Critical infrastructures as complex systems: a multi-level protection architecture ⋆

Pierluigi Assogna[4], Glauco Bertocchi[3], Antonio DiCarlo[2,5], Franco Milicchio[1], Alberto Paoluzzi[1,5], Giorgio Scorzelli[1,5], Michele Vicentino[5], and Roberto Zollo[4,5]

[1] Department of Informatics and Automation, University "Roma Tre", Italy
[2] Department of Studies on Structures, University "Roma Tre", Italy
[3] Master on Security and Protection, University of Rome "La Sapienza", Italy
[4] Theorematica spa, Rome, Italy
[5] TRS (Technology & Research for Security) srl, Rome, Italy

Abstract. This paper describes a security platform as a complex system of holonic communities, that are hierarchically organized, but self-reconfigurable when some of them are detached or cannot otherwise operate. Furthermore, every possible subset of holons may work autonomously, while maintaining self-conscience of its own mission, action lines and goals. Each holonic unit, either elementary or composite, retains some capabilities for sensing (perception), transmissive apparatus (communication), computational processes (elaboration), authentication/authorization (information security), support for data exchange (visualization & interaction), actuators (mission), ambient representation (geometric reasoning), knowledge representation (logic reasoning), situation representation and forecasting (simulation), intelligent feedback (command & control). The higher the organizational level of the holonic unit, the more complex and sophisticated each of its characteristic features.

1 Introduction

Complexity is ill-defined, as expounded by [1] in the inaugural paper of the homonymous journal:

> What is complexity? A great many quantities have been proposed as measures of something like complexity. In fact, a variety of different measures would be required to capture all our intuitive ideas about what is meant by complexity and by its opposite, simplicity.
> [. . .] As measures of something like complexity for an entity in the real world, all such quantities are to some extent context-dependent or even subjective. They depend on the coarse graining (level of detail) of the

⋆ Development funded by a research grant from the Italian Ministry of University and Research (MUR) to TRS, which stands for "Technology and Research for Security", a spinoff company from University Roma Tre and Theorematica.

> description of the entity, on the previous knowledge and understanding of the world that is assumed, on the language employed, on the coding method used for conversion from that language into a string of bits, and on the particular ideal computer chosen as a standard.
> [. . .] It is probably safe to say that any measure of complexity is most useful for comparisons between things at least one of which has high complexity by that measure.

For our present purposes, the non mathematical definition provided by the Complex System Society on its web page [2] is good enough. Notice that critical infrastructures are mentioned as exemplary:

> Complex systems are systems where the collective behavior of their parts entails emergence of properties that can hardly, if not at all, be inferred from properties of the parts. Examples of complex systems include anthills, ants themselves, human economies, climate, nervous systems, cells and living things, including human beings, as well as modern energy or telecommunication infrastructures.

If *controlling* a complex system is the issue at stake, then the stress should be laid on *integration*: monitoring and simulating separately the behavior of its parts is pointless, unless the same (or better) care is taken of their interactions. Recognizing global behavioral patterns, through (space and time) correlation among local events, is more important than detecting minute details. However, in a highly nonlinear system, *some* local minutia may have a strong global impact, and nobody can foretell with certainty *which* ones: hence the need for contextual knowledge and educated guesses. In order to provide a higher-level of awareness for security and safety of complex critical infrastructures, we need a system architecture that is able to integrate the human insight with the capacity of combining a myriad of events dispersed in time and space.

Accordingly, we introduce here an advanced architecture for protection of complex critical infrastructures. It includes: (a) a geometric reasoning engine, providing a multi-scale digital model of the infrastructure to be protected and supporting video surveillance and sensor fusion; (b) a distributed data mining environment, dedicated to event discovery and tracking; and (c) an advanced control center, supporting situation evaluation through dynamical modeling and simulation. In our opinion these components are the best candidates to: (i) serve as a point of reference for the integration of vision, sensor, tracking and security systems committed to infrastructure protection; (ii) provide a reliable basis for high-level situation awareness; (iii) enable coordinated and optimized decision making.

