units and vice versa
Short data service	Allows to send predefined messages to single users or group of users
Data transmission CCM	Data transmission using a circuit commutation mode
Data transmission PCM	Data transmission using a packet commutation mode (X25, TCP/IP)

Every BS can support four 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 and 10 W, always ensuring the better communication quality between the radio units and the nearest BS.

A complete scheme of the telecommunication subsystem (fixed and mobile) is shown in Fig. 5.

The telecommunication subsystem has been designed to be capable of using satellite connections so that it is possible to ensure the telecommunication services 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 control rooms of the Vatican City State using satellite connections. Different kinds of satellite connections can be made.

The difficulties of the satellite 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 does not respect the security standards.

A scheme of the satellite connection is shown in Fig. 6.

5 THE VIDEO SURVEILLANCE SUBSYSTEM

The video surveillance TV subsystem is designed to allow the security operators to verify and control in real time any events, managing them immediately, through the telecommunication system, together with the security personnel.

The system is also designed to allow the security operators to study, verify, analyze and understand, in a second time, any critical event, to reconstruct the initial phase. This is allowed only when it is possible to use high quality images. Due to the elevate numbers of critical zones that must be accurately checked, an elevate number of cameras have been installed all over the State and in the detached territories.

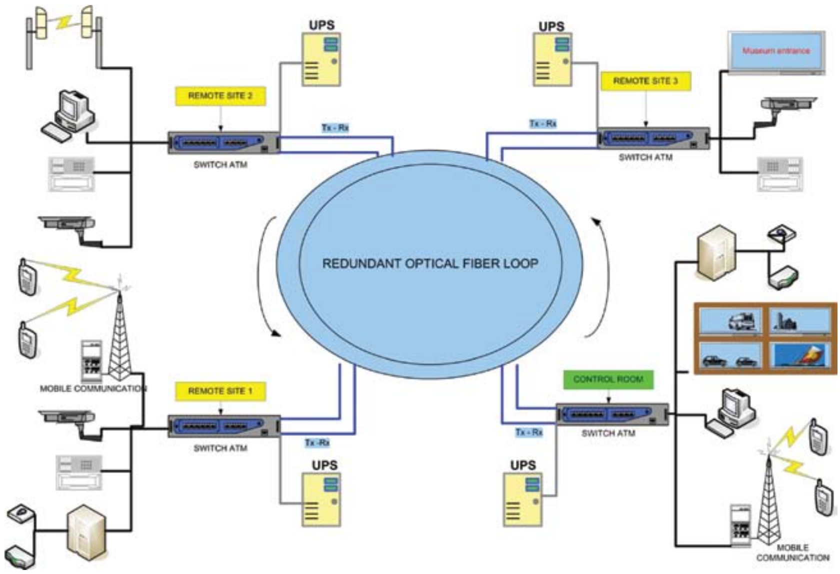

Figure 5: Scheme of telecommunication subsystem.

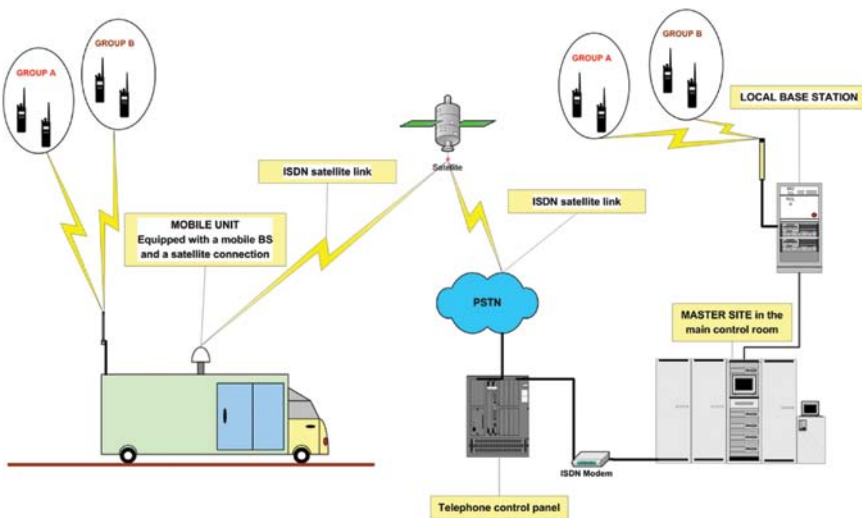

Figure 6: Scheme of the satellite connection.

