Enhancing Security in Public Transportation Services of Roma: the PANDORA System

Pierluigi Pelargonio and Marco Pugliese
ATAC S.p.A. - Agenzia del Trasporto Autoferrotranviario del Comune di Roma
Roma, Italy
{pierluigi.pelargonio, marco.pugliese}@atac.roma.it

Abstract—**Nowadays local public transportation services (TPL) in large cities have to be considered critical infrastructures as, for instance, power plants or dams. Especially in Rome, where quite a million citizens per day uses TPL, any interruption in the public services can cause severe deterioration in urban life quality, congestion, compromised mobility and accessibility and enhanced pollution. Moreover TPL, and particularly subways, has been (remember the tragic facts in London subway on July 7th 2005) and still can be a target for terrorist threats and attacks. Therefore security must be considered as a crucial component in TPL services offer. Nevertheless lessons learnt from our experience, have suggested to apply some enhancements to the "classical" security model to switch the security operator from a mostly passive to a quite pro-active role and from a reaction to occurred events to preemptive actions. In other words, the role of security operators has to move from simple passive control (e.g. "see" events) in real-time, transferring data to stakeholders and ensuring timely decision-making without unnecessary steps in the communication chain. This paper will show how the advanced security services provided by our "PANDORA" system can enable this paradigm evolution. The "PANDORA" system is funded by the Italian Infrastructure and Transportation Ministry within the program framework of TPL security enhancement in the largest italian cities.**

Keywords—local public transportation system, subway security, critical infrastructure, security control room, security command and control chain, security and safeguard management

I. Introduction

Nowadays local public transportation services (TPL) in large cities have to be considered critical infrastructures as, for instance, power plants or dams. Especially in Rome, where quite a million citizens per day uses TPL, any interruption in the public services can cause severe deterioration in urban life quality, congestion, compromised mobility and accessibility and enhanced pollution. Moreover TPL, and particularly subways, has been (remember the tragic facts in London subway on July 7th 2005) and still can be a target for terrorist threats and attacks. Therefore security must be considered as a crucial component in TPL services offer. Nevertheless lessons learnt from our experience have suggested to apply some enhancements to the "classical" security model to switch the security operator from a mostly passive to a quite pro-active role and from a reaction to occurred events to preemptive actions. In other words, the role of security operators has to move from simple passive control (e.g. "see" events) in real-time, transferring data to stakeholders and ensuring timely decision-making without unnecessary steps in the communication chain. This paper will show how the advanced security services provided by our "PANDORA" system can enable this paradigm evolution [2]. The "PANDORA" system is funded by the Italian Infrastructure and Transportation Ministry within the program framework of TPL security enhancement in the largest italian cities.

The "PANDORA" system will implement the today's security guidelines defined by ATAC S.p.A. through the deployment of the latest hardware and software technologies as well as the adoption of the updated security management and organization guidelines (see Sec. II). The application of these guidelines has implied the start-up of a new conceived Security Management & Control Room - from both physical and functional perspective - where the command chain will be fully end-to-end managed. Nevertheless an advanced video-surveillance as well as novel software processing systems have been foreseen on board of trains and along subway tunnels to manage the emergency in case of train accident or fault. Videos from on-board of trains is transmitted to ground via fast radio links deploying WI-FI technology covering all subway tunnels and platform: as far as it results from specialized literature, a comparable employment of such infrastructure in a subway is the Moscow metro where recently has been put into operation a wideband internet connection service to passengers at stations and on trains [1].

Moreover in any station will be installed a pair, one per platform, SOS Emergency Call Points accessible to disabled and visually impaired persons.

A crucial innovation, we believe very few TPL administrations in the world can exhibit, is the availability of a real-time backup data stored in a bunkered elaboration data center so that, in case of destructive attacks engaged by terrorism, all video documentations related to the tragic event remain at disposal of Police investigations.

The paper will show the system architecture as well as the main requirements it is compliant to. To be noted that "PANDORA" design is "energy sustainable" as the foreseen hardware machines and electronic devices are classified as "green technology" which allow significant savings in term of energy consumption and expenditure as well as reduced costs for the maintenance.

The system is envisaged to enter into operation by winter 2014 / spring 2015 but an early demonstration trial on a stretch of subway Line A from stop "Vittorio Emanuele" to stop "Furio Camillo" (the PANDORA "pilot") which includes 6 stops, is available by summer 2014.

