PRISMATICA: A MULTI-SENSOR SURVEILLANCE SYSTEM FOR PUBLIC TRANSPORT NETWORKS

S A Velastin[1], L Khoudour[2], B P L Lo[1], J Sun[1], and M A Vicencio-Silva[3]

[1] Kingston University, United Kingdom, [2] INRETS-LEOST, France, [3] University College London, United Kingdom

1. INTRODUCTION

Public transport systems play a vital role in the daily life of all citizens. There is a recognised need to shift transport patterns of usage from private means to public means as this has beneficial effects in terms of the environment, reduced road-related deaths and general quality of life. Public transport environments are complex ones involving a large number of people (passengers and staff), control management and procedures. One of the many factors that play against increased patronage is related with personal security aspects, both real and perceived. To understand what these factors are and to propose technical, operational and social solutions, the project PRISMATICA ("PRo-active Integrated systems for Security Management by Technological, Institutional and Communication Assistance") was funded by the European Commission, involving important European transport operators (London, Paris, Brussels, Milan, Prague and Lisbon), research institutions, manufacturers and transport consultants.

A public transport environment is then conceived as being in the hands of what sociologists call a "capable guardian". Traditionally, this has meant an operating company deploying staff and monitoring systems (such as CCTV) to carry out manual based surveillance of the environment to prevent undesirable events and to reassure the travelling public that they are in a safe and secure environment.

2. THE PRISMATICA APPROACH

2.1. General Context

An important objective of this project was to explore how the advantages of new technological solutions (hereafter referred as "tools") can be fully exploited and provide opportunities for the enhancement of security management. The introduction of new tools and technologies in organisations can fail because of an inadequate understanding of the practical problems the security staff face everyday in the workplace ("processes"). Thus, the design and development of the innovative tools was informed by field studies and interviews with security staff in public transport networks. These case studies provided a detailed understanding of the working context into which the tools and technologies are to be deployed and formed the basis for the elicitation of operational requirements and user needs.

This detailed understanding of the current practice of security control and surveillance work focused on a number of issues. Firstly, the case studies showed how staff envisage and identify problems. Among the security incidents which the personnel deals with on a daily basis are events such as overcrowding, people falling in escalators, ticket-touts, beggars, buskers, pick-pockets, etc.. It was recognised that the development of detection criteria for these events needs to take into account how the relevance of events are established and how they are identified in the course of the organisational activities.

Secondly, the accomplishment of the surveillance work depends on the technical and organisational resources on which they rely, and how these resources, such as CCTV and traffic information, are interleaved and interdependent. Control room operators use multiple sources of information to assess scenes – these include multiple images viewed simultaneously from several cameras and other technologies like traffic information and alarm systems.

Thirdly, the design process depended on an understanding of the ways in which the staff, as a team, develop and implement solutions to problems and difficulties, and in particular how they manage and coordinate the activities.

In short, the development of automatic recognition systems and passenger alarms was related to an understanding of the various ways in which events are detected and managed, the dependence on collaboration and interaction with other staff and organisations, and the resourceful use of camera views and communication devices.

On aspects pertaining to perceived security, several personal and environmental factors that influence the perception of risks to personal security were identified during this and related projects (Deparis et al (1), Tyler (2), Vicencio-Silva et al (3)). What a person experiences as his/her own personal security is the result of the interplay of all these factors. The main feeling associated with the perception of insecurity is the feeling of isolation. This can be triggered by personal factors alone (depending on the role played by the person, e.g. passenger, staff, police agent, etc.), but usually, one or more external factors are present. Public transport

operators' efforts to improve perceived personal security usually seek to reduce the impact of personal factors by altering environmental ones (space and information). People's most frequent request is site-wide presence of staff, which cannot always be fulfilled. Their stated "second best" is on-line, active, CCTV monitoring, which can only be achieved with the help of an automatic surveillance system for site-wide coverage.