For this reason, it has been necessary to study and design solutions characterized by an elevate technological profile, aimed at ensuring a high quality of images and a high flexibility in video signal managing and recording.

A scheme of the video surveillance subsystem is shown in Fig. 7.

All the cameras, both fixed and dome, are characterized by professional standard quality to promptly respond to the security needs of the State.

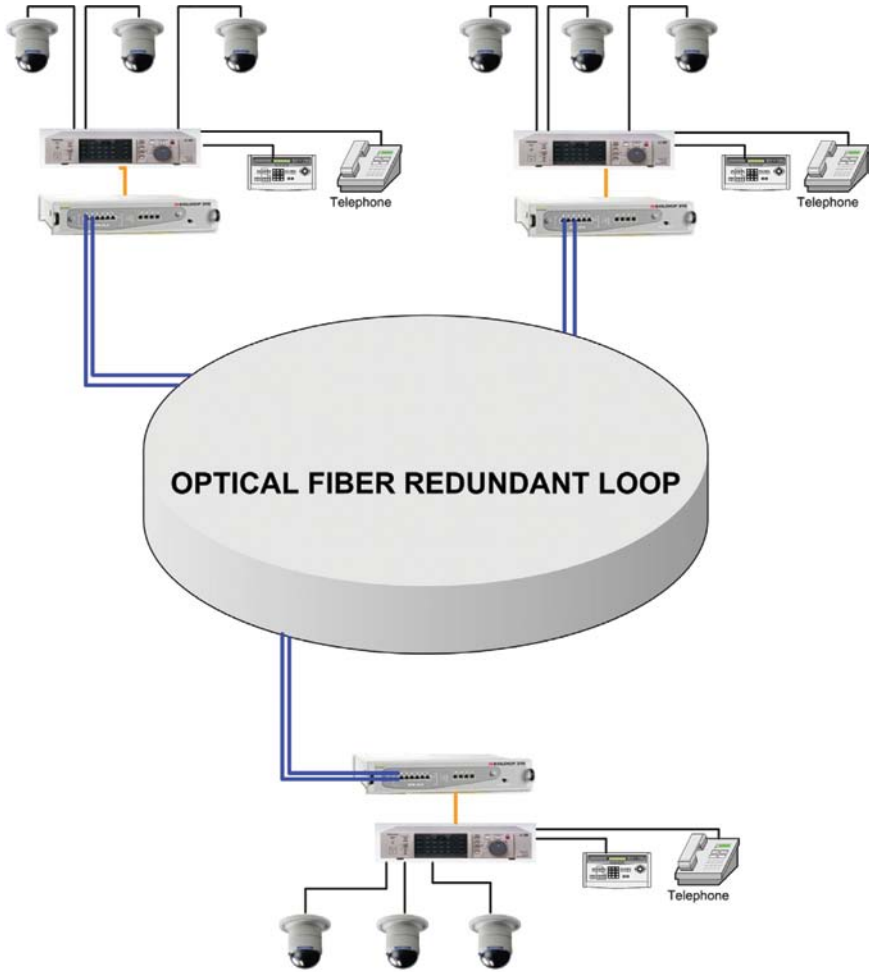

Figure 7: Scheme of the video surveillance subsystem.

The images produced by the cameras and the telemetry data necessary to move the dome cameras in the pan-tilt-zoom movements are transmitted by means of the telecommunication subsystem.

The high quality images converge towards the control rooms where they are properly stored in high quality digital recorder to be eventually seen later. Video images are stored into memory for a long time to avoid of losing important elements necessary to reconstruct eventual critical events.

Thanks to the high quality of the images it is possible to analyze them by means of proper image analysis tools such as motion detector and so on. In this way, even if the operators loose significant details of the scenes, the system is always capable of signaling it using its powerful automatic capabilities.