This paper is organized as follows: Sec. II deals with the security management guidelines which inspired the system, Sec. III the system requirements both in terms of security and technology, Sec. IV deals with the security services provided by PANDORA system, Sec. V enters in technical details and the reference system architecture is shown; Sec. VI reports the results of the pilot demontration.

II. Security Organization and Management Guidelines

An important pillar is the development of a comprehensive subway transport security and management program and procedures.

- Integrate all transportation modes security and emergency management at internal level and preferably also at Council Administration level as well as jointly to the other law enforcements agencies (e.g. Police forces);
- Develop and process internal communications to provide information regarding security risks within the Department of Mobility and Transports and transport operators as well as critical external participants;
- Manage the security risks identified during the all-hazards risk assessment;
- Manage security incidents to minimize impact and speedy recovery.

An effective system for transport security and emergency management depends on interagency cooperation. All relevant organizations (in terms of enterprise structures and external agencies) must understand the role they play in preventing, responding to and recovering from (safety) and security incidents. A key factor in this cooperation will be the availability of effective communication channels. Developing a process that efficiently and accurately provides for the exchange of information is critical to effective coordination and risk management.

III. System Requirements

A. *Security Requirements*

The security guidelines represented in Sec. II have been translated and mapped into the following security requirements for the PANDORA system:

1. Availability of a bunkered Security Management & Control Room;
2. Centralization of all security information to a virtually unique processing point;
3. Share of the relevant security information with other law enforcement agencies (e.g. Police, Carabinieri, Ares, Fireguards, National Civil Protection) and the other central rooms (Questura di Roma, "Sala Sistema Roma" of the Council Administration);
4. Application of the disaster recovery and fault tolerance procedures to security information delivery, storage and processing infrastructures.

B. *Technological Requirements*

Nevertheless system requirements The security guidelines represented in Sec. II have been translated and mapped into the following security requirements for the PANDORA system:

1. Modular design for the different system components;
2. Interoperability among products (e.g. ONVIF, PSIA standards);
3. Introduction of digital technologies as much as possible (taking into account legacy infrastructures and devices still into operation);
4. Adoption of "green technology" to allow significant savings in term of energy consumption and expenditure as well as reduced costs for the maintenance.

ONVIF [4] stands for Open Network Video Interface Forum and is an open industry forum for the development of a global standard for the interface of IP-based physical security products. Therefore ONVIF compliancy allows systems to rely on standardized communications between IP-based physical security products regardless of manufacturer.

Similarly PSIA [5], which stands for Physical Security Interoperability Alliance, promotes interoperability standards for the security ecosystem such as video-surveillance, analytics, area control and storage.

IV. Security Services

The application of the security procedures according to the internal policies and the compliancy to the requirement listed above, return the following security services components:

1. Passive and active monitoring with full coverage of public as well as restricted areas (including tunnels and on-board of running trains));
2. Securing the enterprise real estate, such as civil infrastructures (e.g. stations, stops), rolling stocks and any other valuable equipment;
3. Supporting the application of deterrent actions against potential criminal intents in public areas;
4. Supporting the joint cooperation with Police Forces and other law and sanitary enforcement agencies in engaging critical situations such as protests and riots;

5. Detecting and preventing hazardous environmental situations in order to reduce / reset the risk of burglary, robbery, muggings.

V. Reference Technical Architecture

The PANDORA system is based on the availability of a fast and secure enterprise backbone network to collect and deliver security information (alarms, videos, audios, and so on) from all sensors from the field segment to the Security Management & Control Room. We classify as Sensor whatever device able to capture information from the environment (e.g. video-cameras are considered video sensors and so on). Fig. 1 depicts the reference PANDORA technical architecture: basically three interacting components can be identified: the Field Segment which include the set of all deployed sensors, the Delivery Network (access and backbone networks) and the Security Management & Control Room (in case of particularly critical situations, the Operation Management & Control Room can backup its functionalities).

Each station in the subway (about 50) host what we denote an “Aggregation & Processing Node” which functionality is multiple: analogue to digital data conversion, local video storage, alarms aggregation and data relay to the backbone through the local edge switch. Access networks gathering data from on-field sensors to backbone though edge switches are based on fast optical fibers and broadband radio links. Optical links from on-ground sensors and radio links from on-board sensors. On-ground sensors include video-cameras on stations and platforms, intrusion detection devices and SOS Emergency Call Points. On-board sensors define the video-cameras installed on-board of trains.

