SERKET: an open software platform for preventive security in public crowded places and for large events

F.-X. Josset & J. Mattioli
THALES Research & Technology, France

Abstract

Security of public infrastructures and for large events (cultural, sporting) traditionally relies on monolithic video surveillance systems, where security operators are quickly overloaded with information coming from multiple sources, displayed on multiple monitoring screens. Indeed, in such crowded places, it is quite impossible for operators to detect risk-prone situations in real-time and to react accordingly before such situations degenerate: they can only act after an alarm is triggered; surveillance is said to be passive. Conversely, the European project SERKET of the seventh ITEA call (EUREKA program), involving twenty-four industrial and academic partners, aims at developing an innovative software approach where dispersed data coming from heterogeneous sensors – cameras, microphones, human beings, as well as badge readers, IR barriers for intrusion detection, etc. – are automatically processed (signal processing), combined (information fusion) and analysed (threat assessment) so as to provide security personnel with the right information at the right time: security then becomes preventive. The objective of this paper is to glance at the innovations of the SERKET security system, and to focus on key layers of intelligent signal processing, advanced information fusion and situational awareness rendering.
Keywords: public security, safety of crowded infrastructures, surveillance of large events, open platform-based security system, advanced signal processing, smart sensors, information fusion, threat assessment, global situation awareness.

WIT Transactions on The Built Environment, Vol 94, © 2007 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE070451

1 Challenges of public security

1.1 Context

It is well established that public security represents a major challenge in most occidental countries, with dramatic cultural, economical and political stakes. Consequently to the terrorist attacks of New York in 2001, Madrid in 2004 and London in 2005, with a deep impact on populations due to terrific images over-broadcast by worldwide medias, numerous actions have been taken by governments for safety precautions by increasing significantly the human resources and equipment means. In particular, more and more video surveillance systems are being deployed over urban zones, public crowded places and mass transportation hotspots. Moreover, lower prices and an easier availability of hardware in the past years – video sensors, network equipments, computers, screens – lead to an outstanding rise of public and private video surveillance.

Yet, each country being governed by its own laws, including the protection of image rights of citizens, the spread of such video surveillance systems is very variable. For instance, many years ago more than four million cameras were said to be already deployed in the UK, and every Londoner was filmed three hundred times per day on average (figures have probably increased significantly, but what is relevant in this purpose is the order of magnitude). Conversely, in France where legal constraints are stricter, the number of cameras deployed was estimated in 1998 at one million units, including "only" one hundred fifty thousands cameras in the public domain.

In general, two major categories are recognised as sub-cases of "public security": urban security, and surveillance of critical infrastructures and of large events. On the one hand, urban security concerns the citizens' life in external and subterranean places (streets in the city, roadways, underground corridors, etc.): watching the demonstrations and the traffic in urban and suburban areas are two characteristic activities. On the other hand, the surveillance of public infrastructures and large events rather focus on complex buildings where important flows of people walk across, e.g., the infrastructures for mass transportation: airports, train stations, sea ports, as well as cultural, sporting and entertainment locations (theatres, football stadiums).

Whatever the case of public security taken into consideration, the job of order forces is hard and complex because of one common issue, namely the vulnerability of the location in question, which is as a combination of several factors:

- The high concentration of people exposed to multiple threats,
- The wide dimensions of the location and its environment, as well as the potential complexity of the infrastructures (architecture, proximity of restricted access zones with public areas, danger level inside), and
- The accessibility to the location, and the possibilities of intervention and evacuation (clearance of exits).

1.2 Current means and their limits

Nowadays the security of a public crowded infrastructure or of a large event involves in the best case the installation and the exploitation of video surveillance systems at some key locations, which images are transferred towards security screens and/or screen walls in a local security room and/or in a more global command and control centre. Most of the time these CCTV-like surveillance systems, either owned by a public organisation or by a private company, coexist but separately, and are monitored by different stakeholders assigned to their own location. Indeed, in some particular cases, such as the security of train transportation or the supervision of a risk-prone sporting meeting, the coordination between the various watched locations is ensured at the level of the command and control centre, where the field information are transferred according to predefined protocols.

For example, Figure 1 illustrates the classical approach for the security of sporting meetings as for sensitive football matches. The supervision is centralised at the level of a control room where operators can monitor the sensors deployed outside the stadium, and sometimes the inside sensors as well. In addition, the global ambiance is evaluated and continuously refreshed thanks to different witness media (radio link with security guards on the ground, news broadcasts, phone calls), to support decision-making if necessary.