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 as more as possible the complexity, making them extremely user-friendly. In this way, the stress of the operators is reduced, letting them able to face any critical events with the necessary concentration.

6 THE ACCESS CONTROL SUBSYSTEM

The access control subsystem is divided into internal subsystem and external subsystem.

In the following, only the external subsystem is considered.

The entrances of the Vatican City State are located in different points of the external perimeter.

They are generally protected by two controls:

1. The first control made by the Swiss Guards (Fig. 8).
2. The second control made by the security personnel of the Gendarmerie.

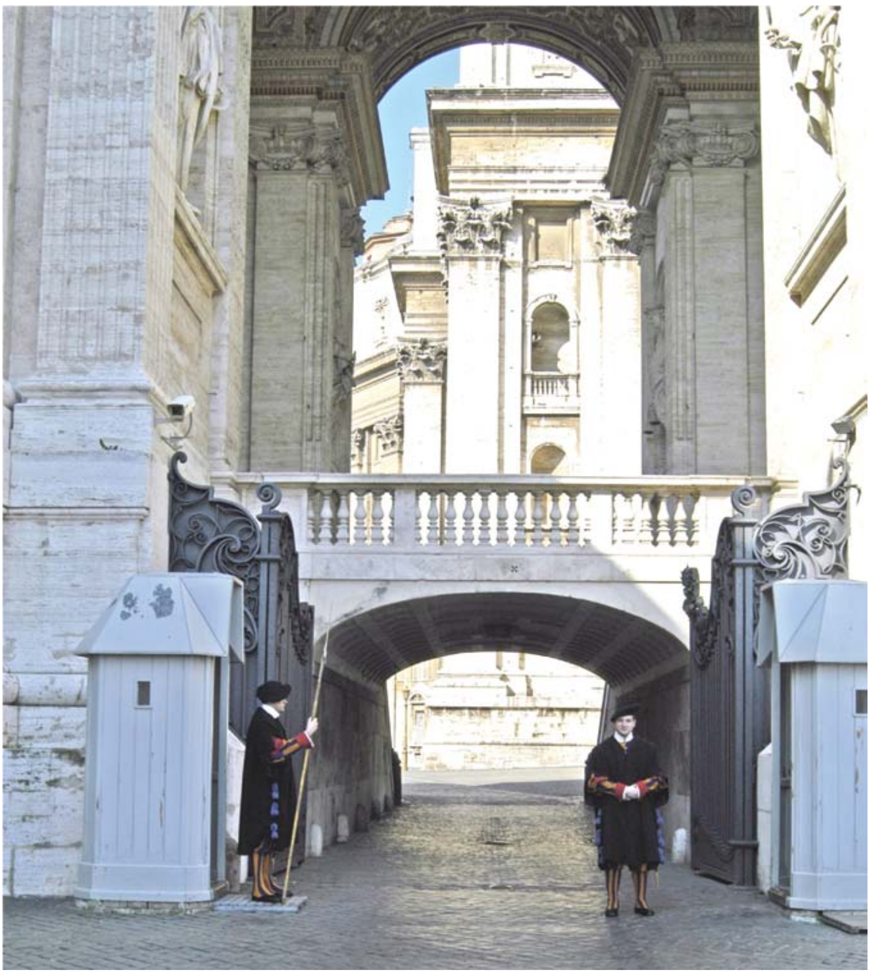

Figure 8: An entrance of Vatican City State controlled by Swiss Guards.

These kinds of controls are extended in different internal zones, to increase the sectoring and the security level.

Through these entrances all the vehicle traffic and the most of people flow.

Due to the elevated number of vehicles and people entering each day, it is quite difficult to control and identify each enabled subject using only human control or anyway it is quite difficult to make it in real time due to the consistent volume of traffic.

For this reason, three systems, that work synergistically, have been designed and realized:

1. car license plate recognition;
2. face recognition;
3. card reader.

