ADAPTIVE RISK MANAGEMENT SYSTEM (ARMS) FOR CRITICAL INFRASTRUCTURE PROTECTION

Mihaela Ulieru and Paul Worthington
Emergent Information Systems Laboratory
The University of Calgary
Ulieru@ucalgary.ca
http://www.enel.ucalgary.ca/People/Ulieru/

Abstract

The purpose of this work is to develop an adaptive risk management framework capable to prevent, identify and respond in critical time to threats. Our focus is on protecting critical infrastructure (e.g. public utilities) which vitally depends on network and information security. As solution we propose a holonic Cybersecurity system that unfolds into an emergency response management infrastructure capable to react in due time to unknown and new kinds of attacks/threats. The system can adapt to its changing environment through its self-organizing capability. Mimicking the way immunity works in biological organisms the system can dynamically adapt to embrace new risk situations and can dynamically create and learn new risk models as it encounters new risk situations.

Keywords. Risk management, holonic, self-organization, multi-agent systems.

1. Rationale

During the emergency response to the September 11, 2001 attack on the World Trade Centre, emergency response commanders on the scene were unable to communicate to '911' Public Service Access Points (PSAP) that people should evacuate the building. As a result, PSAP operators complied with New York City's standard operating procedure for hi-rise fires and advised callers to stay in impacted buildings [41]. The '911' system was inadequate for handling a major disaster and could not adapt to the emergency. The final death toll 2,749 may have been substantially reduced if the PSAP's were adaptive in coping with the overload.

Commanders trying to evacuate fire fighters from the north tower during the World Trade Centre disaster were seriously hampered by ineffective radio communications [43]; the final death toll 343 of New York fire fighters may also have been substantially reduced if the system controlling the radio communications was also adaptive.

According to Ward [42] Robert Prieto, chairman of New York City-based civil engineering firm Parsons Brinckerhoffrieto suggests that any system must be able to respond and adapt to a disaster in 3 ways.

- Resist - A system must be able to resist when loaded beyond its design basis, to fail in as safe a way as possible.

- Respond – A system when stressed beyond its point of resistance must be able to be reconfigured to allow some function to occur.

- Recover – A system must be able to be repaired or rebuilt following total failure. It is this phase that covers 'a host of considerations' including a vision that allows rebuilding with improved reliability, capacity and flexibility to cope with diverse and unpredictable future challenges. Such features of flexibility and coping with unpredictable future challenges are those exhibited by adaptive systems.

Business acumen today is also faced with increasing cost pressures, competitive markets, increasing information dependency, rapidly changing technology and an ever-increasing threat environment leading to a greater level of risk. Many risk management methodologies have been found to offer no more than a checklist approach with a monitoring phase included at the end.

Stoneburner, Goguen and Feringa [15] state "minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems".

As stated by Deloitte Touche Tohmatsu [5], "September 11th was the most destructive instance to date of a new reality—increasing threats of business interruption from a growing list of less predictable, often manmade, risks". The same source further states that several long-term trends that have generated important benefits have also made business operations more complex and vulnerable to disruption.
A recent survey by Deloitte Touche Tohmatsu [4] identified the following major key risk areas:

Failure to manage major projects	Failure of Strategy
Dependency on Key people	Business Interruption/Continuity
Failure to manage key external service providers/alliances	Economic conditions (including Interest/exchange risk
Information security	Failure to innovate
Political risks	Legal risks
Availability of capital/funding	Occupational health and safety
Failure to introduce new products/services	Ebusiness – getting it wrong
Ebusiness – missing the opportunities	New Competitors
Merger/Acquisition Risk	

As cited in the International Critical Infrastructure Protection Handbook [22] Figure 1, public utilities are seen as the hub of requiring critical infrastructure protection.

Arizona Water Resource [1] also agrees that public utilities are seen to have the greatest exposure and have imposed laws at federal and state levels to protect sensitive information deemed potentially dangerous if falling into the wrong hands.

