Enabling the SOS Network

Mihaela Ulieru
Canada Research Chair
The Univerisity of New Brunswick
Fredericton, Canada
http://www.cs.unb.ca/~ulieru/

Abstract - **This work introduces the concept of Self-Organizing Security (SOS) network as a resilient architectural foundation on which the operational mechanism for deploying dynamic, short living emergency response organizations capable to react quickly to emerging crisis situations can be evolved. A simulation Testbed for SOS networks is presented that balances micromanagement of subordinates with the excessive independence of commanders based on a trusted overall operational picture shared via a joint communications backbone. Built on the foundation of the recently introduced *Emergent Engineering* paradigm, the SOS Testbed delivers a picture of the dynamics of emerging trends that enable decision makers to anticipate the evolution of emerging crises and evaluate the effectiveness of different inter-agency configurations coming together in addressing it. Hints towards a 'change of culture' shifting first responders operations from the traditional hierarchical towards a 'power to the edge' heterarchy point to policy changes that allow emerging leaders to take action in the 'chaos of crisis'. The strategies proposed increase the responsiveness and effectiveness of first responder meta-organizations thus reducing the vulnerabilities to asymmetric threats to increase the safety quotient and by this the social resilience in today's convoluted world dynamics.**

Keywords - **Network Enabled Operations (NEOps), Emergency Response Management, Evolving Crisis, Emergent Engineering, Asymmetric Threat Anticipation, Decentralized Command and Control, Holistic Security Ecosystem**

I. INTRODUCTION

The new security challenges of the 21st century are qualitatively different than in the past, as new networked organizational structure of threatening parties-with many groups actually being leaderless-and their quickness in coming together in swarming attacks requires more dynamic collaborative approaches to counteracting measures. To confront this new type of conflict, response shall encompass harmonious inter-organizational coordination across a *holistic security ecosystem* [1] to achieve a total effect greater than the sum of the individual parts. The kind of integration, responsiveness and adaptability needed to meet these requirements is best achievable through Network Enabled Operations (NEOps) [2] which is defined as "An evolving concept aimed at improving the planning and execution of operations through the seamless sharing of data, information and communications technology to link people, processes and ad-hoc networks in order to facilitate effective and timely interaction between sensors, leaders and effects". NEOps would enable joint first responder organizations to be effective and adaptive, capable of providing tactical, proportional response to specific situations thus opening new possibilities to deploy units or teams as agile groupings – which we refer to as SOS – Self-Organizing Security – networks. SOS networks are dynamic, short lived *meta-organizations* deployed 'on the fly' from units belonging to different organizations (military forces, police, firefighters, ambulance, provincial emergency response organizations, red cross and other non-government organizations, etc.) coming together in a collaborative endeavor to address an emerging need (an acute and developing crisis situation). SOS networks bring agility to the joint first responder forces via the NEOps communications backbone - to facilitate a common information environment that would allow people, sensors and systems to be dynamically grouped or configured according to particular mission requirements.

The SOS framework requires an optimized sharing of information, teamwork and a collaborative working environment. Currently, these activities are very often not valued in the first responder organizations (including the military) nearly as much as individual accomplishments. Moreover, the current culture needs to progress towards increased interdependence between national first responder organizations while maintaining or increasing interoperability with international security partners. While the popular view indicates that collaboration is usually better than solo problem solving, it may not be all that simple when it comes to decision making and problem solving within newly formed, hybrid and agile first responder teams of individuals coming from different organizational cultures and training backgrounds – having sometimes conflicting success metrics (e.g. military vs. red cross). There is a time-information trade-off between the cognitive speed, agility, surprise, and adaptability that comes from individual decision-making

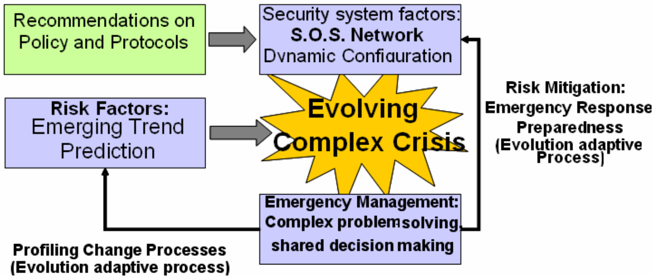
Recommendations on Policy and Protocols
Security system factors: S.O.S. Network Dynamic Configuration
Risk Factors: Emerging Trend Prediction
Evolving Complex Crisis
Risk Mitigation: Emergency Response Preparedness (Evolution adaptive Process)
Emergency Management: Complex problemsolving shared decision making
Profiling Change Processes (Evolution adaptive process)

Fig. 1 – Elements of a controller capable of containing an evolving crisis

versus the quality of decisions informed by the views of members of a team. This triggers a need to consider collective vs. individual problem solving when trying to maximize anticipation, reaction speed, opportunism, and fast adaptation in the case of an emerging crisis.