The efficiency of the aforementioned classical means is conditioned by the speed of detection of a risky situation, i.e., a threat. This stresses the *curative*

Figure 1: Classical approach for the supervision of sporting meetings.

behaviour of such usual approaches: one decision (intervention on the field, move of guards, etc.) can only be taken once the operators in the command and control centre are aware of the situation, and especially of the exact nature of dangers; in the opposite case, no decision can be taken in order to avoid undesired consequences. It is important to notice here that at the control centre level, video is not used as a particular media from which dangers can be detected. In other words, images displayed on operators' screens are not by essence intended to help them in identifying threats, but rather in enhancing their awareness of the local situation in the frame of their mission (order keeping, traffic surveillance, etc.), and in particular when an abnormal situation has been reported to them through other means.

Concretely, the crucial phase of detection (threat, risk, danger…) is very difficult, if not impossible, to be achieved by the operators themselves due to an overload of information, a.k.a., "cognitive overload", more especially when watched areas are vulnerable public places with wide dimensions (thus potentially equipped with lots of cameras) and with huge flows of people with complex activities. To give an idea, the ratio of the number of cameras per operator usually amounts to one hundred, a little bit less in some cases; but this ratio goes higher and higher since the number of cameras and surveillance systems grows rapidly whereas the control centre staffs rarely follow that trends in accordance.

Besides this important issue of cognitive overload, some limits of current solutions for public security are admitted by the various stakeholders:

- Manipulated sensors (IMINT) are not uniquely fixed indoor analogical surveillance cameras: they are of different types and present various capabilities, they supply very heterogeneous information that are hard to manage optimally because of their different levels of richness, of reliability, of relevance, etc.
- Low or no "intelligence" at all is used to exploit the signals supplied by the physical sensors (SIGINT); in other words, there is a lack of automatic processing of data flows that could help in analysing the watched scenes.
- Human beings (security guards) are not considered as sensors like single physical cameras: their witness about the ambiance and physiognomy of the public place is reported directly by radio to inform the operators but it is processed no further (HUMINT).
- The roles, the activities and the responsibilities of all the stakeholders for the security of a large event or a public place – security guards and policemen on the field, agents in the remote security room, operators and decision makers in the command and control centre – should be taken into account in a more suitable manner in order to optimise the definition and planning of the security missions at their charge as well as the real-time decision making process, above all when constraints become too complex to handle (short time for responses, bounded resources available, impact of decisions, etc.).

2 ITEA project 04005 – SERKET

The European project SERKET [1] – *SEcuRity KEeps Threats away* – aims at supporting the surveillance personnel and increasing their global efficiency by enhancing their global awareness of the situation, and by reporting to them alerts detected automatically though on-the-fly analyses of data supplied by the sensors. Hence an intelligent processing of the heterogeneous content coming from various types of sensors (video, audio, human) implies a novel dimension to public security: the surveillance becomes *preventive*, in the sense that it now consists in recognising undesired situations before they actually develop and lead to irremediable damages.

Consequently, the major objective of SERKET consists in bringing some intelligence within software components in order to process data flows generated by hardware components and to deliver a precise picture that synthesises the current status of the situation. To meet this goal, one open software platform is being designed especially for the specific needs of public security. This platform encapsulates several innovative services:

- An integrated management of heterogeneous sensors: cameras, microphones, and security guards in a first set, which can be extended next to access control sensors, intrusion detection means (e.g., infra-red barriers), etc.;
- Some multi-source information processing: correlation, fusion, combination, aggregation, filtering;
- A qualification of information: systematic computation of a trust degree for each piece of information according to its origins: reliability of the causal sensors, precision of the signal processing algorithms, etc.;
- Shared situation awareness presentations, and qualitative and quantitative evaluations of threats.

The functional architecture of the SERKET system is depicted on Figure 2. It simply consists of four stacked layers, from the low-level equipment (sensors and other hardware) to the communication layer (signal processing components and middleware), the supervision layer (information fusion and situation awareness algorithms), and finally the command and control layer (visualisation and alert triggering devices).

Referring to this global architectural view, the SERKET project focuses on the specification, development and validation of:

- One vertical software platform that integrates several processing components, interfaces with various recording and display services, and that connects to hardware equipment and surveillance sub-systems,
- Advanced processing components at a low level (native signal processing) as well as at a higher level (information processing),
- Mechanisms for computing, triggering and displaying alarms on different devices (operators' screens, large tactical screen for situation awareness and decision making).