Inherent in an information system are risks that must be managed with respect to design. In a survey by Crossland et al [3] of current practice in managing risk during the design process in sixty three UK design companies (a subset of risk management of information systems):

- 68% of the companies surveyed had formal operating procedures for managing project risk and 80% have formal operating procedures which explicitly include risk/reliability assessments for the designed entity.
- Qualitative techniques were more widely used to measure risk, with a strong emphasis on risk identification as opposed to quantification.

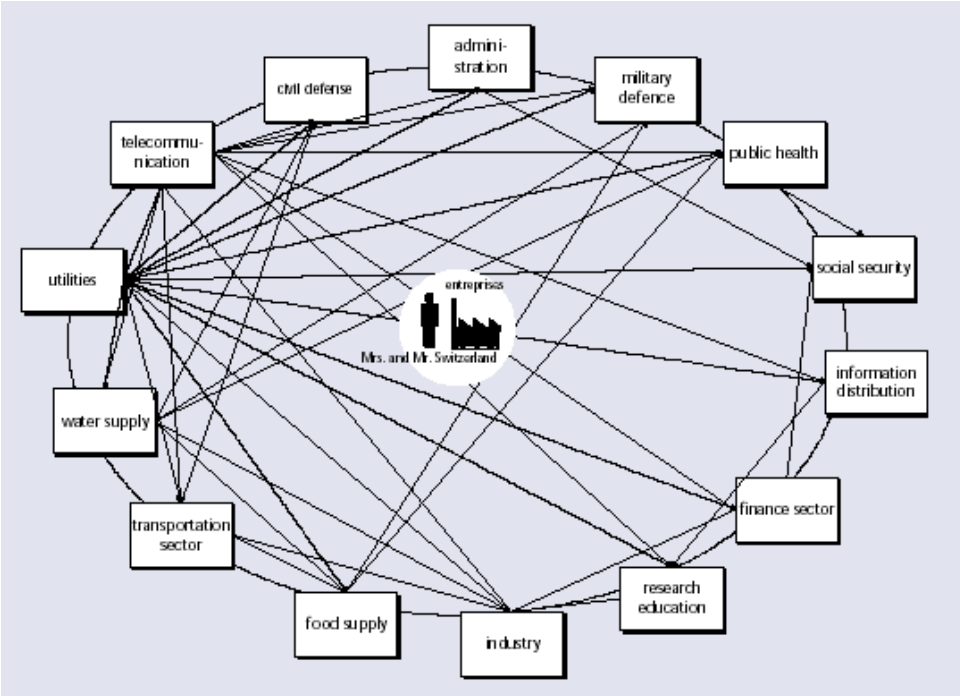


Figure 1: International Critical Infrastructure Protection Handbook [22]

Information systems facing rapidly changing technology and increasing information dependency must be able to adapt to changing needs of the organisation and changing risk within the information systems themselves. In response to this need we aim to develop an Adaptive Risk Management System (ARMS) that can:

- Identify various situations by matching them with a library of Risk Management Frameworks (RMF)s.
- Anticipate danger
- Detect a possible threat which does not match any of the known frameworks.

2. Risk Management for Critical Infrastructure

The phrase "risk management" has a broad definition and is applied in a number of diverse disciplines e.g. statistics, economics, psychology, social sciences, biology, engineering, toxicology, systems analysis, operations research, and decision theory. Each discipline associates a different meaning to the phrase. For psychology and social sciences it is the management of environmental risks, to technology professionals it is those technology generated risks that appear to threaten computer systems, to bankers it is the use of techniques to control monetary concerns, to insurance buyers and sellers it is the review of insurable risks and the reduction of costs (Carnegie Mellon Software Engineering [23]).

Sesel [24], states that the origins of risk management arose as a consequence to issues concerning the insurance industry in the 1970's. The major issue of concern was to protect against probable loss and disasters. There are many different approaches and methods of analyzing and managing risk but all have the central theme of thought, processes and action.

