The access control system of the Vatican City State

F. Garzia[1], E. Sammarco[2] & R. Cusani[1]
[1]*INFOCOM Department, University of Rome "La Sapienza", 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 access control technology systems. Any weakness of the integrated access control 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 access control systems. The authors illustrate the work made to design and realize the integrated access control system of the Vatican City State.
Keywords: access control system, integrated security system, sec system.

1 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 near 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 needs of any other State that are further amplified by the reduced dimensions of the State.

For this reason an integrated security system that is able of guaranteeing a high level of efficiency of the security services of the State has been designed and realized.

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

WIT Transactions on The Built Environment, Vol 94, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE070431

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

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

2 Roles of information systems 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 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 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, is it 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, such as access control, 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 illustrated in the following.

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 it has been designed a system 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 the following.

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 directly events 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 thousand of people go into S. Peter Square in the presence of the Pope.
It must not be forget that normally some parts of Vatican City State such as S. Peter Basilica and Vatican Museums are visited by million of people each 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 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 one to design the telecommunication system that represents the backbone of the whole security system.

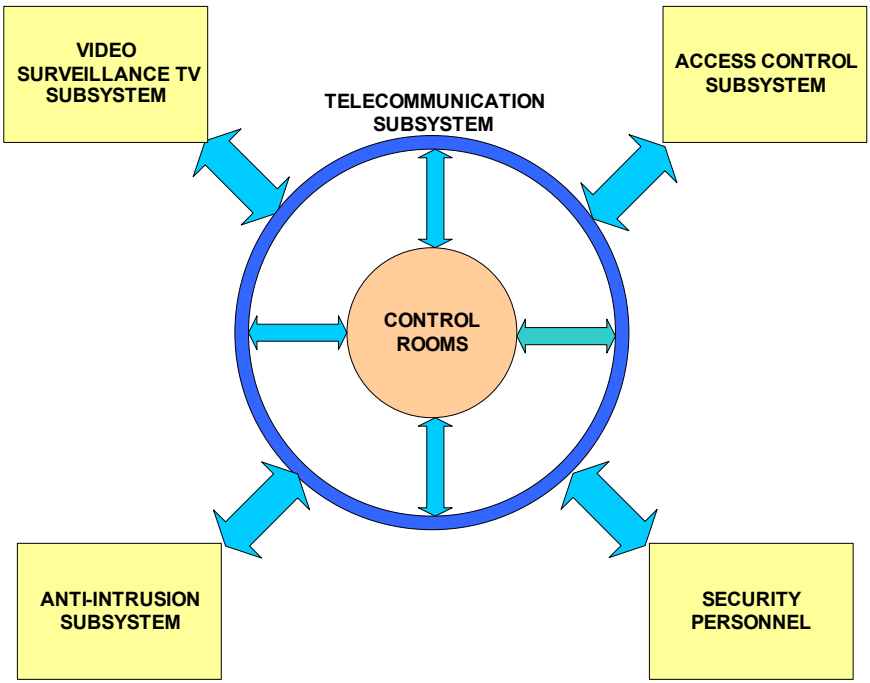

Figure 2: Scheme of integrated security system.

4 The access control system

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;

2) the second control, made by the security personnel of the Gendarmerie.

This 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.

Figure 3: An entrance of Vatican City State controlled by Swiss Guards.

For this reason three systems have been designed and realized:
1) car licence plate recognition;
2) face recognition;
3) card reader (that is illustrated in the following).
that work synergistically.

Once a vehicle approaches an entrance, the system, through the video surveillance system, acquires the licence 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 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 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.

4.1 The card based access control system

The internal access control subsystem uses not only face recognition and licence 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 is illustrated in the following.

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) RFID (Radio Frequency Identification).

The magnetic strip allows one 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 unaltered the stored data 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 4000 oersted).

Low coercivity strip is recognizable from brown colour and it is generally used for banking applications. High coercivity strip is recognizable from black colour 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 of 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 cards are 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 application that is a worldwide programming language used in a plenty of devices.

The used card is also equipped with RFID (Radio Frequency Identification) system that allow it to work contact less and within a certain distance from the reader. The working principle is the following: the reader send a electromagnetic pulse to the RFID or TAG (composed by the reader/writer system and the antenna) that send back an electromagnetic pulse to the reader, containing the requested information. The TAG can be characterized from different shape and can be inserted into glass, resin, label or card. It is composed by 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 if 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 from the reader.

The active TAG is characterized by using a battery to work as an autonomous transmitter allowing of 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 with the 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 manage a proper anti collision protocol which allows different TAGs to communicate at the same time. It can implement different action 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) RTF (Reader Talks First);
2) TTF (Tag Talks First).

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 of people, even if they are characterized by a reduced operative range and by a reduced data bit rate.

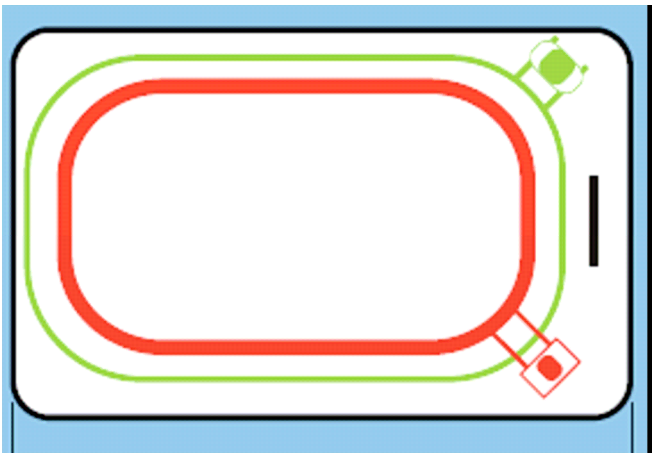

Figure 4: Scheme of a double antenna RFID card.

4.2 The considered solution

The implementation of the access solution needed to respect the current entrance criteria, optimising 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 card existing in the Vatican City State to simplify the entrance control of both Gendarmeries and Swiss Guards.

For this reason:

1) it has been created a central office for personal data acquisition and for cards creation;
2) it has been created an indexed database for data management;
3) it has been created a unique information visualization graphic interface;
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.

5 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 access control system that is capable of integrating the different security functionalities, ensuring the maximum reciprocal interaction of the different systems involved.

In this way it has been possible to realize a powerful and versatile integrated access control 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", *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 City State", *Risk Analysis IV*, WIT Press, Southampton (UK), pp.773-782, 2004.

[8] Garzia, F., Sammarco, "The integrated security system of the Vatican City State", *SAFE 2005*, WIT Press, Southampton (UK), pp.391-403, 2005.