The Security Management & Control Room represents the terminal site where all the security information is processed and managed. To this aim, the Security Management & Control Room hosts a dedicated Elaboration Data Centre and a Monitor Room where specialized operators can manage PANDORA clients from their desks.

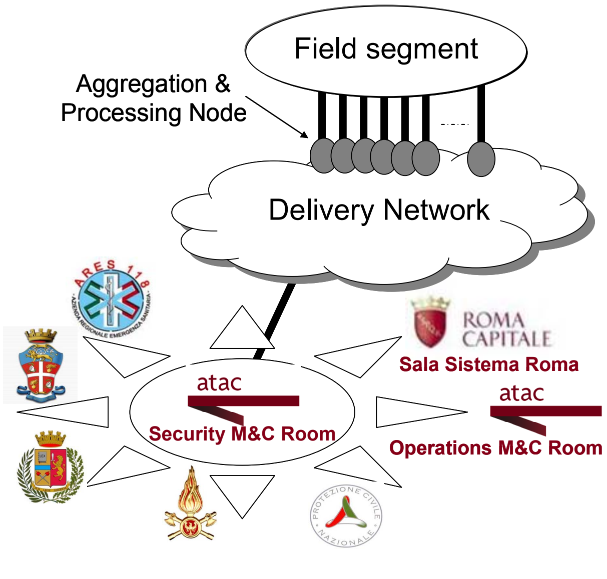

Fig. 1 Reference PANDORA Technical Architecture

Lastly, it seems remarkable that PANDORA technical architecture with the detailed list of the security requirements [3] has been the reference framework for Roma Metropolitane, the enterprise in charge of design and work directorate on behalf of the Council Administration of Roma, in designing the technical security of the subway Line B1: therefore the Line B1 is natively designed to be compliant to PANDORA systems currently foreseen in lines A and B.

A. Field Segment

Different class of sensors characterised by different traffic profiles have been deployed. The primary source of data traffic volume are about 3,000 analogue and digital (IP-based) video-cameras widely diffused on the subway lines, especially on stations, platforms, tunnels as well as on-board of running trains: the availability of infrared video-cameras into tunnels, allows an effective management of some highly critical emergencies, such as the passengers evacuation due to a sudden fault of a train, or automatically generating fire alarms or supervising secondary accesses such as ventilation ducts; on the other hand, the availability of real-time videos from on-board of running trains allows a capillary and effective active security action against robberies and muggings by the information of the coach number where the criminal event has to be managed. The traffic shapes generated by these sensors are typically CBR-like (Constant Bit Rate) from fast changing scenarios (e.g. from crowded environments) or VBR (Variable Bit Rate), typically ON/OFF profiles, from slow changing scenarios (e.g. from tunnels just when a train is passing). Another important class of sensors are the SOS Emergency Call Points (about 100 points). Each platform in each station hosts a SOS Emergency Call Point accessible to disabled and visually impaired persons and it is basically an advanced video intercom equipped with an emergency button to be helped from the enterprise security service hosted in the Security Management & Control Room.

Furthermore tens of double technology infrared-microwave intrusion detection sensors have been installed to prevent secondary accesses in tunnels from ventilation ducts and fire-guards dedicated wells.

An important security enhancement has been the introduction of special carpet shaped sensors sensitive to trampling (hereinafter trampling sensors) located at the end of platforms to prevent access in tunnel. To be considered that most suicides exploit this possibility. Once trampled on, the sensor issues an alarm to the Security Management & Control Room as well as an environmental video-camera pops-up to individuate the person who illicitly has accessed. Each station is equipped with 4 trampling sensors.

Particular attention has been cared to the safety of passengers at the platforms in stations. Each station is equipped with 2 SOS Emergency Call Points depicted in Fig. 2. These SOS points will be located, accessible to the disabled and equipped with Braille systems for the visually impaired. The SOS Emergency Call Points will allow audio-video contact with the Security Management & Control Room, and the operator will have the opportunity to see the person who requires assistance both through a video-camera integrated in the unit and an environmental video-camera installed in the surrounding area where the device is located. The call handler records all multimedia tracks and stores them with a retention time of seven days in compliance to italian privacy regulations.

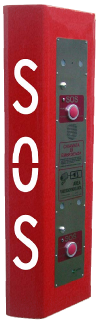

Fig. 2 A prototype of SOS Emergency Call Point

B. Delivery Network

We will focus only on the access segments, i.e. the radio trains to ground links and the optical links. For what concerns the enterprise backbone network, here is enough to recall that its topology results to be a mesh of optical rings (to assure tolerance to breakings) where CISCO routers have been adopted as switching nodes.

