eNetworks in an Increasingly Volatile World: Design for Resilience of Networked Critical Infrastructures

Mihaela Ulieru
Canada Research Chair
Faculty of Computer Science
The University of New Brunswick
CANADA
Ulieru@unb.ca
http://www.cs.unb.ca/~ulieru/

Abstract.** Any critical infrastructure is controlled and managed by networked information and communication technologies (ICT) systems. Tremendous progress in the emerging area of ubiquitous, pervasive and tangible computing enables hardware and software to be integrated to a degree that makes possible a technological revolution in which ICT systems merged with physical infrastructure will be transformed together into a vast intelligence network, called an 'eNetwork'. eNetworks are the 'nervous system' of interdependent critical infrastructures and as such are the 'the weakest link'. We introduce a novel approach to building resilient critical supply networks of any kind (electricity, water, gas, finances, materials and products, etc). The proposed approach endows the eNetworked infrastructure with self-awareness such that it is able to identify possible threats or emerging vulnerabilities and reconfigure itself to attain resilience to both accidental failures and malicious attacks. By using natural models of emergence, much in the same manner that DNA is controlled in genetic engineering, we will be able to control the emergence of a network configuration resilient to anticipated threats before they manifest. The novelty consists in the integration of context-aware modelling as a tool for controlling the clustering mechanism through which the eNetwork self-organizes its services to tune its resilience according to the dynamics of the occurring situation. A significant step forward in the area of complexity science this novel approach enables a major breakthrough in the way we interact with the surrounding environment and physical world. Resilient eNetworks open perspectives unthinkable before on how to approach major technological, economic, societal and ecological problems of international concern, such as blackout-free electricity generation and distribution, optimization of energy consumption, networked transportation and manufacturing, disaster response, efficient agriculture, environmental monitoring, financial risk and sustainability assessment.

Keywords. Complex adaptive systems, Emergence and self-organization, Ubiquitous computing, Design for resilience, Infrastructure interdependencies, Agent-based modeling and simulation, Threat anticipation modeling, Adaptive risk management, Cyber-physical systems, Networked embedded control systems.

Introduction

The aim of our modern human society is its safe permanent and sustainable development. A Critical Infrastructure supports the orderly functioning of the society and economy at large. For that reason, it is of utmost importance that these Critical Infrastructures are both functional (efficient and powerful) and *reliable*. Networked ICT systems (which we coin as 'eNetworks') have pervaded in all traditional infrastructures, rendering them more intelligent but more vulnerable at the same time. Physical infrastructures' efficiency often depends on monitoring and control by eNetworks, which usually have high levels of automation and remote controlled functionalities. Additionally, at a higher level, many complex networks are managed by man, and their performance finally depends on man's organizational performance, which is the most susceptible to failure. Networks are generally linked together and the services offered to or requested from a single network are dependent on other interdependent networks: as a consequence we do not have to deal with single isolated systems but with *systems of systems* [Rinaldi 2001]. Identifying all potential vulnerability of such systems and finding solutions to reduce the failure probability become very difficult and ambitious tasks [Heller, 1999].

There are three types of *interdependent networks* in today's critical infrastructure [CNIP 2006], [Brown 2004]:

- Supply networks: transportation grids for electrical power, oil and gas; water distribution networks; transport/road tunnel systems; production flow supply chains; health care systems.
- Cyber-networks: tele-control and SCADA (Supervisory Control and Data Acquisition) networks, e-banking/finance networks, etc.
- Managerial/organization networks where human resources supervise and/or utilize the services delivered by the above systems.

The 'Internet of the Future' (as coined in the EU FP 7 Future and Emerging Technologies Program [IST 2007]) is envisioned to go through a radical transformation from how we know it today (a mere communication highway) into a vast *hybrid network* seamlessly integrating physical (mobile or static) devices with distributed sensing and actuation, communications, storage and computation mechanisms to power, control or operate virtually any device, appliance or system/infrastructure. Manipulation of the physical world occurs locally but control and observability are enabled safely and securely across a virtual network. (It is this emerging ‘hybrid network’ that we refer to as an ‘eNetwork’.) Resonant with this radically new vision, the US National Science Foundation’s new Cyberengineering Research program [NSF, 2006] approaches the future Internet as a *networked embedded control system*, referred to as ‘Cyber-(Physical) System’. A cyber-physical system integrates computing, communication and storage capabilities with the monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time.

eNetworks are envisioned to seamlessly pervade all traditional infrastructures, rendering them more intelligent but more vulnerable at the same time [ICIIP 2006]. Given that all other critical infrastructures depend on them, eNetworks are emerging as the weakest link in systems of critical infrastructure [Balkowich 2004]. The destruction of eNetworks systems or the degradation / disruption of their services would have a serious impact on health, safety, security, economy, and government, therefore it is essential that eNetworks are designed to be efficient, powerful and reliable [Gill 2006].