Complex critical infrastructures, in particular those crossing national borders (such as tunnels, bridges, etc.) or affecting the everyday life of thousands of people (such as railways hubs, airports, power plants, etc.), require a novel security approach and architecture. Their security, i.e., the capacity of preventing threats and reacting to menaces, should be based on a strong control and awareness of daily operations, since a security threat can arise not only from malicious attacks but also from natural events (storms, floods, etc.) or unexpected facts, like traffic congestion or collisions. An advanced security architecture should also provide means to infer the consequences of events from available information, possibly augmented via interpolation of missing elements. This is, in our view, the actual value of including virtual/augmented reality and advanced interfaces in our proposed architecture. Moreover, the knowledge base should be used for events analysis and decision-making. Modeling and simulation are complementary components for decision support. Conversely, present-day security systems are generally assemblies of sensor subsystems, with very limited capabilities of assisting the personnel during normal operations and crises.

In this paper we discuss the development goals and the implementation directions of a new platform for security of critical infrastructures based on the above described architecture. This platform is based on: (1) capability of providing (natural or artificial) sight instruments; (2) events analysis and correlation for decision support.

2 Critical infrastructures are complex adaptive systems

Saying that critical infrastructures are generally complex, and that their way of being operated and utilized is complex as well, is obvious and tautological. It is like saying that life is complex. What is useful, on the other hand, is examining specific characteristics of this complexity, and deriving specifications for a system aimed at protecting these infrastructures.

Evolution Any infrastructure that works in a public environment, providing a service or products, even if it has been designed to be simple, evolves rapidly towards complexity. Such an evolution is unavoidable, because the environment itself evolves, in terms of technology, user requirements, styles of consumption. Simple systems (and artificial systems start like that), when integrated into an environment where people are a major actor, evolve into complexity, and if this evolution is successful (that is, if the infrastructure keeps maintaining its design goals), then it develops adaptivity. This means that people dedicated to its maintenance modify, make additions, take out parts no longer needed, inevitably diverging from the original design. A working critical infrastructure can be considered a *Complex Adaptive System* (CAS) [3, 4], i.e. macroscopic collections of simple interacting units (typically in a nonlinear way) that are endowed with the ability to evolve and adapt to a changing environment.

> A Complex Adaptive System (CAS) is a dynamic network of many agents (which may represent cells, species, individuals, firms, nations) acting in parallel, constantly reacting to what the other agents are doing. The control of a CAS tends to be highly distributed and decentralized. If there is to be any coherent behavior of the system, it has to arise from competition and cooperation among the agents themselves. The overall behavior of the system is the result of a huge number of decisions taken simultaneously by many individual agents (John H. Holland, in [4]),

Holonic organization Except for very special cases, CASs are organized in a multi-level holonic architecture, typical of evolving systems. A modular architecture is good enough for static systems, where the maintenance or substitution of each module is made greatly easier by modularity, as long as the original interface specifications do not change. On the other hand, an evolving adaptive system needs modules that are able to accept interfaces different from the originally designed ones, adaptive more capabilities than those required by their present role in the system, capabilities that can be awakened by the intervening circumstances. These modules are the *holons* [6].

Discontinuous co-evolution The evolution of a CAS is always a co-evolution with all the (complex) systems that make its environment. We can talk of synplastic systems, derived from syn (together) and plasso (modify). This evolution is generally discontinuous, alternating periods of rest with bursts of activity. The mutual influence of each system on its neighbours forces shifts and re-organizations, where adaptivity is the tool for survival. In this game each system tends to maintain its configuration, absorbing exogenous disturbances. However, sometimes it has to re-organize, and then it generally shoots disturbances all around. This interplay of absorb-or-react is cause (and effect) of discontinuities in the overall co-evolution.

The protection platform A basic rule of control mechanisms is that the controller has to have a level of complexity higher than the controlled. A system aimed at protecting the complex systems represented by critical infrastructures should be provided with an architecture that mimics that of the environment it has to support. By having this architecture, it can more easily co-evolve with the infrastructure, adapting its resources to the changing requirements. Its architecture should be:

Holonic : each module needs the capability of coping with different logical interfaces (even if physically normalized such as for Web Services);

Multi-level spatial nesting : a universal characteristic of holons is that they are composed of holons: different platform modules should have a modular architecture, in accordance to the spatial modularity of a typical infrastructure (i.e., site, buildings, floors, rooms).

