Next generation of supervision systems for public security

F. X. Josset & N. Museux
THALES Research & Technology, France

Abstract

The increasing mass of information available from a wide range of sensors – video-surveillance cameras, badge readers, intrusion detectors… – tend to overload operators who co-ordinate security over public places and for large cultural, sporting or other public events. Although more and more images and low-level alarms are intended to boost the management of their complex missions, it is often impossible in practice for the operators to identify risk situations in real time, and then to avoid such situations degenerating. In this paper we present the principles of an innovative open software platform that automates processing, fusion and analysis of such information in order to provide security operators with timely warnings for effective preventive actions. Eventually we focus on the innovative information processing technologies that were integrated into the key mid-layer of the software platform.

Keywords: security of crowded infrastructures and public places, supervision systems for command & control, information fusion technologies, multi-threat assessment and situational awareness.

1 Challenges of public security

Public security missions generally require co-ordination from a centralized command and control room, where information of very different types is transmitted for supervision and decision making whenever necessary. Such missions include the supervision of:

- Large demonstrations of protest,
- Public transport strikes with outbursts,
- Order keeping in sensible districts suffering from damage and violence,
- Visits and trips of high-level political, cultural and religious VIPs,

WIT Transactions on the Built Environment, Vol 108, © 2009 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE090241

- Organization of large-scale sporting events,
- Surveillance inside and outside stadiums with high risk of violence.

Very often, these missions are difficult to manage since they depend on a combination of several factors of complexity, among which are:

- The variety and severity of latent threats,
- The layout and distances over the scene to watch,
- The presence of crowds and of hidden small violent groups,
- The control degree by the operators over the security sensors,
- The availability and ease of co-ordination of order forces,
- Overlapping demands of simultaneous missions.

Consequently, the supervision of one large event and the surveillance of a public site are hard to monitor from a remote command-and-control room. The accumulated experience of operators and good preparation remain today the best guarantees of adaptation to unexpected situations that occur regularly and that require fast decisions with dramatic consequences. Indeed, there is no complete solution available on the market to support the security stakeholders, which would tackle *all* the aforementioned factors of complexity in a satisfactory manner.

Yet, most western countries acknowledge the efficiency of video surveillance in preventing delinquency, and fighting criminality and terrorism – as exemplified initially in the UK. This trend is confirmed by an impressive acceleration of video-protection hardware installations – although providing lots of images rather than good quality ones. As an illustration, one study by ABI Research, issued in early 2008, predicts that the global video surveillance market will "expand from revenue of about $13.5 billion in 2006 to a remarkable $46 billion in 2013." [1] In particular, the combined market for CCTV hardware products – network cameras, video servers and NVRs – shall exceed $2.6 billion by 2010.

2 Concept of preventive security

Security devices, and more particularly video systems, play an ever-greater role in fighting public disorder. However, while video surveillance can provide important evidence for criminal prosecutions, there is a growing need to prevent threats, i.e. risk situations that develop in the first place. When installing more and more cameras and converging the video surveillance systems (interconnection through IP networks), the amount of information now provided to command-and-control rooms is simply overwhelming, making it impossible for security stakeholders to react in real time.

Still, such assets are straightforward for investigative activities – the more recorded images, the higher the chance to find clues – even if numerous questions are still pending, such as solving the trade-off between storage capacity and clarity of recorded images.

On the other hand, new doctrines and procedures have to be established for an appropriate exploitation of this overloading information in order to enable command-and-control rooms to cope efficiently. In these situations security

operators are responsible for assessing all the information related to their running missions, as well as relaying information and coordinating the security forces deployed on the field.

Currently, the sources of alarm for the command-and-control room are radio reports from order forces on the ground, plus small textual reports supplied regularly by intelligence offices. Video itself is *not* a source of alarm by default: it is impossible for operators to view in real time all the images related to their missions, it is only possible to focus from time to time on those judged the most informative. Unfortunately the multiplication of streams does not simplify the supervision tasks.

When analyzing automatically the information supplied by different types of sensors – such as video-surveillance cameras, intrusion detectors, access control barriers and microphones – one intelligent supervision system could alert operators as soon as any threat is detected and identified, allowing them to focus on the supervision part of their mission rather than trying to analyze themselves visually all incoming information. Their knowledge of the situation would be enriched – of prime importance when such a situation is particularly sensitive (violence), complex (risk of interference) and liable to concealed threats. This is the sound principle of *preventive security*.