Once a vehicle approaches an entrance, the system, through the video surveillance system, acquires the license plate and immediately checks if it is enabled to enter. Anyway the vehicle is visually controlled by the Swiss Guards before and by the security personnel of the Gendarmerie after. If the vehicle is not enabled, an immediate signaling is sent to the control personnel.

In the same way, each face of entering people is checked by the face recognition module of the access control subsystem and the identity is verified through the card reader.

The strong interaction of the mentioned access control modules, together with the other subsystems, ensures an easy and efficient management of access to the State and inside the different internal zones of the State.

6.1 The card-based access control system

The internal access control subsystem uses not only face recognition and license plate recognition but also card readers.

The card reader technology allows:

1. high entrance velocity ensuring maximum privacy and minimum environmental impact;
2. high expandability of the system since it allows multiple services such as entrance control, personnel control, services applications, etc.

The used card is based on multiple technologies, and it is described in Section 7.

The architecture is based on central server and regional servers.

The central server communicates constantly, through the telecommunications subsystem, with the regional servers to keep updated the local databases. The regional servers are totally autonomous from the functional point of view since they are capable of operating without the central server. In this way, in case of lost of telecommunication subsystem, they continue to operate, updating in a second time the database of the central server.

The central server is properly redundant to ensure the maximum reliability of central database.

The technologies implemented on the card are:

1. magnetic strip;
2. microchip;
3. radio frequency identification (RFID).

Magnetic strip allows to store and read a reduced series of data. The magnetic strip is applied on the back of the card according to ISO recommendations. An important feature is the coercivity, that is, the capability of keeping the stored data unaltered under the effect of an external magnetic field. The magnetic strip can be:

1. low coercivity (LoCo, generally 300 oersted);
2. high coercivity (HiCo, generally 4,000 oersted).

Low coercivity strip is recognizable from brown color and it is generally used for banking applications. High coercivity strip is recognizable from black color and it is generally used for access control applications, such as the considered one. The magnetic strip is divided into three different tracks, characterized by different storing capabilities:

1. ISO 1 track (high zone): 79 alphanumeric characters – 210 bpi code density;
2. ISO 2 track (medium zone): 40 alphanumeric characters – 75 bpi code density;
3. ISO 3 track (low zone): 107 alphanumeric characters – 210 bpi code density.

Data recording depend on the used technology and complies with international standard such as ISO/IEC 7811-2/6.

The used card is a high coercivity one, characterized by a high quality and a laminated magnetic strip (not glued). All the three tracks are used as a function of the requested application.

The used card is also equipped with an electronic microchip. The microchip contains a microprocessor and a digital rewritable memory ensuring not only storing capabilities but also computation capabilities to execute particular program or ciphering applications. The microprocessor can execute Java applications, that is, a worldwide programming language used in a plenty of devices.

The used card is also equipped with RFID system that allows it to work contact less and within a certain distance from the reader. The working principle is as follows: the reader sends an electromagnetic pulse to the RFID or TAG (composed of the reader/writer system and the antenna) that sends back an electromagnetic pulse to the reader, containing the requested information. The TAG can be characterized from different shapes and can be inserted into glass, resin, label or card. It is composed of an antenna and an electronic chip and it can be:

1. passive;
2. battery assisted;
3. active.

The passive TAG uses the energy of the received electromagnetic wave emitted by the reader. In this way, the TAG is usable only if it is exposed to the reader using the so-called back scattered technique that consists in inserting the information in the back scattered electromagnetic wave.

The battery assisted is similar to the passive TAG with the difference that a battery is used to give energy to the microprocessor. In this case, since no energy is taken form the incoming electromagnetic wave, it is possible to reach a longer distance with respect to the reader.

The active TAG is characterized by using a battery to work as an autonomous transmitter allowing in reaching longer distance with respect to the previous ones. In this case, the cost of the card is quite higher and the battery is subjected obviously to discharge after use.

The electronic chip includes a microchip and a memory. The TAG communicates with the reader by means of radio interface that complies with ISO 18000 recommendations.