A simple definition of risk, as provided by the Association of Project Management [25] is the "process whereby decisions are made to accept known or assessed risks and/or the implementation of actions to reduce the consequences or probability of occurrence". The risk management process in itself may encompass as many as five different, but closely related, activities. The Sandia National Laboratories Energy, Information and Infrastructure Technology Division [26] has identified five different but closely related activities

(i) Identification of the hazards associated with a technical system or with potential solutions to a technical or non-technical problem.
(ii) Determination of the risks (i.e., the consequences and likelihoods) of those hazards.
(iii) Reduction of the risks to acceptable levels through appropriate design and control measures.
(iv) Thorough documentation of activities (i) through (iii).
(v)Continuing re evaluation (reiteration of steps i through iv) in order to improve the system or solution

No matter what definition, all activities or disciplines that choose to associate with risk management will deal with risks that have 3 components, namely an event, a probability of occurrence and an impact [27]. According to Foote [7] "a well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential capabilities" this will aid the management of the 3 components as outlined above.

The problem with risk management according to Kontio et al [12] is that "at best where problems are complex and involve various types of risk and commitments, risk management largely relies on intuition and luck except for the few organisations that have applied systematic risk management. Take the case of a head of an organizational unit that must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats.

2.1 Existing Risk Management Systems

Organizations are complex systems and for effective risk management, a systemic view is vital [37]. A systemic approach implies an interconnected complex of functionally related components. The effectiveness of each component relies on how it fits into the whole, and the effectiveness of the whole depends on the way each component functions. A systemic approach considers the larger environment that affects processes and other work. The environment includes inputs, but, more importantly, it includes pressures, expectations, constraints, and consequences. Moore proposes a cyclic systemic approach to risk management systems development (Fig. 2). It is important to distinguish a systemic approach from a systematic or process model.

Many existing risk management models and methodologies are found to be systematic. Webster's dictionary [38] defines a system that is characterized by order and planning as systematic. A systematic system is also formed with regular connection and relating to the design as a whole [39]. According to Wiegers [54], a barrier to effective process improvement or 'adaptive' behavior is the checklist mentality as exhibited by systematic models. As described by Fastenersources.com [40] a checklist is 'a tool used to ensure that all important steps or actions in an operation have been taken'.

A process model 'captures the essence of the system being configured and developed' and 'ensures that the user's perception and needs are appropriately understood and accounted for within the model' [44]. According to the American Society for Training & Development Linking People, Learning and Performance [37], a process model contains inputs and outputs and has feedback loops.

Below a historical perspective of "risk management" and examples of existing systems are shown.

According to Sesel [24], Canada developed a 'risk management standard in the early 1990's' and in 1995 a group of leading business thinkers developed the Australian and New Zealand Standard for risk management - AS/NZS 4360:1995 [28]. This last mentioned standard has received a wide degree of international interest and is widely used as a guideline for implementing risk management.

Newport News Shipbuilding [29] also shows a risk management plan process that identifies the process required to perform risk management.