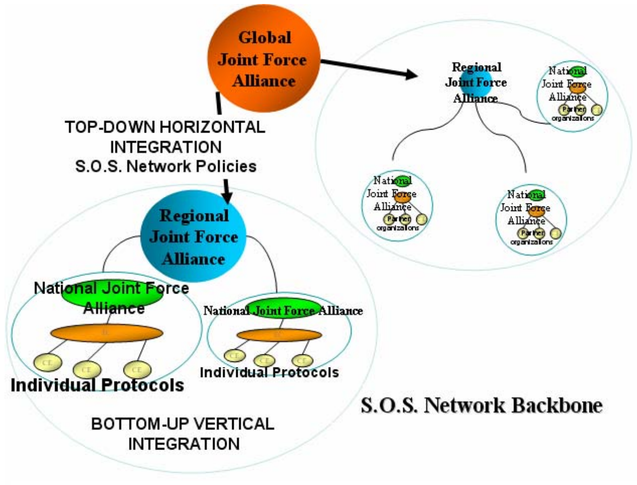
Global Joint Force Alliance
TOP-DOWN HORIZONTAL INTEGRATION
S.O.S. Network Policies
Regional Joint Force Alliance
National Joint Force Alliance
National Joint Force Alliance
Individual Protocols
Individual Protocols
BOTTOM-UP VERTICAL INTEGRATION
S.O.S. Network Backbone
Regional Joint Force Alliance
National Joint Force Alliance
Partner organizations

Fig. 2 – SOS as 'nervous system' controlling the crisis

This work is concerned with the vision, design and development of an an ***SOS simulation test bed*** that will contribute to a change of inter- and intra- organizational policies to ease the way toward teaming into a *joint response alliance (JRA)* which exploits the latest advances in communication networks and services to enable cross-border (organizational, polytical, national and geographycal) productive collaboration in dealing with acute and developing crisis situations. The JRA acts as a controller for the evolving crisis, Fig. 1 deployed on the SOS network regarded as a 'nervous system', Fig. 2 that co-evolves with the crisis to regulate the emerging processes while deploying ad-hoc protective mechanisms similar to how anti-bodies are being created to fight unexpected/unanticipated intrusions. The foundational principles fueling this SOS nervous system are detailed in [3]. As an overarching simulation modeling capability, the SOS testbed is envisioned to capture social, cognitive and information conceptual factors into a *complex systems approach to security systems dynamics* [1] for the purpose of assessing meta-organisational decision-making structures, practices and processes.

