THE INTEGRATED SECURITY SYSTEM OF THE VATICAN CITY STATE

Fabio Garzia¹, Enzo Sammarco²

¹INFOCOM Department
Università degli Studi di Roma “La Sapienza”
fabio.garzia@uniroma1.it
w3.uniroma1.it/sicurezza

²General Direction of Safety, Security and Civil Protection
Vatican City State
The Vatican City State extends over a surface of about 44 hectares in the heart of Rome. 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.

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 an integrated security system that is able of guaranteeing a high level of efficiency in ensuring the security services of the State.
Information plays a crucial role in security, since it is vital in the typical offence, defence and dominance phase of any conflict.

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

**DATA**
- Observations, measurement, and primitive messages

**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.

**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 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.
SECURITY MANAGEMENT SYSTEM – SECURITY TRIANGLE

- Procedures and human resources
- Physical security
- Technological security
- 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.

- 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 in subcomponents totally autonomous from the operative point of view, to increase the reliability of the subsystems themselves.
Any components 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 signalling 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 TV 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.
THE INTEGRATED SYSTEM - SCHEME

VIDEO SURVEILLANCE TV SUBSYSTEM

ACCESS CONTROL SUBSYSTEM

TELECOMMUNICATION SUBSYSTEM

ANTI-INTRUSION SUBSYSTEM

SECURITY PERSONNEL
- The telecommunication subsystem is composed by two strongly integrated sub-systems: 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.

- 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 signalled 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 TELECOMMUNICATION SUBSYSTEM

TELECOMMUNICATION SUBSYSTEM

FIXED INFRASTRUCTURE

MOBILE INFRASTRUCTURE
- The main data flow of the integrated system are 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 illustrated in the following.

- 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 signalled 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).
FIXED TELECOMMUNICATION INFRASTRUCTURE

REDUNDANT OPTICAL FIBER LOOP

NODE A
SWITCH ATM

NODE B
SWITCH ATM

NODE C
SWITCH ATM

NODE D
SWITCH ATM

NODE E
SWITCH ATM

NODE F
SWITCH ATM

NODE G
SWITCH ATM

NODE H
SWITCH ATM

CONTROL ROOM
STRUCTURE OF THE NODES OF FIXED TELECOMMUNICATION INFRASTRUCTURE

REDUNDANT OPTICAL FIBER LOOP

REMOTE SITE 1

REMOTE SITE 2

REMOTE SITE 3

Museum entrance

CONTROL ROOM

SWITCH ATM

UPS

UPS

UPS

SWITCH ATM

SWITCH ATM

TETRA

TETRA

TETRA
- 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.

- The mobile system checks continuously the coding/decoding quality of the voice, allowing an optimal communication service even in the presence of disturbs.
- The mobile subsystem 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 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.
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 radio communication system offers also data services.
- 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 be aided by 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.

- 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.

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

- 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 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 tool such as motion detector and so on. In this way even if the operators lose significant details of the scenes, the system is always capable of signalling 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.
The access control subsystem is divided into internal subsystem and external subsystem. Since the internal subsystem is considered classified, it is not illustrated here. 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;
  2) the second control, made by the security personnel of the Gendarmerie.

- These kind of control is 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 two systems have been designed and realized:
  1) car licence plate recognition;
  2) face recognition;
that work synergistically.

- Once a vehicle approaches an entrance, the system, through the video surveillance system, acquires the licence plate and immediately check 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 signalling 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.

- 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.
The security management in complex contests such as the Vatican State needs a detailed risk analysis of menaces and dangers that must be faced.

It is also necessary 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.