Multi-level temporal nesting : the processes involved in the management and use of complex infrastructures are organized in levels. These levels are represented by cycles (weeks, days, shifts, etc.) and by waves of activity. Security enforcing processes must be tuned to these cycles and waves, in order to analyze threats and recognize weak signals of possible abnormal people behaviour or technical failures.

Holonic architecture In [7], each holon can be considered a *situated multi-agent system*, i.e. a finite-state machine where for each pair of state and input symbols there may exist several possible next states. We notice with great interest that the Environments for Multiagent Systems (E4MAS) community has undertook an effort to accept the *environment* of a multi-agent system as a first-class entity, distinguishing indirect interaction via the environment from the environment role in message transport [8]. [7] define classes of interaction (sequential and multi-agent, direct and indirect) and environments (physical and virtual, persistent and amnesic, dynamic and static). These notions provide an underpinning for proper acknowledgement of the roles of MAS environments and for powerful MAS design techniques using indirect interaction.

3 Protection functions

We imagine a holonic, multi-level organisation of custodians, which will maintain and use an awareness base represented by the integration of models, environment sensing, and surveillance and control activities. In this section we discuss the range of functions supported by the surveillance and protection units, either in isolation or combined together. Each of the characteristics discussed below becomes more complex and sophisticated when the organizational level of each holonic unit grows.

Perception Several passive and active sensor systems may be integrated, including video surveillance [9], access control (transponder, smartcard, RFID, etc.), intrusion detection (sound, infrared, etc.), sensing of environmental components (fumes, fire, humidity, temperature, concentration of pollutants, etc.). Direct sensor fusion provides better information by combining data provided by homogeneous or heterogeneous sensors [10]. Indirect sensor fusion enforces the process by using a priori knowledge about the scene and its environment. A statistically clustered history is assumed to be available. Furthermore, a hypothesis of known scene is also assumed to hold, where a solid model of the surrounding environment is always available, at the appropriate level of detail.

Computation A holonic architecture has to support distributed, fault-tolerant, real-time, non-stop applications. It should even supports hot swapping of programs, so that the code of some agents can be changed without stopping the system. The actor model has been used both as a framework for a theoretical understanding of concurrency, and as a basis for several practical implementations of concurrent systems. An actor can (a) make local decisions, (b) create other actors, (c) send and receive messages, and (d) determine how to respond to received messages. The actor model provides the easiest approach to agent-based computing, a computational model for simulating the actions and interactions of autonomous entities and individuals, which affect the system as a whole. In our holonic architecture the agents (often called *holons* here) could either be software agents, humans, human teams or combined human-agent teams. Monte Carlo Methods are used to introduce randomness.

Visualization According to the holonic architecture of the security platform and its strong 3D orientation, each holon will be provided with appropriate information visualization tools, ranging from graphical displays on mobile handsets held by security agents, to single workstations and service hubs dislocated in key points of the security network, up to wall-panel displays in the control room(s). Visualization tools of virtual and augmented scenes will be mainly used for training the security personnel, and for displaying in a realistic way the results of simulations needed to support the decision makers during a crisis. The visualization tools may display highly realistic views of the rendered scene using a combination of advanced graphics techniques. For each location they will provide both visual and verbal directions on how to approach the selected destination. The main problem in the realistic visualization of virtual environments is the low quality of the (local) lighting models employed, since the Gouraud/Phong model used by graphics hardware is too simplistic, the number of light sources is usually too low, and there is no interaction between reflecting surfaces, that should conversely integrate perfectly into real scenes, that is to say without visual discontinuity and with adaptive tone mapping.