CCTV monitoring affects environmental factors by letting the public transport operator be seen as in charge of its *space*. Of course this perception is lost if no response is obtained when trouble occurs. Thus, the need for the system to be on-line and for special response procedures dealing with alarms to be established at the same time. Information on the existence of this CCTV system, the related procedures and any results obtained (from customer surveys and/or prosecutions) while using active CCTV need to be displayed in a clear and accessible way, so that it reaches potential users of the system. It is therefore important that the design and provision of tools not only take into account specific operational requirements (how the tools are used in a particular management context), but also as means to free-up staff resources to increase direct presence and, eventually, to route appropriate information to passengers (e.g. on levels of congestion or "solitude" of particular areas).

2.2. System Components

Given the context described in the previous section, the PRISMATICA tools are aimed at providing an "instrumented" detection/action environment that enables control room operators to obtain timely information to improve personal security (reported and perceived) in public transport sites (in particular, metropolitan railway systems). It is clear that this can only be effected by deploying a range of sensing technologies and transmission means combined with usable human machine interfaces. Key requirements include:

- The deployment of detection devices especially in areas that cannot be constantly monitored due to the costs associated with deploying conventional (human) monitoring, especially in the context of lower costs of hardware.
- The integration of diverse devices into a flexible system architecture first to mirror the variety of information sources that are needed to support decision-making and secondly to support future improvements in the development of detection devices.
- Convergence of information into an integrated form of presentation (Human Computer Interface).
- Use, as far as possible, of current site infrastructure (hardware and liveware: people) to improve the chances of early deployment with evolutionary changes in organisational procedures and equipment.

A PRISMATICA system can be regarded as providing a set of diverse *devices* each of which can contribute added value to the monitoring task, generally in a localised manner. That is to say, each device deals with a relatively small physical area (e.g. a camera, a microphone, a mobile camera, a mobile panic button) without necessarily being required to handle global information. A possible analogy is a human guard checking that people do not jump over the gates in a particular area of the station. This is her/his limited task, dealing with it locally and sending information to a (more central) supervisor only when needed. The supervisor could also instruct the guard from time to time to change her/his task or her/his location. In PRISMATICA, many of these devices are capable of processing/analysis, so they are can also be referred to as "*Intelligent Devices*".

Using the same analogy, a supervisory point is needed to coordinate the action from such devices and to gather information generated from them so as to make informed decisions on the need to take preventive or corrective actions. This analogy, gave rise to the concept of a supervisory computer with the acronym of MIPSA ("Modular Integrated Passenger Surveillance Architecture").

The set of components used in PRISMATICA demonstrators, Velastin et al (4), is outlined in the following sections.

2.2.1 MIPSA. The MIPSA (developed by Kingston University) is the supervisory computer that provides a single point of contact with an operator and a means of controlling and communicating with intelligent devices (for other subsystems to be configured by the operator and to send information on detected events) over a scalable Local Area Network using a CORBA-based architecture with a flexible messaging protocol encapsulated in XML. The system also incorporates its own video processing subsystem e.g. for crowd monitoring purposes. This system was demonstrated in Liverpool St. station (London) and Gare de Lyon (Paris).

2.2.2 Intelligent camera system. Developed by INRETS (F). which integrates in a single device (PC) a system that can simultaneously deal with up to four video sources and implementing most of the event detection mechanisms developed in the earlier CROMATICA project (e.g. stationarity, queuing, occupancy rates, etc.). This system was demonstrated in Liverpool St. station (London) and Gare de Lyon (Paris).

2.2.3 Local camera network. INRETS has devised and tested in real-life situation an architecture to address security problems. The general idea is to avoid sending many full-resolution, real-time images at the same time to the video processor, by deporting the processing

power close to the cameras themselves, and sending only the meaningful images through the general network to the control room (where the MIPSA is for instance). Until recently, computers and video grabbers were much too expensive to even dream of having multiple computers spread all over the network. But costs are decreasing at a steady pace, and it is becoming realistic to believe that such a thing will be commonplace soon. Existing technologies already allow, although still at a cost, to realise such a working network.

2.2.4 Wireless transmission. At the core of this subsystem (developed by CEA (F)) is a transmitter/receiver using spread-spectrum techniques able to send multiple video/audio/data channels on a single radio link operating in a license-free band. The motivation is to provide mobility of sensors in a cluttered environment (such as those in the underground). Tests were conducted in Gare de Lyon station (Paris).