3 Supervision systems of the future

THALES Research and technology, the corporate research centre of the THALES Group, initiated an important work that started in 2005 by proposing the principles of a novel software platform enabling the introduction of *intelligence* at each layer – lower level (sensors output), middleware, application (display input) – of a generic infrastructure especially dedicated to the surveillance of public places and large events. By leading the ITEA project #04005 called SERKET ("SEcuRity KEeps Threats away") until its end in 2008, we monitored R&D activities amongst a 23-partner consortium (SERKET partners are: BULL, CEA-LIST, EADS Defense and Security Systems, INRIA Sophia-Antipolis, Ministry of the Interior of France, THALES Research and Technology, THALES Security Systems (FR); 4CT/kZen, ACIC, BARCO, Capvidia, Faculté Polytechnique de Mons, Multitel, Vrije Universiteit Brussel-ETRO, Vrije Universiteit Brussel-MECH (BE); Atos Origin, INDRA Sistemas, Universidad de Murcia (ES); DELTABIT, Ministry of the Interior of Finland, Nethawk, Uphill, VTT Research Centre of Finland (FI).) who collaboratively prototyped such a software platform with easier integration and deployment capabilities, that is totally innovative in the business of security systems [2].

Besides the adaptation of some existing hardware devices and software components, new functions have been especially designed such as the generalized concept of heterogeneous smart sensor, the mediation principle applied to the security platform, some advanced signal processing algorithms for the recognition of abnormal behaviors, and the fusion of the generated information for an automatic detection of risk situations [3, 4].

The software platform includes the up-to-date technologies and standards – SOA, mediation middleware, Complex Event Processing (CEP) for information

fusion – enabling to meet the requirements of low-level processing algorithms (signal and data processing, e.g., images, sounds, interruptions) and upper-level applications (information filtering, correlation and combination for threat assessment, alarm triggering and situation picture display). The proposed event-oriented architecture is seen as the base of a new generation for integrated security systems.

Numerous technologies have been developed or tuned by the consortium in order to cope with the end-users requirements (including the French and Finnish Ministries of Interior). Amongst this set of technologies, some of them represent a genuine breakthrough, which we report in 3 categories:

- Intelligent signal and data processing:
  - Video: Robustness to challenging conditions, individual tracking, novel crowd motion algorithms;
  - Audio: Sounds detection (gun shots, shouts, window/pane breaking…), emotion classification in speech (fear);
  - Combination of both video and audio processing: Uncertainty mitigation (false alarm reduction);
- Information processing and fusion for enhanced situation awareness:
  - Complex Event Processing (CEP): Filters, matching rules, spatiotemporal correlations (see next Section);
  - Threat assessment: Trigger an alarm to the operator as soon as one potential threat is detected;
- Architecture: From classical surveillance equipment to a novel generation of integrated security systems
  - Event-driven architecture by coupling SOA and CEP service;
  - Heterogeneous smart sensors: (meta-)data produced in a generalized format.

The market segments addressed by such a software platform for complex security systems concern principally: mass transportation security (ports, airports, train stations…), urban security and road surveillance, and the organization of large cultural or sports events in stadiums, sports grounds, Olympic sites, concert halls, operas, etc. If we consider the video analysis means only, IMS Research published in a former report that the world market for software to analyze video content are exploding, growing from $67.7 million in 2004 to $839.2 million in 2009, at a CAGR of 65.5% [5]. One more recent report by IMS Research states that the market for video surveillance devices with mid/high end video analytics (person detection, vehicle detection, perimeter intrusion detection, asset protection, object detection, behavior recognition, people counting, etc.) is estimated to reach approximately $1 billion in 2012, with intelligent video cameras being one of the fastest growing segments.

4 Intelligent information processing to enhance mission support

Some developments initiated in SERKET are still continuing through the French project SIC ("*Sécurité des Infrastructures Critiques*": Security of critical

infrastructures.), in the frame of the world-class ICT cluster (*Pôle de Compétitivité*) "SYSTEM@TIC" dedicated to complex systems. The objective of this latter project is to develop new and generic homeland security solutions, adapted to varieties of predefined situation topologies: Open places, mid-open places, under control access places, and routes from A to B.

In a context of surveillance and security/safety of public places or critical infrastructures, having such system is interesting if it supports the understanding of the on-going situation. That means to be aware of the activities, the actors and to detect the intent in order to forecast what can happen later on.