Interaction The protection platform has a holonic architecture where each holon is autonomous within its defined limits, takes care of a defined portion of the infrastructure, and must be able to alert and communicate, in all circumstances, with the stakeholders of the controlled scene. All stakeholders involved in security and safety can communicate with any level of the monitoring platform, being aware that the controlled scene (and the impact of their decisions) grows generally bigger as the interface level gets higher. Accredited people will be able to access any detail of the awareness base, as required by the dinamics of the situation. The protection platform will provide:

1. the capability of planning all the activities of the security personnel, for both normal situations and emergencies;
2. the capability of planning the frequentation patterns [11] of people for normal situations, and the escape procedures in case of emergencies;
3. full awareness of the aspects of the situation that can impact security and safety of the infrastructure, of the people involved and of its surroundings;
4. means of communicating as efficiently as possible (given the situation) with the personnel and the public involved.

Information security Enforcing information security is a fundamental property for a holonic system whose purpose is to protect critical infrastructures. Every security failure in a single component may result in a security breach or crack of the security system and, as a consequence, of the critical infrastructure. Consequently, each holon must be protected with state-of-the-art security technology, in particular with mutual authentication of agents, machines, processes and services. Several ICT infrastructures, and most private companies, attempt to use firewalls to solve network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a bad assumption. Most of computer crimes are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict the use of the Internet. The restrictions of network functionality imposed by firewalls are often both unrealistic and unacceptable. Therefore, we assume network connections to be insecure.

Geometric reasoning Spatial models play a key role when interpreting a dynamic and uncertain world for a surveillance application. In particular, [12], in "Spatial Models for Wide-Area Visual Surveillance: Computational Approaches and Spatial Building-Blocks", chooses the *cellular decompositive representation* of the space as the most promising spatial primitive to support visual surveillance applications. This paper discusses also the necessity to associate a semantics to the hierarchical elements of the spatial subdivision.

To satisfy these requirements, we use the geometric language PLaSM for generating and handling contained geometric information contained in our holonic security architecture. PLaSM (Programming LAnguage for Solid Modeling) is strongly influenced by FL (programming at Function Level), the approach to functional programming [14, 15] developed by the Functional Programming Group leaded by John Backus and John Williams at the IBM Research Division in Almaden in the early nineties. PLaSM provides the full power of a Turing-complete programming language, with support for conditional, recursion, higher-level functional abstraction, etc. Moreover, it is multidimensional by design, a property that enhances its expressive power and allows very terse definitions of highly complex models.

Logic reasoning The assessment of static and dynamic knowledge requires an extensive use of the self-consciousness provided by geometric models of the infrastructure and by dynamic patterns of usage [11] derived from sensor systems. Each holon must learn which configurations of its controlled scene are good, acceptable or to be avoided in order to enforce safety and security for scene's stakeholders and users. This knowledge, again represented by models, involves security protocols, use of new technologies, procedures, etc., and has to evolve in relation to the changes of the social and physical environment. Therefore, a basic requirement for the effectiveness of the security platform is that these models be distributed and integrated as much as possible, because in case of emergencies a prompt response to events is critical and automatic or shortcut reactions can make the difference. In particular, we imagine a multi-level holonic organization of both software and human custodians, which maintains and uses an awareness base that integrates models, environment sensing, surveillance and control activities. By awareness we mean the capability of having, in all situations, a clear view of what is happening, a history of past events, forecasts of future events, simulations of possible scenarios. Such *knowledge in perspective* of the present situation, its precursors and its possible outcomes, maximises the possibility of control.

Simulation Living organisms learn through a trial-and-error process, which leads to optimized internal representations and simulations of the environment, which are in turn a consequence of the environmental configurations. Some models are inherited, some are developed during lifetime. This learning process never ends, as the environment evolves and changes. The unconscious, and successful, assumption of this survival mechanism is that even if events are all different from each other, there are similarities and categorizations that allow an organism to infer the evolution of events, while they are happening, on the base of experience. A concept central to the security platform is therefore to enhance as much as possible its modeling capabilities, since all the supports provided are based on model-based simulations. In order to simulate the behavior of an environment, the basic activity is modeling all the objects, actions, actors, that in any way influence the behavior of the environment itself. Through the capability of simulating all kinds of events and all actions and reactions that may animate the environment, the platform will be capable of maintaining the controlled infrastructure, as much as possible, in an optimally secured state for its users and for the management personnel. The platform will also provide all possible support to security enforcing personnel, in case of situations that exceed its capability of automatic management.