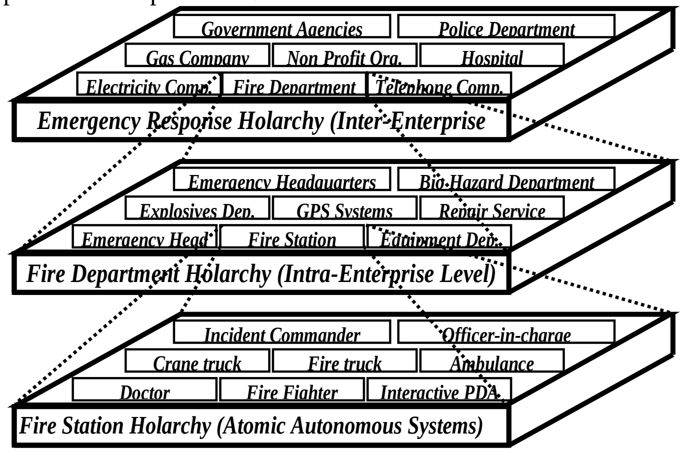

Fig. 3 – Snapshot into an SOS Network instance represented as a holarchy

II. BACKGROUND

The key characteristic of an SOS network (Fig. 3) is the ability to rapidly "pick, plug, and play" processes to configure for meeting an unexpected situation [4]. One might regard an SOS network as an *expectant web* of participants ready to jump into action (pick) and combine rapidly (plug) to meet the requirements of the specific situation (play) [5]. On completion, the participants are dispersed to "rest" while, perhaps, being active in other endeavors including their normal operations outside the SOS network. In this regard when responding to an unforeseen problem SOS networks exhibit a *collective behavior* much in the same manner as swarms self-organize [6] by simple individuals interacting locally with one another and with their environment without centralized control [3]. Such systems can be modeled using the Agent-Based Modeling and Simulation (ABMS) paradigm [7] with each individual modeled as an agent and their interactions modeled as links. With this, an SOS Network equates a *network of agents* interacting intensely with each-other in generating a collective behavior that co-evolves with the environmental dynamics. Usually this imposes certain constraints on the overall network of agents – constraints encapsulated in a higher strategy, a high-level policy enabling the undertaking of concrete action plans that would adapt to the crisis dynamics. To realize this, the high-level policies (termed *overall rules of the network* [8]) will materialize into concrete action plans that have to be broadcast on the fly and compiled down into local rules transmitted to all agents involved in addressing the particular complex situation. The individual-to-collective dynamics (how the agents create the collective behavior through the way they interact/influence each-other) in such a network depends on the particular action plan desired. Thus balancing individual protocols with the network policies to achieve a best possible collective meta-organizational behavior resulted in action plans deployed across the SOS network becomes the key issue when deploying emergency operations.

The collective dynamics resulted from the tensions between network policies and the protocols ruling the individual agent actions can – in view of the Cybernetics school [9] - be represented as an overarching Command (feed-forward) and Control (feed-back) - C2 – backbone, Fig. 2 – acting as a 'nervous system' that regulates individual behaviors to maximize the overall network goal (e.g. under the constraints imposed by the network policies. Thus an SOS network can be regarded as a holarchy (Fig. 3) with a highly adaptive Command and Control (C2) founded on collaborative distributed working skills [8]. This points to the crucial role the C2 network logic (protocols and policies) have on either facilitating or obstructing collaboration across the SOS network.

III. THE C2 MECHANISMS OF AN SOS NETWORK

A. Power to the Emerging Leaders

When selected, the network participants must be able to *interoperate*: they must be 'plugged together' via rules governing the architecture for mixing and matching them to enable the required network outcome. The concepts of architecture and protocol are completely compatible with the challenge of developing new ways to organize human effort [8]. For example, regarding the architectural design space, within a military organization the standard architectural framework has been the *control hierarchy* with its hierarchic authorizations protocol. However in the 'chaos of crisis' the behaviors of groups / teams of first responders do not simplify sufficiently to be controlled by individuals. Instead of a progressive simplification from an individual to larger and larger collections of individuals along the traditional hierarchy, the dynamics is characterized by an increasing complexity that is tied to an increasing complexity of the demands of the (crisis) environment. This makes it impossible for an individual to effectively control collective behavior in such a situation [10].

The 'robustly networked organization' paradigm shift was suggested in [11] through the *power to the edge principle*, which implies that the power of decision is vested primarily with the lowest level elements-those at the edge, away from the power centers. This decentralization of authority approach opens the possibility of implementing an agile organization that 'self-organizes' around the needs of an evolving crisis through *emerging leaders* creating operational units as the situation demands.