Therefore, we consider that a situation is the conclusion of a reasoning involving a combination of different observable elements, according to a context, of which one doesn't often know when and where they occur.

This implies that to assess and understand a situation in progress, a system needs reactive and asynchronous reasoning capability. The Complex Event Processing (CEP) rules paradigm is an ideal candidate: it consists in an asynchronous and reactive principle based on extended reactive rules, providing a hierarchical modeling of the situation [6].

Such principle enables the introduction in supervision systems of a high level of detection of abnormal situations. This level is reached thanks to holistic threat assessment providing threat scenario detection. It is then easier to consider weak signals, understand here the detection of an activity that seams locally neutral but that is a step in the realization of an attack scenario. This implies a filtering of false positives too.

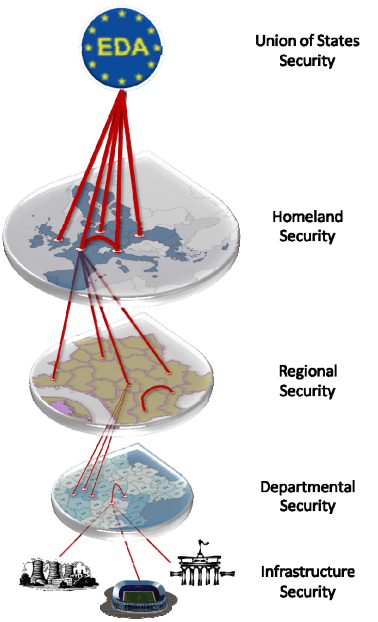

Figure 1.

Another property of CEP is its distributiveness capability. That means that two CEP-based systems can communicate and share knowledge remotely.

Figure 1 illustrates a hierarchical structure of security policies, from a very local focus (infrastructures) to a very global one (symbolized by the European Defense Agency). At each level, a CEP based system can be used to ensure the Situation Understanding function. But each of them can also provide inputs to its neighbors. Of course, detection at a low (= local) level of security can't have the same usefulness as at a higher (= global) level. According to those levels, the threats are different, in term of their impacts and consequences. One riot in the suburb of one big city is not the same "threat" than quite a lot riots almost everywhere in one country at more or less the same time. Actually, the forces engaged in response are not the same in both cases.

5 Technical focus

A *CEP event* is the report of an activity. It has one *significance*, i.e., the semantics of the activity, one *form* describing the activity in order to be process by a computer, and one *relativity* with other events (in many cases, the direct causal relationship).

The events are filtered and correlated by reactive rules, consistently with content and context assessments. Such rules provide as a result the generation of new events (called complex) and/or the execution of commands. The complex event can trigger another rule of the CEP rules set.

One CEP rule filters and correlates events thanks to an *event pattern*. It describes the way that events must occur (or not occur) before triggering the conclusion of the rule. One can use conjunctive, disjunctive or negative occurrence operators (Even if those operators look like traditional logical ones, one must remind that they deal with the appearance of events, and not with any truth-value of events. Thus, the negative occurrence corresponds to the absence, meaning the non-receipt, of an event.). Temporal order of appearance is also used (chronological or inverse chronological order). When this temporal order is constrained by a direct dependency relationship, one speaks about *direct causal* relationship.

Few other operators are also used to support the event pattern filtering description, as a time window (defining the time range of realization of a pattern) or a pattern repetition (defining how many times the pattern must be realized).

When a pattern is realized, a set of constraints or conditions is assessed. They verify that the events received and kept thanks to the event pattern are effectively the right ones (content filtering), but also that they occur at the right moment (context filtering). In the case of a positive assessment (i.e., the constraints are satisfied), the CEP rule runs the action in its conclusion part.