Operation command and control A programmable geometric platform is, in our opinion, the best candidate to integrate, through the digital model of the infrastructure, the various vision, sensor and security systems committed to security and protection. It is needed to embody a self-consiousness in the intelligence center devoted to security command and control, to continuously acquire permanent information and perform a continuous information treatment for the detection of alert situations, as well as to simulate normal and abnormal behaviors of the infrastructure and to plan both standard security procedures and appropriate reactions to abnormal events. Last but not least, VR and gaming techniques founded on geometric information may be very useful both to train security forces and to improve operational procedures.

In this holonic, multi-level control structure, the custodian agents will be structured in teams, and in teams of teams: in this way the organization will be scalable to any size. Each team or single custodian controls a portion of the infrastructure, and/or exercises a specific technology. The stakeholders, i.e., the people responsible for security and safety, communicate with all levels of this monitoring structure. Security personnel activities will be performed across the entire structure, on the base of *routine* and *emergency process plans*, and directed by an *Operation and Control Center* (OCC). In this respect, human-controlled activities will work as an orchestration of the Software Agents, whose autonomy will be greatly reduced, leaving people in complete control of the situation. People will be able to communicate with any level of the system, and to access all details of the awareness base.

4 Advanced interfaces for mobile information supports

The instruments provided are grouped into a number of *metaphorical tools*, which are named here *Newspaper*, *Agenda*, *Map*, *Telephone* and *TV*. Flexible interface methods will properly port each logical instrument to the physical interaction device (mobile hand-set display, computer display, video monitor, wall panel display), accounting for their different sizes and interaction capabilities.

The Newspaper The newspaper tool collects the knowledge gained over time of the different aspects relevant to the security of the infrastructure. As it happens in a real newspaper, there will be sections where the most recent events are categorized, described and commented (in terms, e.g., of efficiency and effectiveness of specific interventions), sections for a meditated analysis of specific situations, sections with the near-future events planned within the infrastructure, with the relevant security enforcing plans, sections with forecasts of mid- and long-term future events, and so on. Exactly as in a newspaper, these sections will have recalls on the first page and extensions in internal pages, so that any user may navigate in depth and bredth according to her needs. The visualization will employ the most vivid and effective interaction modalities available, including advanced interfaces for video-gaming.

The Agenda The agenda tool represents the chronicle of what is going to happen, and contains notes and comments about situations, decisions, and so on. Each event, once closed, is logged as history, ready for further analyses. There will be a general Agenda of the entire infrastructure, and an individual one for each Holon or decision-maker in charge of the security management.

The Map The map tool represents the infrastructure and its context, i.e., the stage where events happen, activities are planned, simulations are run. In comparison with a typical GIS map, this tool will feature various important extensions. In particular, most common descriptions of the real world use drawings, symbols and operational patterns, all of which require abstraction and interpretation skill to produce a mental image of reality. For several purposes, such a symbolic representation may result too complex, hard to manage and ineffective when a crisis calls for a prompt reaction. As we all know, the humans are accustomed to live and move in a three-dimensional world, not in a flatland made of 2D drawings and schemes. Augmented reality may visualize hyper-realistic aspects of the infrastructure, e.g., the presence of an anomalous temperature gradient or of a microwave field.

The Telephone The telephone tool includes all the communication means of the control network, incorporating automatic devices (cameras, sensors, actuators) and all the people and offices involved in security management, inside the Infrastructure and outside of it (fire brigades, the police, etc.). In all situations the Platform will screen the lists and maps of the communication partners that need to be reached for help, alert, etc.

The TV The TV tool will collect the video-deduced knowledge, putting it in a spatial perspective. For this purpose it is possible to present a multiple-camera system—instantly switchable upon the mouse-click of a OCC operator—either as an intelligent composite viewpoint or as a mosaic-like multi-sensor viewpoint, for each presumed-threat event. Among the innovative aspects of the TV tool there is the 3D modelling of the video surveillance inputs. This feature is realized while maintaining the multiple viewpoint proposition, which is also important when trying to understand and react quickly to a rapidly evolving emergency situation.