Objectives

In line with this emerging need we aim to develop generic methodologies of design for resilience of critical infrastructures in which the eNetwork middleware will continuously self-organize to adapt the resilience of the infrastructure accordingly as vulnerabilities and threats emerge. We build on previous experience in developing adaptive information infrastructures and adaptive risk management strategies following three streams of research briefly described below.

Stream 1: Network self-organization to preserve/increase resilience. The goal is to develop self-healing and reconfiguration methodologies integrated into a framework in which services flowing through eNetworks are able to organize themselves (and the eNetwork) in a resilient system without requiring any manual intervention by performing short-term adaptations to the environment as well as long-term evolution of new self-healing functionalities. **Research questions**:

- What are the global properties that are important for self-management, self-optimization, self-monitoring, self-repair, and self-protection (self-* properties) in large and complex networks?
- How do local and random or individually motivated connections between nodes affect the global properties of the resulting network?
- How do abrupt changes in global properties result as a consequence of gradual changes in the parameters that characterize the policy of local connections?
- Which patterns of large scale network evolution can be exploited to ensure network scalability?

Stream 2: Risk Mitigation via eNetworks. The goal is to endow eNetworks with the ability to quickly evaluate system vulnerability with respect to potential threats / undesirable events. We aim at a methodology of design for anticipation in networked intelligent surveillance systems for the security of critical infrastructures. **Research questions**:

- What methods and tools can capture, clarify, and predict the undesirable evolution of an eNetwork controlled infrastructure?
- How can threat anticipation be incorporated into models of complex network dynamics?
- Can maximal efficiency during normal operations of eNetworked infrastructures be balanced with resiliency, sustainability, and minimal vulnerability to common and catastrophic failures?

Stream 3: Impact of Interdependencies. The goal is to develop a strategy for resources allocation (such as sensor networks and mobile devices) to discover vulnerabilities in distinct components of the eNetworked infrastructure. **Research questions**:

- How can interdependencies be captured between the eNetwork and the controlled infrastructure?
- How and from where can the information be appropriately collected considering the interdependent topology and structural vulnerability of the network of networks, to anticipate an attack on the supported infrastructure?
- How can situational awareness be enhanced by providing an integrated view of high quality contextual information to support decision making by combining relevant information from multiple disparate sources?

By following these streamlines in the long run we aim to discover new frameworks for understanding eNetworked systems of infrastructure systems and methodologies for designing and operating these in a way that provides the best trade-off in terms of efficiency, vulnerability, resiliency, and other competing objectives, under normal and disrupted conditions. By taking into account the multifaceted dimensions of interdependencies and risks in such large scale systems of systems, these designs will endow interdependent infrastructures with intrinsic resilience, without human intervention, while continuously notifying them of the status quo.

State of The Art

Many infrastructure systems (e.g., power, transportation, and telecommunications) are complex adaptive systems [Brown 2004], [CNIP 2006] [Rinaldi 2001], that is, their collective, systemic behaviour is emergent (i.e., it follows patterns that result, yet are not analytically predictable from, dynamic, nonlinear, spatiotemporal interactions among a large number of components or subsystems). CASs are adaptive in that the capabilities of components and decision rules change over time in response to interactions with other components and external interventions [Gell-Mann, 1994]. Because a CAS is greater than the sum of its parts, the system can only be described at levels higher than the components. The size and frequency of electricity disturbances, for instance, obey the power law, a characteristic of complex systems at the critical edge between order and chaos [Amin, 2001]. This feature, known as the small-world (SW) [Watts, 1999] property, is shared by most real networks, involving a high degree of interconnectedness both at local and global level (Fig. 1).