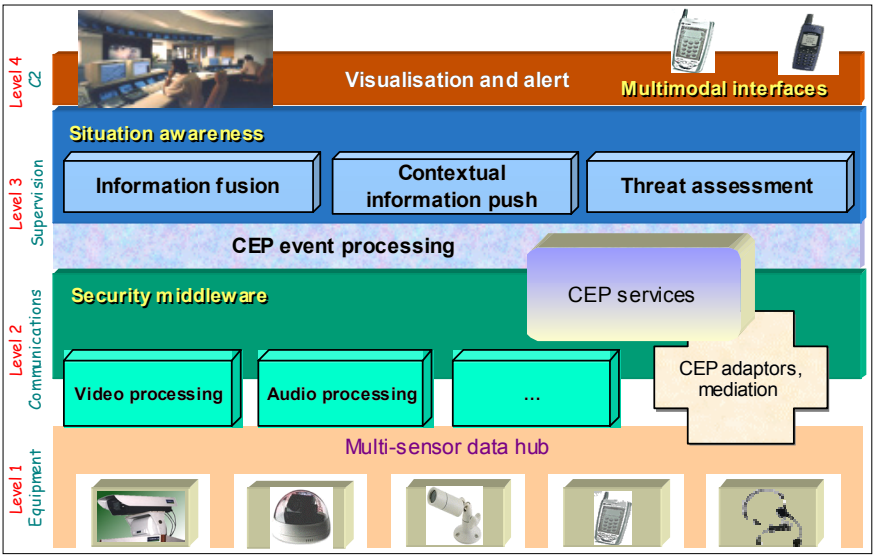

Figure 2: SERKET functional architecture.

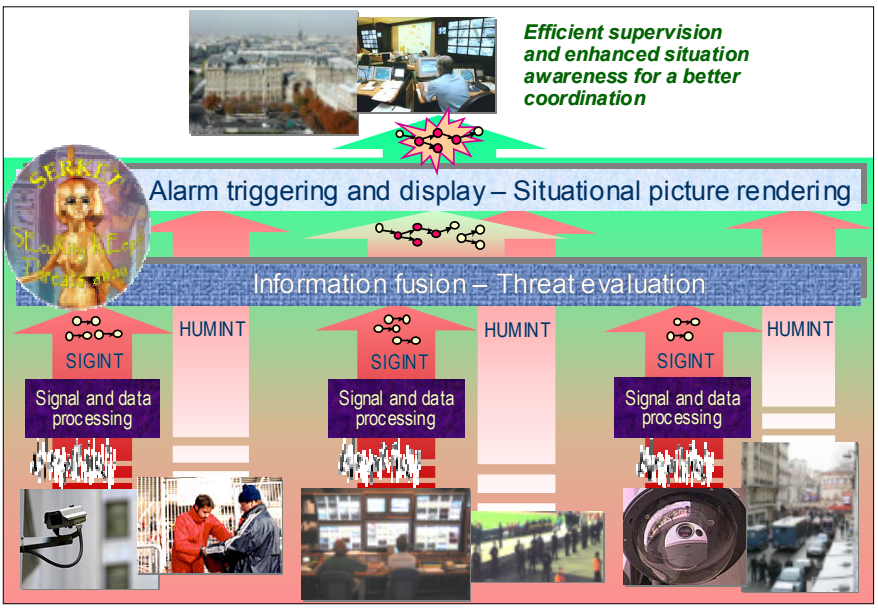

Figure 3: Supervision with the SERKET approach.

Coming back to the use case of Section 1.2, Figure 3 illustrates how a future SERKET system could be instantiated to enhance security of a sporting event.

Started in December 2005, the twenty-four-months SERKET project weighs a global manpower of one hundred fifty-three persons.year over four European countries (France, Belgium, Spain and Finland), for a total cost of seventeen millions euros. This project, led by THALES Research & Technology, federates R&D activities and integration work achieved by several big European companies (THALES Security Systems, EADS Defence & Security, Bull, Atos Origin, Indra Sistemas, Barco Views and Control Rooms, 4C/kZen from the Cronos group, Nethawk), in collaboration with research centres (CEA, INRIA, Multitel, VTT), universities (Murcia, Brussels, Mons), SMEs (Capvidia, ACIC, Uphill, Argosec) and governmental organisations (French and Finnish Ministries of Interior).