5 Intelligent video surveillance

Surveillance systems consist of three main elements: Data acquisition, Information analysis, and On-Field Operation. Large surveillance systems acquire data from hundreds of networked cameras. With an increasing number of cameras and other data sensors, Information Analysis becomes increasingly difficult. Human operators can easily get overwhelmed by a flood of unorganized visual information, and they may fail to effectively inform On-Field operations in an effective way. The use of conventional user interfaces and fixed video display matrices is no longer sufficient, due to the increasingly large scale and complexity of the information flow [16]. The available screen resources and operator attention needs to be empowered in a subtler, semantically richer and more interactive way [17].

Furthermore, today's cutting edge surveillance systems perform very well [9] in relatively vacant environments. In an underpopulated scenario, people, vehicles and other objects can be easily tracked without a robust treatment of occlusions and of complex scene dynamics. However, as the monitored environment gets crowded, which is usually the case in transport infrastructures, these systems tend to fail and the accuracy and reliability of the surveillance systems dramatically deteriorate.

The holonic architecture of our security platform is aimed at integrating the video surveillance in a way that will make the video surveillance an independent subsystem that can be implemented, modified or substituted by providing the integration, modification o substitution of interfaces to 3D modeling and knowledge base. Video surveillance subsystem shall permanently refer to the 3D model of the infrastructure, in order to be able to switch between the two representation as desired or useful (e.g., because of smoke, blackout, tracking a subject outside the camera field, etc.). Intelligent video surveillance subsystems capable of detecting and analyzing events and abnormal behaviors will work in a stand-alone mode and pass detected alerts to the knowledge base. The video surveillance encoders will form a resilient inter-networked framework, fully and automatically redundant within itself, remotely managed and controlled. The video information originating from many sources will be distributed over the network to Operation Control Center (OCC) stations, equipped with video displays or desktop monitors, and simultaneously archived for offline analysis.

6 Automatic generation of digital 3D models

Our geometric modeling and reasoning is based on BSP (Binary Space Partition) generated cellular decomposition of buildings from architectural plans. The paradigmatic reference is to PLM (Product Lifecycle Management), where geometric information provides the exchange/collaboration layer shared by all business departments and all product data. A VR representation of whatever infrastructural part may be of interest, progressively generating higher levels of detail, may be produced at runtime by a streaming data-flow process.

A fast semi-automatic solution was already experimented, and can be summarized as follows. Input line-drawings of 2D architectural plans are transformed into proper data structures, in order to answer proximity queries in an efficient way. Then semantics is assigned to small subsets of lines, via pattern-based recognition of the components of the building fabric (internal partitions, external enclosures, vertical communication elements, etc.), and subsequent translation into PLaSM scripts, i.e., symbolic generating forms. Later, the evaluation of symbolic scripts produces either streaming solid models at variable levels of detail or adjacency graphs of the critical infrastructure as a whole or of parts thereof [18].

To achieve our purpose we capitalized on a novel parallel technology [19, 20] for high-performance solid and geometric modeling, that (i) compiles the generating expression of the model into a dataflow network of concurrent threads, and (ii) splits the model into fragments to be distributed among different computational nodes and independently generated. Progressive BSP trees are used by [20] for adaptive and parallelizable streaming dataflow evaluation of geometric expressions. They are associated to the polyhedral cells of the HPC (Hierarchical Polyhedral Complex) data structure used by the language. Hasse graphs are used to maintain a complete representation of topology. [21] associate an Hasse graph to a new tensorial representation of the chain complex mock-up, namely the Hasse matrix.

7 Conclusion

The enormous size and complexity of modern surveillance scenarios generates a tremendous stream of data. The use of conventional user interfaces and fixed video display matrices appears no longer satisfactory, due to the increasingly large scale of the information flow. Therefore, the available screen estate and operator attention need to be empowered in subtler, semantically richer and interactive ways. To this end, advanced computer graphics and state-of-the-art user interfaces are of paramount importance. Skills from visual perception, 3D interactive computer graphics, Virtual Reality and Serious Games are closely integrated.

The central feature of our security platform is the design and the maintenance of software holons acting as a *Community of Custodians*. This community will embody the intelligence of the infrastructure, i.e., all the activities of sensing, operating devices, alerting security personnel, and so on. In particular,it makes up a holonic multi-scale organization, which maintains and uses an awareness base integrating both behavioral models and environmental sensing data and supports surveillance and control activities.