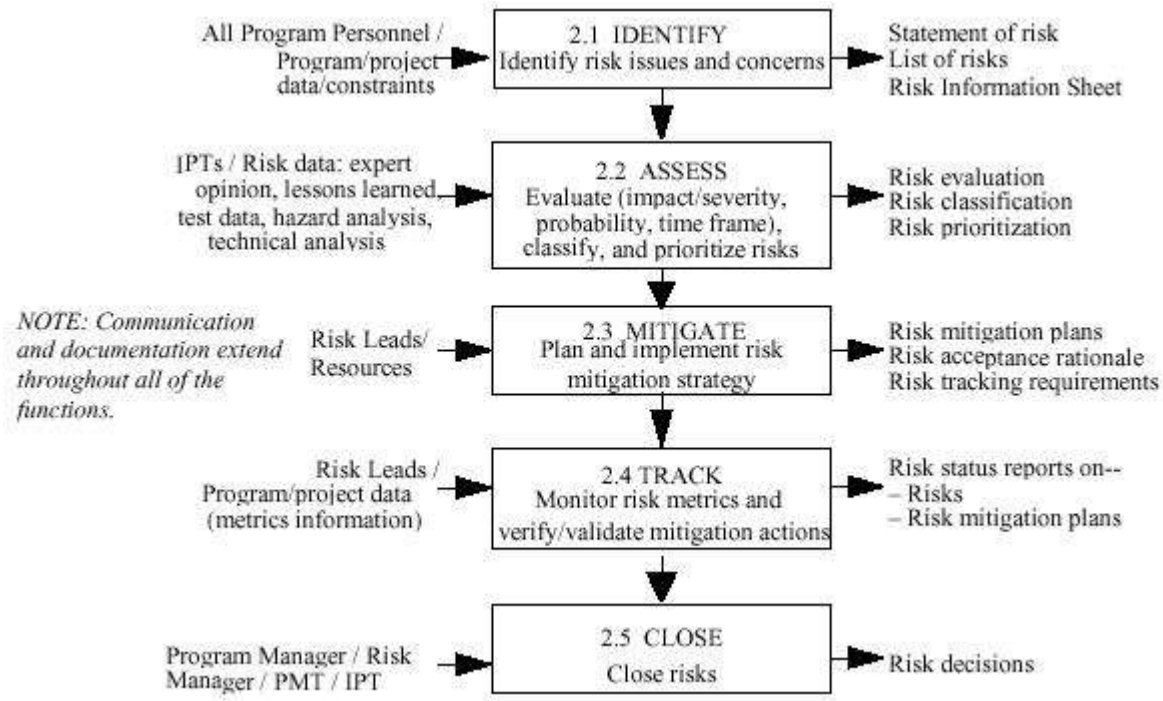


Fig. 2: Risk Management Cycle (from Moore, 1998 [32])

Standards Australia [30] adds monitoring and review / communication and consultation steps to implement feedback into the cycle to provide continuous monitoring (Fig. 3), but specifics to monitor and review are at best based on intuition as identified by Kontio et al [12].

.

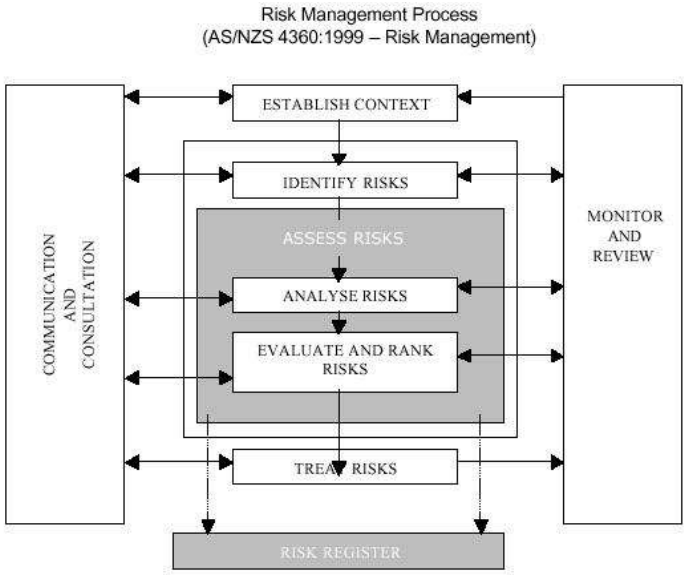


Figure 3: Australian/New Zealand Standard for Risk Management (AS/NZS 4360: 1999) [28]

According to the U.S. Department of Defence – Risk Management Plan Template and Guide [2], the following steps depict the risk management process steps (Fig. 4):

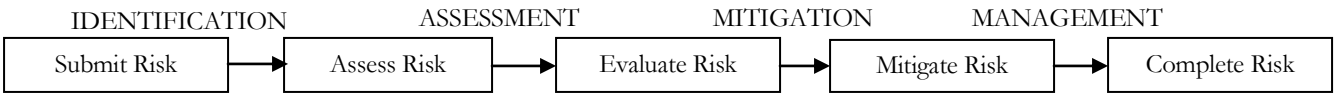


Figure 4: Department of Defence [2] Risk Management Process Steps

This attempt offers no more than a series of steps with no identifiable feedback for each of the activities.