SERKET addresses the broad and growing market of homeland public security: mass transportation of passengers, urban security and traffic surveillance, organisation of large cultural and sporting events and meetings. The targeted customers are manifold: first they directly concern the security system providers who wish to extend their product offer (some of them belong to the SERKET consortium), and indirectly they also concern the customers of the formers, namely the organisers of large evens (local associations, public administrations), public authorities in charge of urban surveillance and traffic, state or private owners of crowded sites and infrastructures (railway companies, airports, etc.).

3 Some technical innovations

Technological innovations of the SERKET project are present at two principal levels: the security platform and the advanced information-processing layer. Additional R&D activities are led in SERKET as well, such as multi-camera multi-object tracking and the development of new video processing algorithms under more challenging conditions like light variations in indoor spaces (e.g., light turned off and on) or outdoor spaces (e.g., with weather conditions affecting the environment light); however, they are not detailed hereafter for the sake of conciseness.

3.1 Mediation principles for the security platform

One of the two major expected results from the SERKET project, namely the security platform, represents by itself one important innovation. Indeed this platform integrates the latest technologies and standards – Service-Oriented Architecture, Complex Event Processing, Mediation middleware – that enable one to satisfy the requirements outlined by the lower-level and upper-level processes.

Data mediation is the process of collecting and processing usage data from networked equipments and smart devices and delivering them to operation and business applications in real-time. Mediation services [2, 3] are intelligent middleware components that sit between heterogeneous data sources and applications which exploit these data for implementing functions such as: distributed monitoring, supervision and remote maintenance, customer relationship management, etc.

The SERKET platform relies on the mediation framework developed and deployed by the French SME ScalAgent [4]. Its central role in the SERKET architecture for (meta-)data transport and process is illustrated on Figure 4.

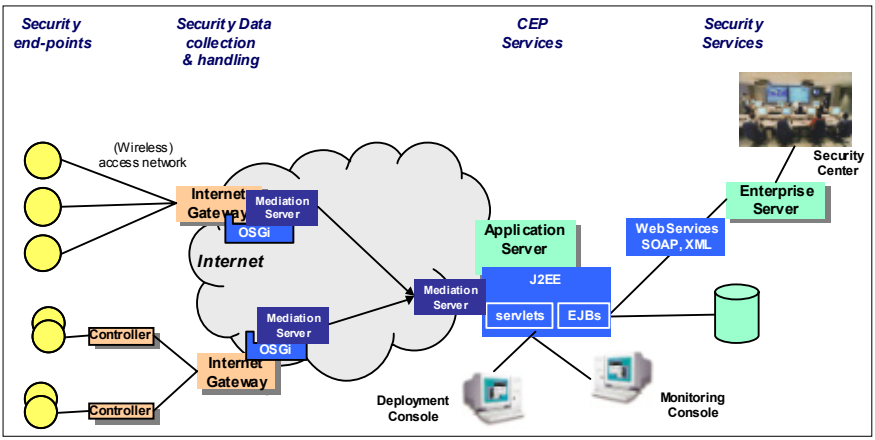

Figure 4: Technical architecture for (meta-) data transport and process (credit: ScalAgent).

The mediation is indeed a platform of choice for the overall integration of the SERKET system:

- The mediation binds distributed devices to the information system;
- The mediation enables two types of integration:
  - Data flow driven integration, by collecting the appropriate usage data, local processing (filtering, transformation, aggregation…) and transferring to the information system;
  - Commands flow driven integration, to control the devices.

The mediation also represents a common base for the whole software platform:

- For the middleware components, the mediation implements a reliable and secured asynchronous communication, i.e., a message bus based on standardised Internet protocols (TCP/IP, HTTP-SOAP, SSL…);
- For the application components, the mediation allows to implement the two-ways flows aforementioned (data and commands).

3.2 Advanced information processing

Complex Event Processing (CEP) is an emerging technology defined by a set of tools and techniques for analysing and controlling the complex series of interrelated events that drive modern distributed information systems [5]. CEP is particularly well suited for complexity arising from asynchronous, non-deterministic execution in distributed systems.

The innovative developments related to the creation and process of CEP events focus on the two following activities:

- The design of adaptors that enable the creation of CEP events, linking the lower level (multi sensor hub) with the CEP service;
- The application of CEP service components especially adapted to the SERKET scope (security of public crowded places and of large events):
    - Information fusion algorithms [6]: event pattern matching, filtering, transformation, correlation, aggregation, etc., that help is decreasing the number of low-level false alarms (thanks to a better qualification), and uncertainty mitigation;
    - Threat detection and triggering of the first alarms [7];
    - Risk evaluation resulting from the correlation of information over one or several simultaneous situations;
    - *A posteriori* analysis, by tracing the event path back to their origins (use of causal models: maps, graphs, etc.);
    - Efficient management of a big number of different CEP events generated by various sources (smart sensors, external systems, signals, humans beings) and at several levels (control, supervision, maintenance, etc.).