2.2.5 Train-to-track wireless transmission. Developed by Telemation (D) in conjunction with STIB (B). The wireless transmission is intended for video and data transmission. The pictures captured by cameras on board the trains are recorded locally in exchangeable ring storage. Video sequences are transmitted in real time from the carriages to a surveillance centre. The triggering of an alarm leads to the immediate transmission of pictures between central control and the carriage alarmed. The system was installed and tested on trains running on a line section between four metro stations of Line 2 between station Simonis and Rogier of the STIB (Brussels) network.

2.2.6 Audio surveillance. Developed by Thales Underwater Systems (F). A subsystem consisting of a PC with dedicated DSP boards has been developed able to detect abnormal sound signatures typically originating from passengers shouting for assistance. It was demonstrated in Gare de Lyon station (Paris).

2.2.6 Contactless passcard. Developed by RATP (F). It expands the concept of a smartcard ticket to using the same device as a "panic button", whereby a passenger that requires assistance can press the button and radio beacons distributed in the area pick up the signal, localise its position and identify the caller (the card). A signal is then sent to the Control Room (e.g. to the MIPSA) where it is combined with video information to allow operators to react in a timely fashion. It was demonstrated in Gare de Lyon station (Paris).

3. EXPERIMENTAL RESULTS

This section illustrates some of the experimental results that were obtained with the PRISMATICA components in various metro stations in Europe (London, Paris, Newcastle Airport). In this paper, we focus on the description of the MIPSA and the Local Camera Network

3.1. MIPSA

3.1.1 Communication Architecture. The communications architecture is based on CORBA. In broad terms, a CORBA-based system is based on software objects that are instantiated by distributed applications and normally registered through what is called a Name Server (located somewhere on the same network). When an application needs to access an object, it locates it through the Name Server. It then uses it as if it were a local software object. The implementation uses ACE/TAO, Schmidt et al (5), as a particular characteristic of this open source implementation is the ability to work with real-time applications.

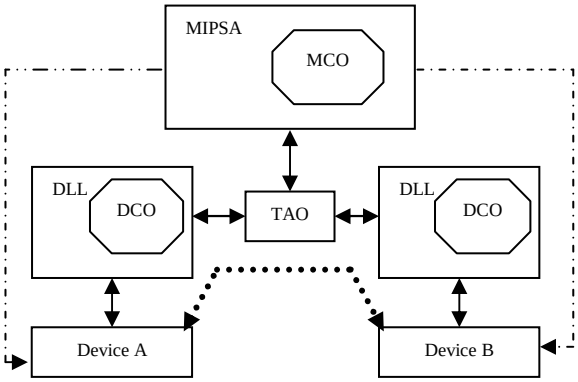

Figure 1: Overview of MIPSA/Device communications Architecture (DLL is a dynamic library that hides CORBA communications from Device applications)

Figure 1 gives an overview of the communications scheme, Velastin et al (6). MCO is a "MIPSA Communications Object" that resides on the MIPSA and that responds to messages sent by devices (a *device* in this context is a software application that can handle one or more sensors). The MCO can be used by a device to send event information to the MIPSA. DCO is a "Device Communications Object" that can be used by the MIPSA (or any other device) to send information to the device (e.g. configuration data). "TAO" is TAO's Object Request Broker that manages the distributed system objects (MCO, DCO) so that requests to access their data or call their functions are handled independently of where these objects are on the network.

A device connected to the MIPSA can establish a link to any other device in the system. This caters for situations that might benefit from such direct communications links (e.g. a camera "talking" directly to one of its neighbours, an audio device prompting a camera). This link between devices is shown as the thicker dashed line in Figure 1.

Devices or the MIPSA may need to send/receive large amounts of data between one another. In this architecture it is possible to set up socket communication links between devices and the MIPSA (or any other device). There are three types of connection, namely: Multicast (broadcasting), TCP (point-to-multipoint), and UDP (point-to-point, asynchronous, e.g. for non-critical streaming of data). Any device, or the MIPSA, can act as the server or client in a socket connection. Data can be distributed or sent to another device, once the socket connection is established. In Figure 1, an example of a Multicast connection is shown by the thinner dashed lines, where the MIPSA acts as the Multicast server, and the devices are the clients. The overall intention has been to emulate as far as possible the different types of communications that can take place in a monitoring environment.