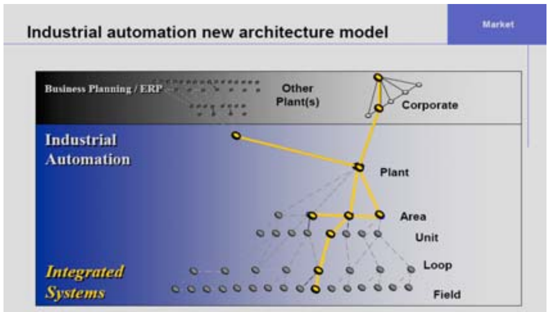

Fig. 1: ‘Small-World property in networks as foundation for Networked Embedded Control Systems

That is, for every node, most nodes close to it should also be close to each other (high clustering coefficient), and every pair of nodes is separated, on the average by a number of links that grows at most logarithmically with the network size (small diameter). One effective way to investigate complex adaptive systems is to view them as populations of interacting agents [Holland 1998]. Multi-Agent Systems (MAS) are emerging as the most promising modeling techniques for predicting, controlling, and optimizing infrastructure systems [CNIP 2006]. While no single agent knows how to tackle the entire problem, the knowledge is “distributed” across the system, such that in case of a sudden dysfunction at some node (e.g. collapse or attack) it can be easily removed from the network with its functionality seamlessly taken over by the other nodes [Ulieru and Worthington 2005].

Agent-based CAS approaches, which are being used to represent both the physics and finances of highly fluid, interdependent markets, have captured the interplay among economic and societal factors and the operation of multiple infrastructures [North 2000]. Extensible actor-based software frameworks for the modelling, simulation, and analysis of interdependent infrastructures are also being developed [Heller, 2001]. Other approaches, such as those based on the Leontief economic model, compute flows of commodities and shared risks among sectors [Haimes 2001]. None of these approaches capture emergent behaviour, a key element of interdependency analysis.

In Europe the Critical Information Infrastructure Research Co-ordination (CI2RCO,http://www.ci2rco.org) aims to establish a European Research Area (ERA) on CIIP as part of the larger Information Society Technologies (IST) Within this the CRUTIAL project, *CRitical UTility InfrastructurAL Resilience*(http://crutial.cesiricerca.it/default.asp), addresses new networked ICT systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet. GRID (http://grid.jrc.it/) is a co-ordination action funded by the IST programme within the 6th European Framework Programme, to achieve consensus on the key issues involved by power system vulnerabilities and the relevant defence methodologies, in view of the challenges driven by the transformation of the European power infrastructure. The aim of *Highly DEpendable IP-based NETworks and Services* (HIDENETS, http://www.hidenets.aau.dk/hidenets) specific targeted research project is to develop and analyze end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. The new European project IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems, http://www.irriis.org) aims at increasing the dependability and resilience of Large Complex Critical Infrastructures (LCCIs) by introducing appropriate Middleware Improved Technology (MIT) based on Information and Communication Technology (ICT). ReSIST (Resilience for Survivability in IST, http://www2.laas.fr/RESIST/index.html) is a Network of Excellence (NoE) integrating leading researchers active in the multidisciplinary domains of dependability, security, and human factors.

Also noteworthy are the efforts made by the Digital Ecosystems Consortium [http://www.digital-ecosystems.org/] to develop a complex conceptual framework for Enterprise Networking for describing the interactions between firms, technology, and knowledge inspired by biological ecosystems. They suggest self-organization and evolutionary models from biology to be applied to software, based on the assumption that such “biological” behaviour of the software, if attained, is likely to optimize the catalytic function of the ICTs in question for socio-economic growth and innovation.

This current state of the art is the point of departure to advance the latest discoveries in the three research streams as follows:

Stream 1: Network self-organization to preserve/increase resilience. Barabassi and others have identified what appears to be a set of rules governing the emergent behavior of all large scale networks [Barabasi and Albert 1999], [Petermann 2006]. Based on these rules one can identify patterns of self-organization in large scale complex networks based on which anticipation of system’s evolution (emergence) can be realized [Caldarelli 2006]. [Kauffmann 2000] has shown that self-regulatory networks of DNA structures in cellular biology obey similar patterns of emergence, which drive evolution in addition to natural selection. For holonic supply networks in manufacturing, Fig. 2 [Ulieru and Cobzaru 2005], we have independently demonstrated [Ulieru 2002] that complex networks self-organize according to the laws of complex adaptive systems [Ulieru 2005].