B. Balancing SOS Network Policies with Individual Protocols

Our purpose is to develop SOS network policies that build 'synergetic togetherness' across the participants coming together from various organizations to solve emerging problems. Each SOS network participant organization has specific capabilities captured in its own policies as well as in the protocols which define the individual roles within the organization. Traditionally, when such participants combine they create *interfaces* between capabilities to negotiate among the various organizational policies – let alone for the myriad of individual protocols. This acts as a barrier impeding the rapid configuration 'pick, plug, and play' process to meet a timely objective. What we want to achieve is for our SOS network to be able to have the end-to-end management of processes running flexibly across many different organizations in many different forms. The central idea of our approach is that linking partners is on the basis of linking processes while allowing *individual execution* according to those processes. The ABMS approach to our SOS network implementation realizes this via orchestration and choreography [12] of the processes that run across the multi-agent system, following latest Web 2.0 advances to balance the individual protocols at the agent level with the overall network policies. The SOS network policy is implemented using a multi-agent software middleware platform that enables the coordination of inter-organizational interactions via remote process execution and management. The C2 coordination mechanism separates process from execution, acting in the background according to the governance rules of the SOS network – while the individuals coming together from their specific military and civilian units are following their own specific protocols in a goal-seeking self-organizing swarm. It is the balance between the rules at the *microscopic* level of the agents (the 'genotype' aka their individual protocols – in our SOS example) and the overall *macroscopic* behavior of the collectivity (the resulted phenotype – aka the SOS network mediating the policies across all organizations that are hosts for the deployed individual agents to create action plans appropriate for managing the particular situation) that guides the emergence of appropriate action plans for dealing with the crisis most effectively. Relatively complex behavior can therefore result from balancing the genotype – the simple agent-based rules that encode positive feedback - with the phenotype - overall rules of the system that result in the adaptive action plans - by adjusting the individual behavior to the overall goal of the network of agents via negative feedback. This equates with balancing autonomy of the individual agents with the need to cooperate to achieve the overall goal of the system, in a holonic enterprise [13].

3.3. Co-evolving the SOS Network with the Emerging Crisis

One major challenge in our undertaking stems from the fact that - in order to be able to deploy the appropriate action plans by timely, dynamically and appropriately structuring and re-structuring the SOS Network - both the task of “meta-designing” the generative laws of architectural development for the controller that would lead to a desired structure (for the SOS ‘barriers’) to result from the elementary agent interactions, and the task of determining the controller *functionality* (to grow those barriers timely as per the emerging needs of the unfolding crisis) - have to be done in parallel – as they both depend on each-other and in addition they depend on the environmental dynamics (crisis evolution). Thus the network architecture is continuously evolving and adapting to the crisis dynamics to grow the kind of barriers to developing attacks that can attain the functionality that would enable best possible containment of the attacks as they dynamically occur. After reaching structural maturation (possibly on a short “deployment” time scale under high dynamics – aka when the joint teams are deployed in response to the particular malicious event), the SOS network would switch the bulk of its activity from executing the *developmental part* of the genotype (***dynamic architecting*** by positioning the actors within the network such that they can perform their activity best within the team) to executing the *functional part* of the genotype (***adaptive control*** achieved by acting their roles within the team as per their specified individual protocols to realize the most effective action plans).

Once the basic ‘eNetwork DNA’ parameters (genotype and phenotype rules) have been set to achieve the SOS network growth (architecture) and function (control), the remaining question is how to achieve the SOS network *co-evolution* with the developing crisis [3]. This can be done by specifying how the genotype (individual agent rules) *varies* (randomly) and how the phenotype (overall network policies that enable the selection and deployment of appropriate action plans) is *selected* (non-randomly). For our SOS Network example, the more elaborate the genotype (individual agent behaviours), the richer the variety of the overall phenotype (range of action plans that can emerge - aka be dynamically deployed - from the guided individual behaviours). This is because an elaborate genotype opens the door to agent *differentiation*, which allows combinations and recombination of diverse agents into modules and hierarchical constructions – thus evolving architectural structures that can be targeted at certain function (creating barriers to contain attacks or guiding the crowds towards safety in case of an SOS network, as per the example presented in Section IV). This balance – between the ‘freedom’ of the genotype and the functional constraints imposed by the phenotype – enables the SOS Network continuous adaptation to the dynamics of the otherwise impossible to manage / control complex situation / chaos of crisis.