When the MIPSA starts, it registers its MCO with the Name Server thus making it available to any device that is later connected to the system. The MCO is a simple object that can get/send messages from/to devices and also provides a network-wide time reference (for the time-stamping of events). When a new device is connected, it locates the MCO and creates a new object for the device (the DCO). Once the DCO for the device has been created, the MIPSA or other devices can communicate with the new device. Conversely, if for any reason the device is taken out of the system (e.g. for maintenance), it can sign itself out. In short, these mechanisms provide a flexible way of scaling the system up to any number of devices (subject to overall physical limitations such as network bandwidth).

3.1.2 Data protocols. The communication mechanism is always the same and what determines the action of the system is the *contents* of such messages (coded in XML). The set of messages are grouped into the following categories (Velastin et al (7, 8)):

- *Device Class Registration*: How a device informs the MIPSA of what devices of this type (same software) can do and how they can be configured by the system and an end-user. Note the flexibility so that what a device is capable of doing (and how these are expressed in human understandable terms) depends solely on the device and not built-in within the supervisory computer. Generic detection primitives have been defined to cater for a wide range of devices. These include aspects such as “alarm”, “measurement”, “status”, then sub-classified as “instantaneous”, “pulse”, “multi-sensor”, etc. The ability to give different priorities to different types of events is also included as well as a number of generic “primitives” to configure the device.
- *Device Physical Registration*: How to inform the system that a new device has been connected (or removed) from the system.
- *Event Detection Setting*: Messages sent to a device (e.g. through end-user interaction) that give the device what/when/how information on the events to be detected.
- *Event Information*: Messages sent by a device upon detecting an event (or as part of a regular stream of measurements such as people counting).

3.2. Local Camera Network

INRETS has developed a multi-camera vision system specified to meet key requirements of security and monitoring tasks in a transport network, such as intrusion detection in forbidden areas, passengers counting, and occupation rate in strategic areas. The diversity of the tasks at hand implies significant processing power and highly versatile configuration options. These requirements are best met by a modular architecture based on localised image processing (at or near the camera), normally referred as an “Intelligent Camera” and distributed processing whereby cameras are connected on a local network sending event information/video only on detection of an event of interest. Six different detection algorithms were developed and tested:

- Intrusion detection in forbidden areas.
- Passengers counting in several places.
- Queue length measurement at the check-in desks.
- Occupancy rates in the hall.
- Detection of people going counter-flow.
- Detection of people and objects remaining stationary for abnormally long periods of time.

This system was integrated with the MIPSA in demonstrators in Paris and London and also tested with data obtained in Newcastle International Airport.

3.2.1 Intrusion detection in forbidden areas. This function uses a camera overlooking the entrance to the area to be protected (a tunnel in a subway station, for instance). The processor detects the moving edges in the image and takes into account the size of the moving objects, in order to avoid detection of small objects being thrown away by passengers or displaced by air flow. The user can optionally define active or inactive “windows” within the image, in case the frame of the camera encloses both forbidden and unrestricted areas.

This function requires one parameter, namely the minimal size of the moving shapes to trigger an alarm (this is necessary to avoid false alarms caused by e.g. bus tickets dropped by passengers). This parameter was set on images of small objects that we threw into the protected area, such as subway tickets, sheets of paper, of rolls of gaffer tape.

To estimate the rate of false alarms, we allowed the tape to run for a period of time during which nobody entered the field of the camera. We fine-tuned the system a little more by deliberately walking on the edge of the field, in order to cast shadows and reflections on the surface of the floor. Then we threw small objects (the same we had

used to adjust the size threshold), which represented about 100 cases. No false alarms were reported.

To estimate the number of missed alarms, we asked members of the INRETS team to walk (slowly and fast) and run through the field of the camera. Several shots were also made to include people stopping in the protected area. A missed alarm was defined as someone entering and leaving the protected area without being detected by the system. Again, no missed alarms occurred.

Figure 2: An intruder standing in a forbidden area, as seen by the intrusion detection camera.