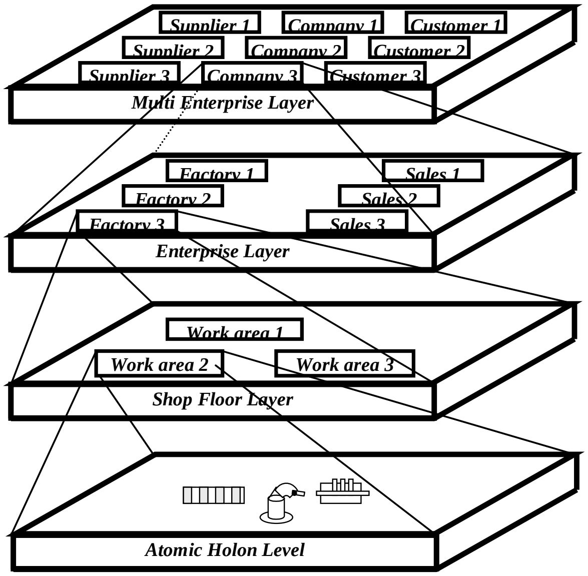

Fig. 2: Holonic Supply Network (Manufacturing Holarchy)

Recent advances in ubiquitous computing envision context awareness mechanisms to self-organize intelligent environments (consisting of autonomic appliances and artifacts) according to user intent detection and analysis [Heider and Kirste 2005], while context-aware supply networks are being developed to model workflow processes as digital ecosystems [Zanet 2006].

Stream 2: Risk Mitigation via eNetworks. The volatility of today's socio-economic and political dynamics renders obsolete the current 'post-attack' approaches to critical supply network security [SCADA 2006]. With a focus on system protection against known attacks through quick detection and relief of major impact incidence, such approaches use pre-developed system restoration plans to minimize the impact of disruption [Dondossola 2006]. Current system security assessment methodologies are unsatisfactory. Protective devices are typically ignored in steady-state or dynamic security assessment. System dynamics are rarely evaluated in real-time. System restoration relies primarily on human operators and off-line procedures; technology serves mainly as a supervisory control and data acquisition tool. Latest advances in Cyberengineering [NSF 2006] open new possibilities for including anticipation into multidimensional risk models [Gill, 2006].

Stream 3: Impact of Interdependencies. Current approaches to critical infrastructure protection that include the effect of interdependencies [CNIP 2006] are still unable to adapt the network resilience to unexpected/unknown effects/attacks. Complex networks have 'critical hubs' [Barabassi 2002] in that disruption of their functionality unavoidably leads to network collapse. Acting on such 'critical hubs' of self-regulatory networks in cellular biology [Zhang 2006], a mechanism of drug design can be envisioned to cure illnesses such as cancer. The drug destroys cancerous cell networks by attacking their critical hubs [Kauffman 2000]. We want to use a similar mechanism to anticipate attacks and annihilate attack propagation on eNetworked critical infrastructure.

Methods and proposed approach

To balance the tension between the need to push our civil infrastructure systems to higher levels of efficiency and competitiveness and the need to ensure minimum levels of service, reliability, and security, even under critical conditions we propose an adaptive holarchy [Ulieru 2005] with ability to tune the degree of autonomy of holons at various levels through a context-model which measures the degree of risk and accordingly tunes the autonomy level to keep the infrastructure safe [Ulieru and Grobbelaar, 2006].

Stream 1: Network self-organization to preserve/increase resilience. What is required is a paradigm shift in confronting the complexity explosion problem to enable building robust holarchic networked infrastructures that are self-organizing and self-repairing. We draw inspiration from biological processes and mechanisms to develop strategies for designing robust, self-organizing and adaptive holarchies as ensembles of autonomous agents. The idea is to ensure the premises for the network to evolve into predefined patterns by setting certain parameters (such as weights in the mathematical models [Barratt, 2005]) at the microlevel and as such to control network's evolution at the macrolevel (as such to control emergence of particular, good behaviour patterns while avoiding the destructive ones). This would keep the complex network in a safety zone in case of unexpected disturbances (such as e.g. a local blackout in a power network) – and by this an intrinsic resilience is built into the network. What renders this approach particularly attractive from a dynamic network perspective is that global properties like adaptation, self-organization and robustness are achieved without explicitly programming them into the individual artificial agents. Yet, given large ensembles of agents, the global behaviour is surprisingly adaptive and can cope with arbitrary initial conditions, unforeseen scenarios, variations in the environment or presence of deviant agents.