IV. SIMULATION MODELING TESTBED

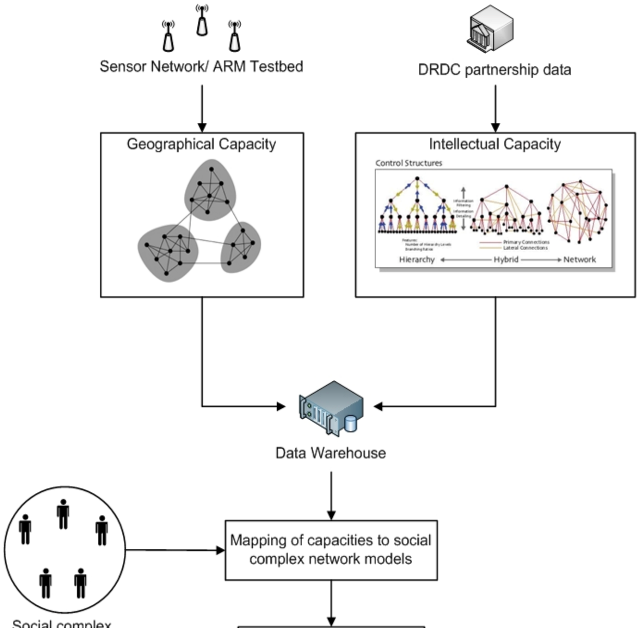

Fig. 4: Holistic Security Ecosystem Simulation Testbed

The Testbed, Fig. 4 - described in detail in [1] – is founded on an emergent engineering software platform described in detail in [3] – which, based on the triad P (port), G (gradient), L (link) (Fig. 5a) can grow barriers to attacks that co-evolve with the crisis dynamics as per Fig. 5b, where e.g. a cordon of first responders evolved to isolate a threat while two chains of first responders emerged to guide the crowds to safety in an ‘Olympic Stadium’ possible scenario – which is further detailed in Fig. 6.

The emergent engineering platform enables specification of the SOS Network functionality be relaxed to the point of being open to surprise and harvesting the useful <structure (architecture) / function (control)> pairs from a free-range “menagerie” of protocols/action plans configurations.

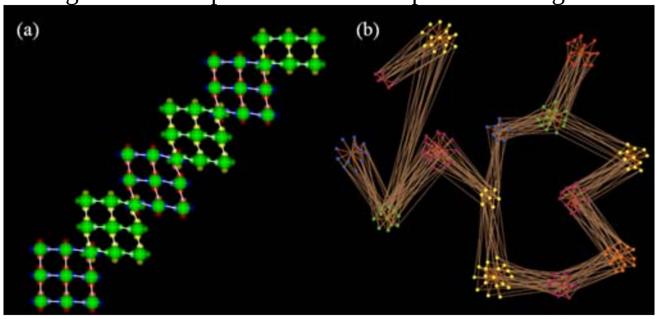

Figure 5: (a) Growth of branching 3×3 lattices attached by their corners via the (P,G,L) model. (b) Complex branching chain of node clusters – e.g. guiding the crowds to safety, and a cycle – e.g. containing the threat via a cordon of first responders.

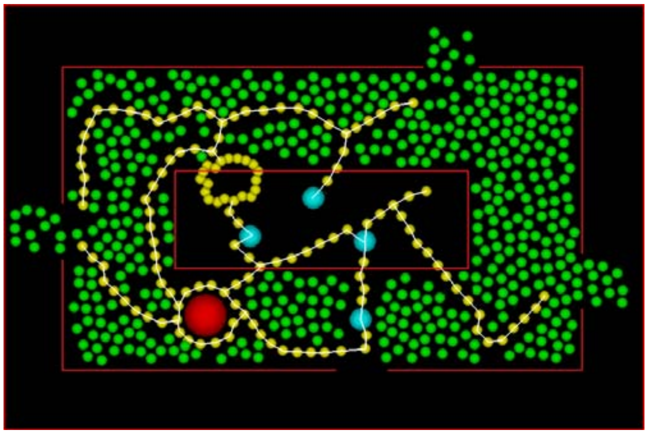

Figure 6: SOS scenario within the space of a stadium. Growing cordons of security agents (orange) encircle the threat (red), guide the crowd (green) toward the exits, carry victims to emergency vehicles (blue, driving in and out through gates under the bleachers), and create special enclosed spaces on the field (cycle).

With the Testbed we are currently exploring the effectiveness of SOS network deployment mechanisms through:

- experimentation and understanding of the high-level effects (resultant collective behaviour) at the SOS network (meta-organisational level) as they emerge from local interactions among the individual participants coming together from the various partnering organisations;
- the design of exercise scenarios involving various combinations of crises configurations to assess the JRA response and decide on most productive course of action; based on this - policy changes will be suggested for the organizations coming together;
- evaluation of the conflict between the individual protocols and the overall SOS network policies to determine the level of integration required to work effectively in a JRA team; based on the extent to which personnel can be educated into thinking and behaving cooperatively and collaboratively within and between mixed teams, decisions regarding changes to individual 'job protocols' assigned to individuals in the partnering organizations will be made.