The radio access network is a chain of WI-FI access points at 5.4 GHz installed along subway tunnels. On-board video-cameras data are transmitted by streamers tuned to predefined sub-carriers (each frequency associated to each train) centered at 5.4 GHz. Signal continuity is guaranteed through a fast handover between ground antennas managed by a control unit, the Out Door Unit (ODU).

From the acceptance preliminary tests a bandwidth of 15 Mbps can be still available on the link even with the train reaching speeds of about 80 Km/h, the maximum operation speed. The radio interface is not fully compliant to IEEE 802.11.x standard (it derives from military standards) even the working in the same unlicensed frequency range: that's to strongly enhance network security to make un successfully conventional attacks and intrusions engaged by hackers.

Fig. 3 shows the entire transmission chain from on-board video-cameras to the Security Management & Control Room.

The on-board video-recorder (VideoNetBox™) locally stores 7 videos per half-train (2 video-cameras per coach, 3 coaches per half train, 1 external video-camera) and the streamer converts analogue videos into ITU H.264 compressed digital streams up to a bandwidth occupation of 2 Mbps. In line of principle, the residual bandwidth could be at disposal of passengers to access internet connections, as in [1].

The optical access network gathers data traffic from ODUs to the backbone. This access infrastructure is shared with the trunks of the Fireguards radio network.

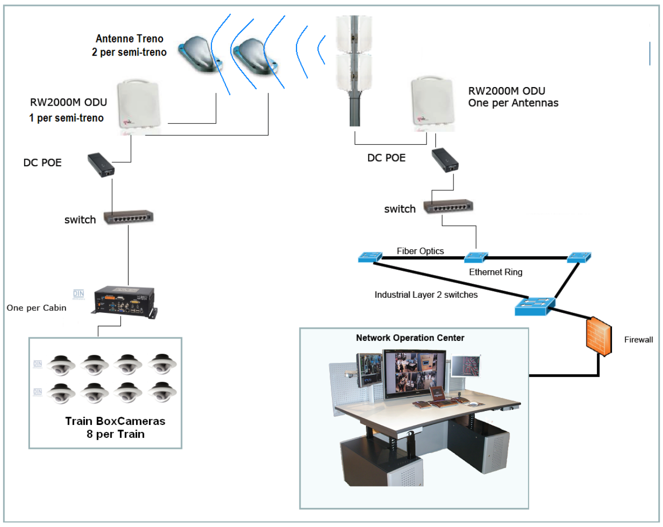

Fig. 3 Train to ground data transmission chain

C. Security Management & Control Room

The Security Management & Control Room must be able to fulfil the requirements during critical emergencies. It is the heart of the overall PANDORA system as it is the site where the command-control chain is managed.

Fig. 1 shows how the Security Management & Control Room can dispatch selective security information to the other law enforcement agencies (as Police forces, Fireguards) and sanitary emergences as well as to ATAC Operation Management & Control Room. This is made possible by the multicast facilities available from PANDORA video devices: once a real-time video is requested by a new user, the system first verifies if the corresponding stream is already active for some existent user and, if yes, the system simply addresses this stream to the new user without creating another identical stream. This is the well-known “add party” operation in a multicast communication. Multicast allows a true optimization in the usage of network resources.

Moreover the Security Management & Control Room can be classified as a “bunker” due to its compliancy to UNI 11068-2005.

A crucial innovation, we believe very few TPL administrations in the world can exhibit, is the availability of a real-time backup data stored in the bunkered Security Management & Control Room so that, in case of destructive attacks engaged by terrorism, all video documentations related to the tragic event remain at disposal of law enforcement investigations.

It will be operative 24x365. Security applications will be supported by computing facilities organized in a dedicated Data Elaboration Center and will be used by the operators at their desks (Security Operator Desk). Each desk will be equipped with the best-in-class electronic facilities.