Finally, it is important to mention one additional innovation of SERKET. It relates to audio and multimedia processing, and presents several aims:

- Detection of deviations from the normal sound ambiance;
- Detection of speech and acoustic events that are characteristic of situations where human life is in danger (e.g., shouts, gun shots);
- Correlation of audio events with video events in order to increase the reliability of the underlying information (e.g., crowd movements, aggressive gestures).

4 Perspectives

This paper motivates and introduces the European project SERKET coordinated by THALES Research & Technology, that aims at building an innovative software platform for enhancing the security in public crowded places and for large cultural and sporting events. The key idea is to bring more intelligence to existing video surveillance systems at several levels: generalised smart sensors of different types, advanced information processing for threat evaluation, global picture rendering for improved situation awareness.

Several exchanges with many stakeholders in homeland security from both public and private organisations, as well as the analysis of their technical requirements [8] and the emergence of competitive initiatives [9], lead to the conclusion that SERKET objectives come as a response to a true and immediate operational need. This is the reason why the perspectives of result exploitations are very promising, even if very ambitious due to the sensitiveness of the application domain: SERKET represents a technological breakthrough upon which several partners will rely in order to increase their offer by providing more powerful and more adapted security solutions (supervision systems, services of integration, smart sensors…) according to the market expectations.

In particular, the reinforcement of security because of terrorist threats in the airports and in public transportation infrastructures [10] represents an important vector of business development for security system providers, and SERKET-like technology naturally comes as an outstanding differentiator in the offer of the expanding homeland security market, said to be of second generation [11].

References

[1] ITEA project 04005 – SERKET, http://www.research.thalesgroup.com/software/cognitive_solutions/Serket/index.html

[2] Tolk, A. & Garcia, J. J., Model-based Data Management for Mediation Services for Intelligent Software Agents, *Proceedings of the Symposium on Intelligent Software Systems for the New Infostructure, 16th International Conference on Systems Research, Informatics and Cybernetics (InterSymp-2004)*, 2004.

[3] Tolk, A., XML mediation services utilizing model based data management, *Proceedings of the 2004 Winter Simulation Conference*, eds. R.G. Ingalls, M.D. Rossetti, J.S. Smith & B.A. Peters, 2004.

[4] Mediation Framework, ScalAgent Distributed Technologies, http://www.scalagent.com/pages/en/products/tech-framework.htm

[5] Luckham, D., *The Power of Events: An introduction to complex event processing in distributed enterprise systems*, Addison Wesley, 2002.

[6] Museux, N. & Vanbockryck, J., Event based heterogeneous sensors fusion for public place surveillance, Submitted to *the 10th International Conference on Information Fusion (Fusion 2007)*, Québec, Canada, July 2007.

[7] Josset, F.-X., Mattioli, J. & Museux, N., SERKET: Une infrastructure logicielle ouverte pour la sécurité des lieux publics et des grands événements. *Actes du Workshop Interdisciplinaire sur la Sécurité Globale (WISG'07)*, Troyes, France, 30-31 January 2007. In French

[8] Guyonneau, P. & Robine, G., Les besoins interministériels en matière de technologie de sécurité. *Actes du Workshop Interdisciplinaire sur la Sécurité Globale (WISG'07)*, Troyes, France, 30-31 January 2007. In French

[9] Mecocci, A. & Pannozzo, M., Automatic detection of anomalous events for advanced real-time video surveillance, *Proceedings of the First International Conference on Safety and Security Engineering (SAFE'05)*, eds. C.A. Brebbia, T. Bucciarelli, F. Garzia & M. Guarascio, WIT Press: Southampton, UK, pp. 439-448, Roma, Italy, 13-15 June 2005.

[10] Katzman, G., Protecting against terrorist attacks for urban transportation projects, *Proceedings of the First International Conference on Safety and Security Engineering (SAFE'05)*, eds. C.A. Brebbia, T. Bucciarelli, F. Garzia & M. Guarascio, WIT Press: Southampton, UK, pp. 763-772, Roma, Italy, 13-15 June 2005.

[11] Civitas Group, *The Homeland Security Market*, 2006, http://www.civitasgroup.com/register.php?goto=/reports/20061208.pdf