Stream 2: Risk Mitigation via eNetworks. Our approach will make a radical shift from the current stream by looking at the security of eNetworked critical infrastructures from an ***anticipative*** perspective. To induce immunity into the eNetwork we propose the following 'vaccine': A hybrid mixture of static and mobile (physical and software) agents with an underlining *holonic self-organization mechanism* will be injected into the eNetwork to continuously monitor the status of the critical nodes (hubs). The vaccine will behave like an artificial ant colony [Ulieru and Grobbelaar 2006] in which the source of an attack is tracked, much like ants track food sources, by specialized agents who leave informational traces (artificial pheromones) to announce the attack throughout the eNetwork [Foukia 2005]. Evolution and adaptation for survivability in such complex (biological) systems that are able to work in the absence of central control and to exploit local interactions will be extracted into patterns of design for resilience of fully integrated network and service environments that scale to large amounts of heterogeneous devices, and that are able to adapt and evolve in an autonomic way [Carrera 2006]. Our approach is original in that it combines the latest trends in context-aware supply networks [Zanet 2006] with the latest ideas in implementing self-organizing sensor networks [Di Pietro, 2006] and the holonic paradigm [Ulieru 2005]. A resilient eNetworked infrastructure would consist of holons navigating the supply network (via the eNetwork) to monitor and detect any suspicious changes that could lead to an undesirable effect [Georgiadis, 2005]. The eNetwork would self-organize in appropriate resilience patterns using novel a context-awareness mechanism [Ulieru and Grobbelaar 2006] envisioned to tune the autonomy across the holarchic levels according to the detected/anticipated intent of eventual malicious holons.

Using context models, instead of anticipating the intent of the user (which triggers self-organization of an intelligent environment [Heider and Kirste 2005] to meet the user need in ambient intelligence applications) we perform *intent analysis* on other *agents/resources* (holons) that are part of the eNetwork (such as mobile devices including the software that operates the eNetwork) as well as on holons from and/or interfering with the supported infrastructure to be monitored (such as sensors, sensor networks or devices such as a power generator or a powered 'intelligent' home appliance). Instead of 'user intent' triggering the appropriate reaction of an intelligent appliance or environment, the eventual *malicious intent* of an 'agent'/holon (physical or software) will trigger annihilation mechanisms that will act at the critical hubs to protect them against the eventual intrusion. This will anticipate and annihilate malicious intents before they manifest, ensuring the eNetworked critical infrastructure is 'immune'.

Stream 3: Impact of Interdependencies. We integrate latest advances in the evolution of complex networks topology [Fisher 2005] with latest findings in infrastructure interdependencies [CNIP 2006] to model the complex dynamics of critical hubs emergence under various threats. Such dynamics will be encapsulated in control algorithms that will act on critical hubs as they evolve towards criticality before the catastrophic effects occur [Barabasi 2002]. Through proactive monitoring strategies, every critical hub in the eNetwork is alerted at the first sign of an eventual malicious intent, triggering fighter agents that specialize in eliminating attackers similar to how antibodies fight viruses in biological systems. As such, the eNetwork will behave like a *cyberorganism* that reacts to attacks in the same way as the immune system reacts to protect biological organisms. The drawback of false alarms is tackled via a thorough risk assessment threshold mechanism [Ulieru 2006].

Conclusions and Impact

Resilient eNetworks can revolutionize a wide range of safety and security applications, such as: blackout-free electricity generation and distribution; terrorist network interception and annihilation [Vidyasagar, 2005]; interception of and defence against biochemical attacks (e.g. using dedicated sensor networks capable of long range detection of various agents; buildings equipped with safety mechanisms, for example, automatically shutting off air conditioning if a biochemical attack is detected); hazard free transportation (automotive networks for aerospace and avionics); disaster response and pandemic mitigation (public notification systems, evacuation and rescue operations coordination).

Success in the proposed research will lead to a major breakthrough in the way we interact with the surrounding environment and physical world, opening perspectives unthinkable before on how to approach major societal and ecological problems, such as: **forecasting long term sustainability and resilience of life on our planet** – e.g., by identifying and modeling interdependencies between climate change, economic (natural resource) scarcity, ecological and environmental influences, including the potential to design eNetworks to monitor such changes to anticipate their trends and impact on mankind's future; **monitoring the evolution of global interdependent economies and markets** – e.g. , by detecting intentional risk through network analysis of global capital flows.