V. CONCLUSIONS

This tool facilitates answers to the following major research questions:

- What are the key enablers and what is the expected benefit of an SOS approach to JRA?
- What are the major characteristics of SOS networks and how can they improve status quo in emergency response operations?
- How to capture the coordination logic over an SOS network using a MABS approach to implement this 'middleware' as an overarching operational layer that enables optimal synergy from the interactions of hybrid individual participants (agents)?
- What are the important trade-offs that must be analyzed and decided upon when choosing to transition from single organization operation to collaborative endeavor in enabling the ad-hoc creation of an SOS network as a meta-organization?

The success metrics of our work will be validated against the ability of the designed Testbed as an enabling tool capable of:

- pointing to indicators on changes to command, control and commander's intent in an SOS network environment, namely how much decentralization of decision making is possible, the conditions for this to happen and the limitations of decision making at various levels;
- emphasizing the most suitable organizational structures to facilitate devolved command and replacement of centralized and hierarchical structures with flexible and 'flatter' structures as required by specific crisis situations;
- pointing to appropriate *institutional policies* and *personnel protocols* according to which agile JRA groupings can be deployed.

ACKNOWLEDGEMENT

The author expresses highest gratitude to Dr. Paul Chouinard, Manager Security Operations Research at the Centre for Security Science of the Defence Research and Development (DRDC) Canada. Without his priceless insights this work would not have been possible. Figure 1 is a modified version of an initial brainstorming result credited to Dr. Chouinard – as it emerged from our numerous meetings and various cyber-discussions on the topic. Figures 5 and 6 are credited to my graduate student Adam MacDonald and my co-worker Rene Doursat – who developed the abstract model for emergent engineering and together with whom I have developed the example scenarios.

REFERENCES

[1] Mihaela Ulieru, A Complex Systems Approach to the Design and Evaluation of Holistic Security Ecosystems, International Conference on Complex Systems, Boston, MA, October 28-November 2, 2007

[2] Enemo, G., Analysis of Command and Control (C2) in Network Enabled Operations (NEOps), The Norwegian Defense Research Establishment, Kjeller, Norway - http://www.ima.org.uk/conflict/papers/Enemo.pdf

[3] Doursat, R. and M. Ulieru, Emergent Engineering for the Management of Complex Situations, Keynote Paper at Autonomics 2008, 2nd ACM Conf on Autonomic Computing and Communication Systems, Turin, Italy, Sept. 23-25, 2008

[4] van Heck, E., Preiss, K., and Pau, L-F. *Smart Business Networks*. Springer, Heidelberg-New York, 2005.

[5] 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 Verlag, Berlin 2004, ISBN 3-540-21201-9, pp. 139-156.

[6] Bonabeau, E. and Meyer, C., Swarm Intelligence: A whole way to think about business, *Harvard Business Review*, January 2008.

[7] North, M J and C M Macal, *Managing Business Complexity: Discovering Strategic Solutions with Agent-Based Modeling and Simulation*, Oxford University Press, Inc. 2007, New York..

[8] Ulieru, M. and Verdon, J. 2008. IT revolutions in the industry: From the command economy to the eNetworked industrial ecosystem. 1st International Workshop on Industrial Ecosystems, IEEE International Conference on Industrial Informatics (Daejoen, Korea, July 13-17, 2008).

[9] N. Wiener, Cybernetics: Control and communication in the animal and the machine. New York, NY: J. Wiley, 1948.

[10] Y. Bar-Yam, Complexity rising: From human beings to human civilization, a complexity profile, in *Encyclopedia of Life Support Systems* , Oxford, UK: EOLSS Publishers, 1997.

[11] Alberts and Hayes 2003 Albert, D. and Hayes, R. *Power to the Edge*: Command &Control in the Information Age, CCRP Publication Series 2003

[12] Peltz 2003 Peltz Chris, Web Services Orchestration and Coreography, SOA World Magazine, July 2003 http://soa.sys-con.com/node/39800

[13] Mihaela Ulieru, Robert Brennan and Scott Walker, The Holonic Enterprise – A Model for Internet-Enabled Global Supply Chain and Workflow Management, *International Journal of Integrated Manufacturing Systems*, No 13/8, 2002, ISSN 0957-6061, pp. 538-550