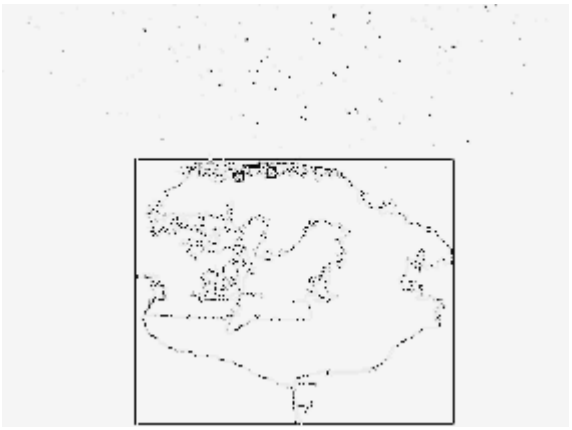

Figure 3: Result of the detection algorithm. The large black rectangle measures the size of the intruder.

3.2.2 Abnormal stationarity detection. This function averages the motions in the passenger flow, and detects whether some part of the image, not being part of the background, remains motionless for more than a user-defined time threshold (usually two or three minutes). This can be a passenger or abandoned packages.

Two parameters need to be set for this function: the time threshold after which stationarity raises an alarm and the time threshold after which it is considered to be normal again, and the object is integrated to the background (e.g. a thrown object or the trolley of a janitor). These thresholds were set to two and five minutes, respectively.

The images were shot in a corridor used by the passengers to go to the airplanes departure gates. The false rate alarm was measured on sequences showing only the passengers walking along this corridor. No such false alarm was found.

Then, abnormal stationarities were acted by members of the INRETS team, standing still in various places for more than five minutes, or leaving a bag for the same duration (cf. Figure 4). A missed alarm was defined as a person standing still for more than the first time threshold, but not raising an alarm. Again, no missed alarm was found in these conditions. It can only be reported that the detection is slightly delayed if many people pass in front of the stationary person or object.

Figure 4: Detection of abnormal stationarity of a passenger standing still.

3.2.3 Queue length measurement. This function uses a camera overlooking the counters with a very wide-angle lens, and can measure simultaneously the length of several queues, using a user-defined position of the start of each queue (this is done once for all, using a simple user interface that runs on the supervising PC, so no intervention on the field is necessary). It can then send these lengths to the supervising PC, for immediate display and/or to a log file for later use. Optionally, a length threshold can be defined by the user to raise an alarm when one or more queues become too long.

The camera was set up over the check-in desks in the hall of the airport, with a very wide-angle lens to capture as many desks as possible (a desirable step to reduce the global cost of both cameras and processors). Eight hours of tape were recorded, and an assessment was made by comparing the output of the queue detection algorithm (solid lines on Figure 5) to the visual appearance of the queues as we could see them on the screen. The algorithm appeared to give good approximations of the actual queues, and was even surprisingly robust in some instances, like that shown in Figure 5, which shows that people standing in the background, which might easily have been merged mistakenly to the queue, were correctly considered as completely unrelated.

The only problem we met is that very short queues are occasionally not properly treated. However, this problem arises only with queues of less than 10 people, and goes away as soon as more people get in line.

Figure 5: Measurement of the length of a queue.

3.2.4 Crowd density measurement. This function, which may run concurrently to the queue length measurement using the same camera, detects the non-background parts of the images and accumulates them through time to define an "occupancy map" of the overlooked area (e.g. the hall of an airport). It then calculates the "global occupancy" (between 0 and 100%) as either the average or peak value of the occupancy over the whole image, and sends this value, via the Ethernet, to the supervising PC, either for display or to a log file. Optionally, an occupancy threshold can be defined by the user to raise an alarm when overcrowding occurs.

Figure 6 gives an illustration of a density map. When the greyscale is white that means the corresponding person is standing for a long time.

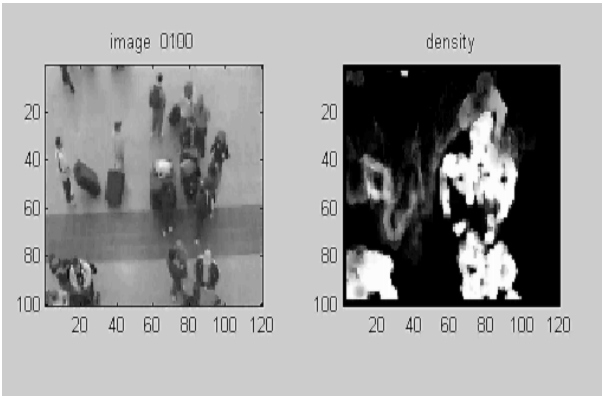

Figure 6: Density Map of people in a hall at Newcastle Airport.