Fig. 4 sketches a prototype fully equipped Security Operator Desk:

1-2 Video-walls to monitor up to 32 video-cameras; each video-wall will be managed by varidecoder devices easily configurable by using the “drag & drop” function;

3-4-5 Other screens on the single desk to be managed by the single operator;

6. Joy Shuttle to fastly access video archives;

7. Display equipped with a keyboard to directly and fastly invoke the visualization functions;

8. Joystick to manage pan-tilt-zoom functions in certain video-cameras.

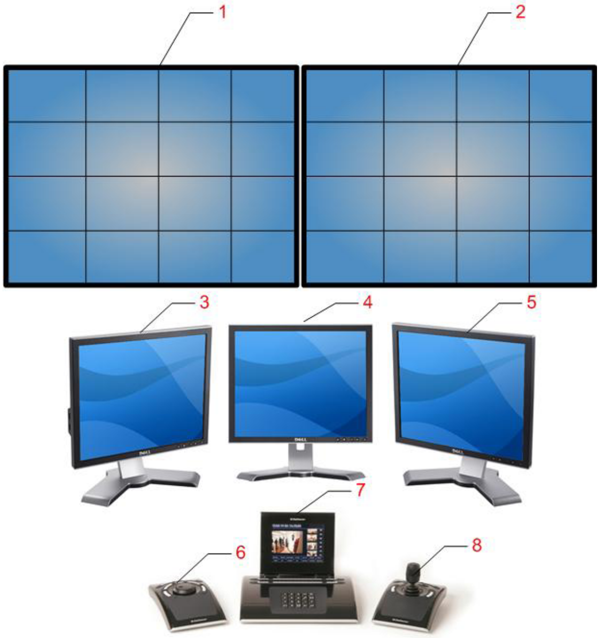

Fig. 4 A prototype Security Operator Desk

From the computing point of view, load balanced workstations and storage systems will be widely deployed.

From the security applications point of view, innovative video processing applications will be available:

- High-performance and self-learning video analysis systems which provides outstanding analytical results due to state-of-the-art image;
- Analysis algorithms and the constant adjustment of the system parameters to the current surrounding conditions (auto-adaptation). If used together with the different analysis applications, it can serve a variety of surveillance and counting purposes;
- Each issued alarm and each stream from a video-camera is reported in its environmental context by mouse clicking on a vector planimetry.

Security applications can be classified in three vertical components: intrusion detection, object counting and changing scenario monitoring:

Intrusion Detection: the system is able to recognise, for example, if an object approaches an area, and the direction it is coming from or how long it stays in a certain area. Based on the carried out classification the system can differentiate between an object “human” and an object, e.g., “car”. The object classification and the analysis of object behaviour provide important information to enable appropriate decisions by the system. Through comprehensive examinations of plausibility, false alarms are reduced to an absolute minimum without ignoring a “real“ alarm message. The alarm is transmitted to the Security Management & Control Room via delivery backbone network, the information is always immediately forwarded to the addressee. The security personnel are supplied with all relevant information at the operator stations to be able to quickly and assuredly make the necessary decisions. Since live pictures are often insufficient for assessing a situation, only the evaluation of the recorded alarm sequence - with pictures from before and after the alarm – can give an explanation about an event. In order to make management easier for the security personnel, the display is carried out automatically, individually and event-related. Especially in platforms, lighting conditions often change. This affects both the functioning of the video-camera unit and the image processing algorithms. In order to still achieve optimal analysis results the system automatically adjusts its parameters (auto-adaption). Event messages are:

- Person enters monitored area
- Person leaves monitored area
- Person stays in monitored area
- Person appears in monitored area
- Camera sabotage

Object counting: the system is able to analyse visitor fluxes and traffic flows within definable areas. The application counts objects, such as individuals or vehicles, extremely reliable if they are distinctly separated and allows for the operator to limit the counting to the entry or exit of an area. Due to the integrated event analysis, the individual counting results can be represented in graphical or tabular form.

Changing scenario monitoring: the system is able to protect objects (e.g. luggages) from theft and damage. The application reports illegal approaches, changes in position, the theft of an object, or unattended pieces of luggage in a platform.

VI. PANDORA PILOT DEMONSTRATION

The performed demonstration has shown all PANDORA security services in the stretch of subway Line A from stop “Vittorio Emanuele” to stop “Furio Camillo” which includes 6 stops. Services have been managed and controlled from the Security Management & Control Room The demonstration has been carried on during the ordinary transport operations, hence in the most realistic conditions.

The demonstration has simulated a burglary. It consists in undue access to a station from a ventilation shaft, then, came in the station, the transgressor vanishes by taking a train. Several alarms have been released by the anti-intrusion devices located in the ventilation shaft as well as the video pop-up from the infrared environmental video-camera; moreover the trampling sensors located at the end of the platform warns that someone has entered (or exited) the station from (or to) the tunnel; the on-board video-cameras allow to track the transgressor along the coaches of the train.