References

[Amin, 2001] Amin, M., EPRI/DoD Complex Interactive Networks/Systems Initiative, Workshop on Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures, Alexandria Research Institute, September 10-11, 2001. Available online at <http://www.ari.vt.edu/workshop>.

[Balkowich 2004] Balkovich, E. E., R.H. Anderson, Critical Infrastructures Will Remain Vulnerable: Neighborhoods Must Fend for Themselves, International Journal of Critical Infrastructures, Vol. 1, No.1 pp. 8 – 19.

[Barabasi and Albert 1999] Barabasi A-L and R Albert. Emergence of scaling in random networks. Science, 286, 509–512.

[Barabassi 2002] Barabassi A-L, Linked: The New Science of Networks, Perseus Publishing ISBN 0-7382-0667-9

[Barrat, 2005] A. Barrat, M. Barthelemy, A. Vespignani. The effects of spatial constraints in the evolution of weighted complex networks. J. Stat. Mech. (2005) P05003.

[Brown 2004] Brown, V. A., Beyeler, T., and Barton, D. W., Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems, Int. J. Critical Infrastructures, Vol. 1, No. 1, pp.108–117.

[Carreras 2006] Carreras I, I Chlamtac, F De Pellegrini and D Miorandi , "BIONETS: Bio-Inspired Networking for Pervasive Communication Environments" IEEE Transactions on Vehicular Technologies, vol. 55, n. 6, Nov. 2006

[Caldarelli et al 2006] Caldarelli, G, Capocci, A and D. Garlaschelli, Self–organized network evolution coupled to extremal dynamics, http://delis.upb.de/paper/DELIS-TR-0410.pdf

[CNIP 2006] International Workshop on Complex Networks and Infrastructure Protection, March 28-29, 2006, Rome, Italy. http://ciip.casaccia.enea.it/cnip06/

[Dondossola 2006] Dondossola G, O. Lamquet, Cyber Risk Assessment in the Electric Power Industry, Cigrè Electra Magazine n. 224, February 2006.

[Fisher 2005] Fischer, S and B. Vöcking Adaptive Routing with Stale Information, Proc. 24th ACM SIGACT-SIGOPS Symp. on Principles of Distributed Computing, Las Vegas 2005, pp 276--283

[Foukia 2005] Foukia N. IDReAM: Intrusion Detection and Response executed with Agent Mobility Architecture and Implementation, Proceedings AAMAS 2005 pp. 264-270

[Gell-Mann, 1994] Gell-Mann, M. Complex adaptive systems. Pp. 17-28 in Complexity: Metaphors, Models and Reality, G.A. Cowan, D. Pines, and D. Meltzer, eds. Reading, Mass.: Addison-Wesley

[Georgiadis, 2005] G. Georgiadis and L.M. Kirousis Lightweight centrality measures in networks under attack. In: Proc. European Conference on Complex Systems 2005.

[Heider and Kirste 2005] Heider T and T Kirste, Evoking Smart Environments from ad-hoc Ensembles with Explicit Goals, Kunstliche Intelligenz 19(3): 17- (2005)

[Gill 2006] Gill H, M Ilic, B Krogh, B Martin and S Sastry, Terms of Reference for the Workshop 'Beyond SCADA: Networked Embedded Control Systems', November 8-9, 2006 Pittsburgh, Pennsylvania

[ICIIP 2006] International Critical Information Infrastructure Protection Handbook 2006, Dunn M and V Mauer(Eds) ETH Zurich, Switzerland ISBN 3-905696-08-8

[IST 2006] Workshop on Resilient Infrastructures and Information Fusion for Security, EU IST Event 2006, November 21-23, 2006 Helsinki, Finland

[IST 2007] http://cordis.europa.eu/ist/fet

[Haimes 2001] Haimes, Y.Y, and P. Jiang. 2001. Leontief-based model of risk in complex interconnected infrastructures. ASCE Journal of Infrastructure Systems 7(1):1-12.

[Heller 1999] Heller, M., E.W. von Sacken, and R.L. Gerstberger, Water utilities as integrated businesses. Journal of the American Waterworks Association 91(11):72-83.