We have defined a CEP language (CEPL) with a clear logical mathematical semantic. Figure 2 shows the simplified Backus Naur Form (BNF) of this language. This syntax is useful at a human level of writing and reading, avoiding misinterpretation. We have also worked on a computer level syntax, based on Description Logic [7] and OWL [8]. The result of this work is a CEP ontology

```
<cep-rule-base> ::=     <cep-rule>+ .
<cep-rule> ::=      [<description>]
                    DECLARE <declare-event>
                    ON <event-pattern>
                    [SUCH-AS <constraint> ]
                    DO <action> {‘,’<action>} .
<description> ::—     Any string .
<declare-event> ::=     ( <event-type> <virtual-event-list> ‘;’ )+ .
<event-pattern> ::=     ‘∀’ <event-pattern>
                    |   ‘¬’ <event-pattern>
                    |   ‘⋁’ ‘{’<event-pattern> (‘,’ <event-pattern>)+‘}’
                    |   ‘⋀’ ‘{’<event-pattern> (‘,’ <event-pattern>)+‘}’
                    |   ‘(’<event-pattern> ‘≪’ <event-pattern>‘)’
                    |   ‘(’<event-pattern> ‘≫’ <event-pattern>‘)’
                    |   ‘(’<event-pattern> ‘→’ <event-pattern>‘)’
                    |   ‘(’<event-pattern> ‘||’ <event-pattern>‘)’
                    |   ‘(’<event-pattern>‘:’<constant>‘)’
                    |   ‘(’<event-pattern>‘#’<constant>‘)’
                    |   <virtual-event> | <filtered-virtual-event> .
<constraint> ::=    <predicat>{‘∧’ <predicat>} .
<action> ::=    generate <event-type>‘(’<property-value-list>‘)’
            |   throw <command-name>‘(’<parameter-list>‘)’ .
```

Figure 2: BNF of our CEP rule language.

defining the several concepts used in that event logic. A CEP rule becomes an individual of such ontology.

For example, admitting that a system is able to detect shot guns (audio analysis) and people falling (video analysis), the CEP rule for "*each time that those two events are sent in a time interval of 2 seconds and such that the* shot gun *event and the* people fall *event are located at the same place, then call the police to intervene*" writes:

- in CEPL syntax

$$
\begin{aligned}
&\textit{R2-BesoinPolice}\\
&\texttt{DECLARE}\ \text{ShotGun sg};\quad \text{PeopleFall pf};\\
&\texttt{ON}\ \forall\left(\bigwedge\left\{\text{sg, pf}\left[\text{hasLocation} = \text{sg.hasLocation}\right]\right\} : 2\right)\\
&\texttt{DO generate}\ \text{PoliceNeeded}\left(\right)
\end{aligned}
$$

- in OWL syntax

```
<cep:Rule rdf:ID="R2_BesoinPolice">
 <cep:hasEventPattern>
  <epdl:ForallPattern>
   <epdl:hasEventPatternOperand>
    <epdl:WindowedPattern>
     <epdl:hasEventPatternOperand>
      <epdl:ConjunctivePattern>
       <epdl:hasEventPatternOperand rdf:resource="#pf"/>
```

```
        <epdl:hasEventPatternOperand rdf:resource="#sg"/>
       </epdl:ConjunctivePattern>
      </epdl:hasEventPatternOperand>
      <epdl:hasTimeLimit rdf:datatype=http://www.w3.org/2001/XMLSchema#int
      >2</epdl:hasTimeLimit>
     </epdl:WindowedPattern>
    </epdl:hasEventPatternOperand>
   </epdl:ForallPattern>
  </cep:hasEventPattern>
  <cep:hasResultingComplexEvent
rdf:resource="securityEventTypesOnto.owl#PoliceNeeded"/>
 </cep:Rule>
```

Such OWL language simplifies a lot the management of a rule-based system. It is easier to know which rules are associated to threats, vulnerabilities, means, goods and so on.

Actually, as event sources are mainly smart sensors (camera + video processing, micro + audio processing, CBRNE sensors, biometric sensors, etc.) provided by various suppliers, the event forms of the detection capabilities (i.e., the observed activities) should be standardized in order to ensure their unicity. Thus, a tracking event would contain the same information (origin, destination, current location, date, etc.) whatever the sensor that caught it. This is necessary to guarantee the independence of the situation models as far as possible.

As a first proposal of standardization, we have established a SecurityEventType ontology by listing known (i.e., that one finds in scientific literature.) detection capabilities classified in different categories:

1. Abnormal (e.g., intrusion)
2. Behavioral (e.g., people scream)
3. Furtive (e.g., loud bang, shot gun)
4. Movement (e.g., crowd, person, object)
5. State (e.g., a door open, a panic crowd)

Another ontology named SecuritySystem, describes the surveillance system components, through the system itself and its features. The system description distinguishes devices, smarts sensors, analyzers, effectors. System's owner, system commands, device properties (zoom, sensitive capabilities, etc.) represent the system features.