Moreover a passenger, aware of the emergency situation, warns ATAC Security from a SOS Emergency Call Point indicating which train the transgressor had taken. Using this information, the Security personnel could identify the transgressor and then capture him.

The performance results have been truly positive from both management and control point of view: the joint information from intrusion detection located in tunnel and at the edge of the platform have allowed the Security personnel hosted in the Security Management & Control Room to alert a security patrol to intervene on place; however the information from SOS Emergency Call Point has changed the intervention strategy. Information from tracking the transgressor along the train, has allowed a punctual intervention directly at the right coach of the right train directly on the following stop. Obviously also the underlying technology has worked well: negligible delays in issuing alarms and videos, good quality of image resolutions, no false positives and false negatives during the demonstration.

VII. Conclusions and Perspectives

The PANDORA system, a largely innovative platform to enhance security for the public transport in Roma, has been presented and a pilot demonstration setup has been shown.

However it should be recall that up to now PANDORA covers only subways. A possible minimal extension is the availability of video-cameras on-board of buses, at least for the most critical and hazardous lines to protect both drivers and passengers. Moreover some PANDORA security services are currently foreseen to be into operation only in part of the subway lines.

Currently ATAC Management is making aware the Italian Ministry of Infrastructures and Transports to devote further funds for these important extensions.

Acknowledgments

The PANDORA project aims to be the “best-in-class” project to support security in the public transportation service. Therefore the design has been based on the availability of the “best-in-class” worldwide technologies in the security sector.

We would like to give credits to the Head of the Security Technology Department in ATAC S.p.A., Dr. Bottaccio, the contractor Standard System Engineering s.r.l., which is the technology enterprise in the Italpol Vigilanza Roma Group, and the following technology suppliers: the german manufacturer Dallmeier G.m.b.H. for the provision of video-surveillance system, the israelian manufacturer Radwin Corporate, supported by the italian Orange Open Solutions s.r.l., for the ground-train board radio segment, the italian Ermes Elettronica s.r.l. for the provision of the SOS Emergency Call Points.

References

[1] Basedin, I., “The On-going Modernization of Moscow Metro,” Eurotransport Magazine, n. 2, 2014

[2] Pelargonio, P., “The PANDORA Project for a Secure Metro in Rome,” Public Transport International Magazine, UITP, n. 1, 2012

[3] Pugliese, M., “Linee Guida di Progettazione dei Sistemi Tecnologici a supporto del Servizio di Vigilanza delle sedi ATAC S.p.A.,” ATAC Technical Report, v.1.0,, November 2011

[4] ONVIF, www.onvif.org

[5] PSIA, www.psialliance.org

Pierluigi Pelargonio: Dr. Pelargonio is currently the Head of Security and Safeguard Department in ATAC S.p.A.; furthermore, he covers the role of Effective Member in UITP (the “Union of International Public Transport Operators”) Security Commission and in the SECUR-ED EU Project (FP7) Advisory Group. Through his activities in these institutions he is pursuing an effective impact on security sector at international level. As former Section Commander of Italian Financial Police, he distinguished himself in the field of fight against tax evasion and revenue damages. Graduated in Economics with honors, Dr. Pelargonio obtained the professional qualifications of Chartered Accountant and Auditor, being invited as lecturer as well as speaker in several events (e.g. Universities, Public Administrations, Financial Police Academy). He has been lecturer of the course in “Direct and Indirect Taxes" for the Financial Police Academy.

Marco Pugliese: Dr. Ing. Pugliese is currently at the Security and Safeguard Department of ATAC S.p.A. as deputy for public works directorate and technology innovation. He is the designer and director of the “PANDORA” project. Since 1995 he has joined different major companies in the field of information and communication technologies (ICT) and involved in standardisation activities in ESA (the “European Space Agency”) and ETSI (the “European Telecommunication Standard Institute”). Dr. Pugliese is graduated in Electronic Engineering and holds a Ph.D. in Electrical Engineering and Computer Science. He has been lecturer in Telecommunications at the Military School of Transmissions of the Italian Department of Defense. He is member of IEEE (the “Institute of Electrical and Electronic Engineers”) and AIIC (the “Associazione Italiana esperti in Infrastrutture Critiche”). He has to his credit more than 30 international publications on ICT and security topics.