[Holland 1998] Holland J, Emergence: From Chaos to Order, Perseus Books ISBN 0-201-14943-5

[Kauffman 2000] Kauffman, S., Investigations, Oxford Univ Press,ISBN 0-19-512104-X

[NSF 2006] NSF Workshop on Cyber-Physical Systems, Austin, Texas, October 16-17 2006 (http://varma.ece.cmu.edu/cps/CFP.htm)

[North, 2000] North, M.J. 2000. An Agent-Based Tool for Infrastructure Interdependency Policy Analysis. Rand Workshop on Complex Systems and Policy Analysis: New Tools for a New Millennium, Washington, D.C., September 28, 2000 <http://www.rand.org/scitech/stpi/Complexity/>.

[Petermann 2006] Petermann, T and De Los Rios, P., Physical realizability of small-world networks, Physical Review E 73, 026114 /2006.

[DiPietro 2006] Di Pietro, R., Mancini, L. V., Mei, A. Panocnesi, A and J. Radhakrishnan, How to Design Connected Sensor Networks that Are Provably Secure, Proceedings of SecureComm 2006, the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks

[Rinaldi 2001] Rinaldi S M, J P Peerenboom, T K Kelly, Identifying, understanding and analyzing critical infrastructures interdependencies, IEEE Control Systems Magazine, Dec. 2001, pp. 11-25.

[SCADA 2006] Proceedings of the 2006 Process Control and SCADA Security Summit, September 28-30, 2006, Las Vegas.

[Ulieru, 2002] Mihaela Ulieru, "Emergence of Holonic Enterprises from Multi-Agent Systems: A Fuzzy-Evolutionary Approach", Invited Chapter in *Soft Computing Agents: A New Perspective on Dynamic Information Systems*, (V. Loia – Editor), IOS Press -Frontiers in AI and Applications Series 2002, ISBN 1 58603 292 5, pp. 187-215.

[Ulieru and Unland 2004] Mihaela Ulieru and Rainer Unland, Emergent e-Logistics Infrastructure for Timely Emergency Response Management, in *Engineering Self-Organizing Systems: Nature Inspired Approaches to Software Engineering*, Di Marzo Serugendo et.al. (Eds.) Springer, Berlin 2004, ISBN 3-540-21201-9, pp. 139-156

[Ulieru, 2005] Mihaela Ulieru, Adaptive Information Infrastructures for the e-Society, in *Engineering Self-Organizing Systems: Methods and Applications*, Giovanna DiMarzo Serugendo and Anthony Karageorgios (Eds.) Springer Verlag – LNAI 3464, Berlin 2005, ISBN: 3-540-26180-X , pp. 32-51.

[Ulieru and Cobzaru 2005] Ulieru, M. and Cobzaru, M. "Building Holonic Supply Chain Management Systems: An e-Logistics Application for the Telephone Manufacturing Industry", *IEEE Transactions on Industrial Informatics*, Vol1, No. 1, Feb. 2005, pp. 18-31

[Ulieru 2006] Mihaela Ulieru and Paul Worthington: "Adaptive Risk Management System for Critical Infrastructure Protection"; Special Issue on Autonomic Computing in Engineering in *Integrated Computer-Aided Engineering*; ISSN: 1069-2509; IOS Press; volume: 13:1 Jan 2006, pp. 63-80.

[Ulieru and Grobbelaar, 2006] Mihaela Ulieru and Stefan Grobbelaar, Holonic Stigmergy as a Mechanism for Engineering Self-Organizing Applications, ICINCO 2006 – 3rd International Conference of Informatics in Control, Automation and Robotics, August 1-5, 2006, Setubal, Portugal, pp. 5-10

[Vidyasagar, 2005] Vidyasagar Potdar, Muhammad A Khan, Elizabeth Chang, Paul Worthington and Mihaela Ulieru, e-Forensics Steganography System for Terrorist Information Retrieval, *Advanced Engineering Informatics*, Volume 19, Issue 3, July 2005, pp. 235-241

[Zanet 2006] Zanet, M.: Context-aware Information Propagation in Supply Chains, ICE'06, 26.-28, 2006, Milan, Italy, June 2006

[Zhang, 2006] Zhang L., C A Athale and T S Deisboeck, Development of a three-dimensional multiscale agent-based tumor model, Journal of Theoretical Biology.July 27, 2006 PMID: 16949103

[Watts, 1999] D.J. Watts Small Worlds Princeton University Press, 1999