This SecurityEventType ontology, associated to the SecuritySystem ontology, both on top of the CEP ontology, provides a powerful modeling framework. Figure 3 shows, in a more general way, our ontological structure. By importing (and linking them to each other) these three ontologies into one (*Domain*Ontology), we obtain a complete description of a domain of expertise, limited to the point of view of situation understanding capability.

The main idea of this modeling framework, based on CEP, is to provide support to an expert of an operational domain (let's say, security domain) in the formulation of his/her experience. The use of ontologies makes easier the development of man-machine interface dedicated to an area of expertise, hiding then some too technical aspects. Readers can refer to [9] for more details as well as for an example of the use of such CEP rules based systems for site surveillance applications.

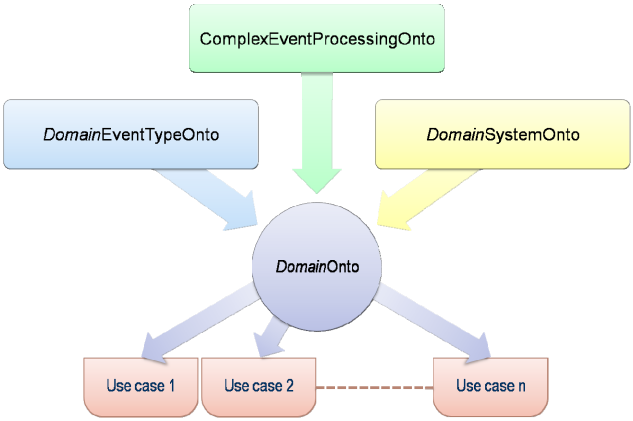

Figure 3: Organization of the ontologies used for CEP modeling.

6 Concluding notes

In this paper we have presented the principles of an innovative open software platform that automates processing, fusion and analysis of such information in order to provide security operators with timely warnings for effective preventive actions. Eventually we have focused on the innovative information processing technologies relying on the so-called Complex Event Processing paradigm, which were integrated into the key mid-layer of the software platform.

To conclude with our experience on the design of public surveillance systems, we claim that the technical requirements must derive from the user needs, but not the opposite. In other words the role of the end-users is crucial as soon as they can provide the industrial and academic actors with details on the limitations of the current means as well as on the functions they wish to be improved. More particularly, the participation of operational end-users to R&D projects enables the statement of a *precise* definition of their activities and the underlying constraints. This mandatory phase shall represent a key factor to success both for suppliers and customers of the security systems of the future.

Acknowledgement

The work described in this paper is partly supported by the French Ministry of the Economy through the project “SIC” of the *Pôle de Compétitivité* SYSTEM@TIC.

References

[1] ABI Research. *Video Surveillance Systems - Explosive Market Growth and New Market Opportunities*, 2008. http://www.abiresearch.com

[2] F.-X. Josset & G. Robine. *Vers une surveillance préventive des lieux publics et des grands événements*. In Actes du 2ème Workshop Interdisciplinaire sur la Sécurité Globale 2008 (WISG'08), January 2008, Troyes, France. In French
[3] F.-X. Josset & J. Mattioli. *SERKET: An open software platform for preventive security in public crowded places and for large events*. In Proceedings of the 2nd International Conference on Safety and Security Engineering 2007 (SAFE'07), M. Guarascio, C. A. Brebbia & F. Garzia (Eds), WIT Press, pp. 451-460, June 2007, Malte.
[4] F.-X. Josset, J. Mattioli & N. Museux. *SERKET: Une infrastructure logicielle ouverte pour la sécurité des lieux publics et des grands événements*. Revue de l'Electricité et de l'Electronique, No. 10, pp. 89-95, November 2007. In French
[5] IMS Research. *The World Market for Video Content Analysis*, 2005. http://www.imsresearch.com
[6] D. Luckham. *The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems*, Addison-Wesley Professional, 2002.
[7] F. Baader, D. Calvanese, D. L. Mcguinness, D. Nardi & P. F. Patel-Schneider (Ed.). *The Description Logic Handbook*. Cambridge University Press, 2007.
[8] *OWL Web Ontology Language Reference*. W3C Recommendation, 10 February 2004. http://www.w3.org/TR/OWL-ref
[9] N. Museux & J. Vanbrockryck. *Event-based heterogeneous sensors fusion for public place surveillance*. In proceedings of the 10th International Conference on Information Fusion, 2007.