3.2.4 Counterflow detection. We can go further about passenger safety improvement by detecting automatically, in due time, opposing flow in corridor. For safety purposes, this can be used as a clue to detect panic situations. A panic affects the motion pattern of the crowd as a whole. A good cue to determine such situation is to detect opposing flow in a one-way corridor. However, to avoid false alarms, the number of people in reverse flow must be high enough during a short period of time and these people must run. The detection of opposing flow is also interesting for the management of crowds. In some station, it is possible to display a message on one-way corridors to warn people that there are disturbing the flow. We see that on such situation, it is interesting to have an automatic process detecting such person. Figure 7 shows how a person going in a reverse way in one-way corridor is detected (Newcastle Airport test site).

Figure 7: Detection of a person going in a reverse way

4. CONCLUSIONS

A system for multiple-sensor surveillance in key public transport networks has been described. The design was closely inspired by what public transport operators are familiar with, i.e. the concepts of distributed sensors, distributed monitoring and decision making in a control room environment. Results have been presented that demonstrate the capability of automatic systems to detect potentially dangerous situations and of a distributed system that can promptly alert operators providing multiple sensor views of the events. Real-world demonstrators on key sites have demonstrated the feasibility of the approach. Further trials and developments are currently underway e.g. in London and Rome. The EU project PRISMATICA (GRD1 – 2000 – 10601) involved major European metro operators (RATP-Paris, LUL-London, ATM-Milan, STIB-Brussels, PPT-Prague, ML-Lisbon), research centres (Kings College London, University College London, Kingston University, INRETS-France, CEA-France) and commercial companies (TIS-Portugal, SODIT-France, FIT-Italy, ILA-Germany, Thales-France). The authors are grateful to London Underground, the Paris Metro and Newcastle International Airport for providing access to their sites and staff.

5. REFERENCES

1. Deparis, J P, Velastin S A and Davies A C, 1999, "The Cromatica Project", VLSI, Computer Architecture and Digital Signal Processing (The Kluwer International Series in Engineering and Computer Science), No. 488: Advanced Video-Based Surveillance Systems.
2. Tyler N A, 2002, "Accessibility and the Bus System: from Concepts to Practice", Thomas Telford, London
3. Vicencio-Silva M A, Allsop R E and Tyler, N A, 2001, "Empirical studies of the perception of key stakeholders". In PRISMATICA Deliverable 4: Report on requirements for project tools and processes, 2001; Brussels, Belgium: CEC DG–TREN, pp. 57-83.
4. Velastin S A, Sanchez-Svensson M, Sun J, Vicencio-Silva M A, Aubert D, Lemer A, Brice P, Khoudour L and Kallweit S, 2002, "Deliverable D7: Innovative Tools for Security in Transports", PRISMATICA Project (GRD1 – 2000 – 10601), European Commission, Brussels.
5. Schmidt D C, Natarajan B, Gokhale A, Wang N, and Gill C, 2002, "TAO: A Pattern-Oriented Object Request Broker for Distributed Real-time and Embedded Systems", IEEE Distributed Systems Online, Vol. 3/2.
6. Velastin S A, Vicencio-Silva M A, Lo B and Khoudour L, 2002, "A Distributed Surveillance System For Improving Security In Public Transport Networks", Measurement and Control, Vol 35, No. 8, September 2002, pp. 209-13, Special Issue on Remote Surveillance
7. Velastin S A, Lo B P L and Sun J, 2003: "A Flexible Communications Protocol for a Distributed Surveillance System", Journal of Network & Computer Applications, Elsevier (in print). Also see http://dilnxsrv.king.ac.uk/protocol
8. Lo B P L, Sun J and Velastin S A, 2003, "Fusing Visual and Audio Information in a Distributed Intelligent Surveillance System for Public Transport Systems", Acta Automatica Sinica, Vol. 29/3, pp. 393-407