References

1. Gell-Mann, M.: What is complexity? Complexity **1**(1) (1995) 16–19

2. Complex Systems Society (CSS). http://css.csregistry.orghttp://css.csregistry.org.
3. Dooley, K.: A complex adaptive systems model of organization change. Nonlinear Dynamics, Psychology, & Life Science **1**(1) (1997) 69–97
4. Waldrop, M.M.: Complexity: The Emerging Science at the Edge of Order and Chaos. Simon & Schuster, New York, NY (1993)
5. Hilaire, V., Koukam, A., Rodriguez, S.: An adaptive agent architecture for holonic multi-agent systems. ACM Trans. Auton. Adapt. Syst. **3**(1) (2008) 1–24
6. Koestler, A.: The ghost in the machine. Arkana, London, UK (1967)
7. Keil, D., Goldin, D.: Indirect interaction in environments for multiagent systems. In Weyns, D., Parunak, V., Michel, F., eds.: Environments for Multiagent Systems II. Volume 3830 of Lecture Notes in Computer Science. Springer, New York, NY (2006)
8. Weyns, D., Van Dyke Parunak, H., Michel, F.: Environments for Multi-Agent Systems II. Volume 3830 of Lecture Notes in Computer Science. Springer, New York, NY (2006).
9. Koschan, A., Pollefeys, M., Abidi, M. In: 3D Imaging for Safety and Security. Volume 35 of Computational Imaging and Vision. Springer, New York, NY (2007)
10. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. Wiley, Chichester, UK (2003) 2nd Edition.
11. Rueda, L., Mery, D., Kittler, J. In: Progress in Pattern Recognition, Image Analysis and Applications. Volume 4756 of Lecture Notes in Computer Science. Springer, New York, NY (2007)
12. Howarth, R.J.: Spatial models for wide-area visual surveillance: Computational approaches and spatial building-blocks. Artif. Intell. Rev. **23**(2) (2005) 97–155
13. Paoluzzi, A.: Geometric Programming for Computer Aided Design. John Wiley & Sons, Chicester, UK (2003)
14. Backus, J., Williams, J.H., Wimmers, E.L.: An introduction to the programming language FL. In: Research topics in functional programming. Addison-Wesley Longman Publ., Boston, MA, USA (1990) 219–247
15. Aiken, A., Williams, J.H., Wimmers, E.L.: The FL project: The design of a functional language (1991) Unpublished report.
16. Sebe, I.O., Hu, J., You, S., Neumann, U.: 3d video surveillance with augmented virtual environments. In: IWVS '03: First ACM SIGMM international workshop on Video surveillance, New York, NY, USA, ACM Press (2003) 107–112
17. Girgensohn, A., Kimber, D., Vaughan, J., Yang, T., Shipman, F., Turner, T., Rieffel, E., Wilcox, L., Chen, F., Dunnigan, T.: DOTS: support for effective video surveillance. In: MULTIMEDIA '07: Proceedings of the 15th international conference on Multimedia, New York, NY, USA, Acm (2007) 423–432
18. Paoluzzi, A., Scorzelli, G.: Pattern-driven mapping from architectural plans to solid models of buildings. In: Israel-Italy Bi-National Conf. on Shape Modeling and Reasoning for Industrial and Biomedical Appl., Haifa, Israel, Technion (2007)
19. Bajaj, C., Paoluzzi, A., Scorzelli, G.: Progressive conversion from B-rep to BSP for streaming geometric modeling. Computer-Aided Design and Applications **3**(5 (6)) (2006).
20. Scorzelli, G., Paoluzzi, A., Pascucci, V.: Parallel solid modeling using BSP dataflow. Journal of Computational Geometry and Applications **17** (2007) To appear.
21. DiCarlo, A., Milicchio, F., Paoluzzi, A., Shapiro, V.: Solid and physical modeling with (co)chain complexes. In: SPM '07: Proceedings on the second ACM symposium on Solid and Physical modeling, New York, NY, USA, ACM Press (2007)