The radio interface is capable of managing a proper anti-collision protocol which allows different TAGs to communicate at the same time. It can implement different actions such as:

1. ask the identification of the whole TAGs obtaining a collective answer;
2. ask the identification of the TAGs characterized by a specific initial character obtaining a restricted number of answers.

The system can operate in two different modalities:

1. Reader Talks First (RTF);
2. Tag Talks First (TTF).

In the RTF modality, the TAG waits for reader querying. This means that even if the TAG receives electromagnetic power from reader, its does not transmit until it receives a specific request from the reader itself.

In the TTF modality, as soon as the TAG receives enough power from the reader, it starts to transmit. This allows a faster communication but keep the radio channel occupied.

RFID can operate at different frequencies that are:

1. 125–134 kHz;
2. 13.56 MHz;
3. 400 MHz;
4. 860–930 MHz;
5. 2.45 GHz;
6. 5.8 GHz.

Lower frequencies work better in the presence of water contained inside the body of entering people, even if they are characterized by a reduced operative range and by a reduced data bit rate.

A scheme of a double antenna RFID card is shown in Fig. 9.

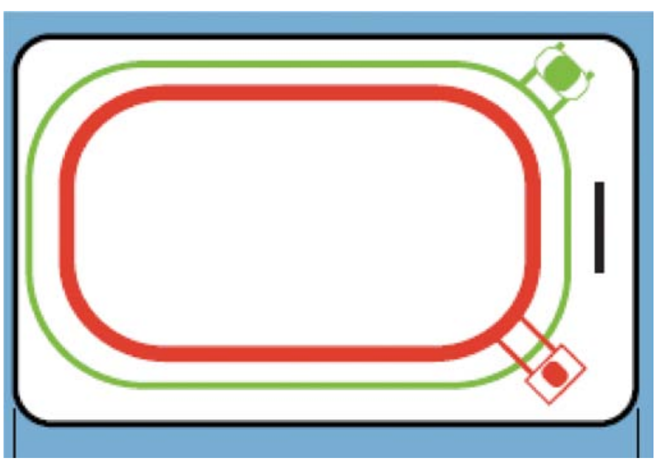

Figure 9: Scheme of a double antenna RFID card.

6.2 The considered solution

The implementation of the access solution needed to respect the used entrance criteria, optimizing them.

It has been fundamental to use a unique card, properly developed both from the graphical and from the technological point of view.

This new card gradually substituted the different cards existing in the Vatican City State to simplify the entrance control of both Gendarmeries and Swiss Guards.

For this reason:

1. a central office has been created for personal data acquisition and for cards creation;
2. an indexed database has been created for data management;
3. a unique information visualization graphic interface has been created;
4. Passes Office has been automatized;
5. entrances have been automatized;
6. readers for active badge inside vehicles have been installed;
7. new readers have been installed to increase the level of internal control.

7 THE ANTI-INTRUSION SUBSYSTEM

The critical perimeter of the State and the interiors are protected by the anti-intrusion subsystem that is strictly integrated with the video surveillance TV system.

In case of alarm, the signaling is immediately transmitted to the video surveillance subsystem that alerts the operators to watch the interested zone by means of the nearest camera.

The video surveillance subsystem is also used, in some zones, as anti-intrusion subsystem by means of its advanced digital motion detection capabilities. In this case, the zones that must be controlled are shown on a monitor and proper bordered using a mouse: when a movement takes place in the bordered zones, an alarm signaling is immediately activated.

This subsystem is vital not only for normal perimeter but also for public interface perimeter, such as inside St. Peter Basilica and Vatican Museums.

8 CONCLUSIONS

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 subsystems, 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 State.

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 Accademia Nazionale dei Lincei at Corsini Palace in Rome, *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 City State. *Risk Analysis IV*, WIT Press: Southampton, UK, pp. 773–782, 2004.
[8] Garzia, F. & Sammarco, E., The integrated security system of the Vatican City State. *SAFE 2005*, WIT Press: Southampton, UK, pp. 391–403, 2005.
[9] Garzia, F., Sammarco, E. & Cusani, R., The access control system of the Vatican City State. *SAFE 2007*, WIT Press: Southampton, UK, pp. 431–440, 2007.