Sandia National Laboratories [9] states "the nation increasingly relies on a complex, interdependent infrastructure for its security and well being" and uses the system depicted in Fig. 5 to deal with increasing complexities. The figure below shows a simple continuous loop for development of mechanisms, assessing vulnerabilities and assessing system risks but does not provide feedback loops in each assessment as to whether the outcome was achieved effectively or if another approach should be adopted.

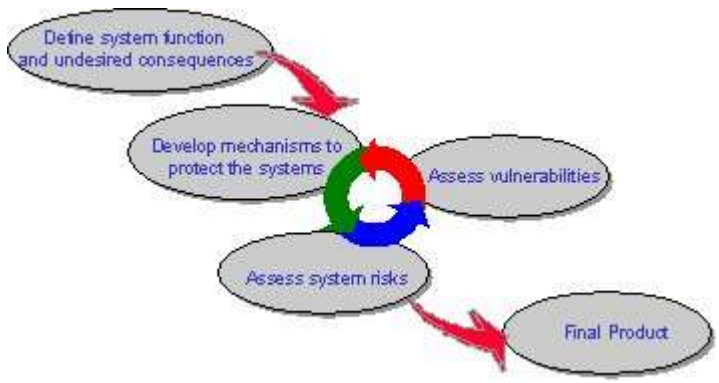


Figure 5: Sandia National Laboratories: Approach to Developing Systems with High Security

Moore [32] provides a risk management process model to show continuous improvement in the system but this model shows a feedback loop in each phase of the cycle but there is no feedback loop between cycles.

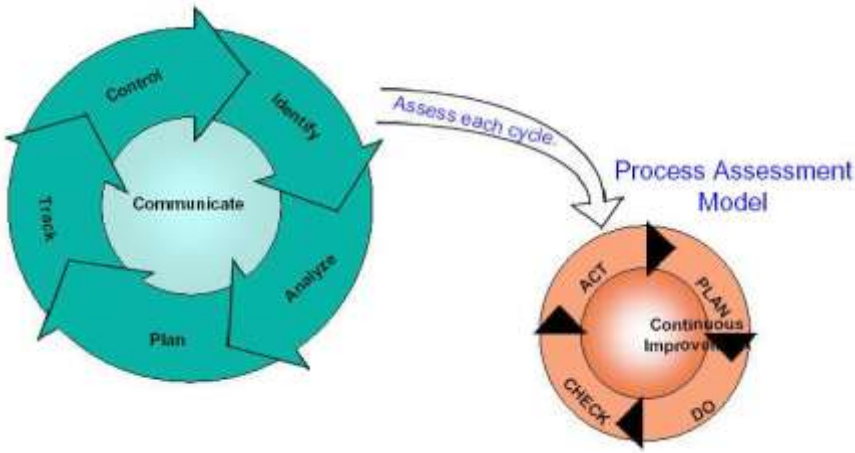


Figure 6: Moore [32] Risk Management Process Model

3. Complex Adaptive Systems

Taking a Department of Defence's system to combat terrorism [8] where the behaviour of terrorism is known and antiterrorism initiatives are focused on measures taken by domestic military installations it has been found that they "lacked critical elements such as a strategic plan containing long-term goals and a performance plan to measure results, assess progress, and identify corrective actions". What is required is real world complex system theory [52] to deal with non linear systems to help predict outcomes based on uncertainty.

The theory of Complex Adaptive Systems [53] may achieve some of the outcome desired. Lucas [6] suggests that Complex Adaptive Systems (CAS) are the merger of three concepts: Cybernetics, Innovation and Complexity. *Cybernetics* deals with the science of control by feedback, *innovation* is required to cope with novel events resulting in unexpected repercussions of actions from deliberate changes of rules and flexibility, and *complexity* that allows the generation of diverse action where parts can interact in different ways [6]. The essence of CAS is that they self-organize, to optimize function such that "an over-constrained system will benefit from more freedom" and "an over-free system will benefit from changes that add stability. Such systems are well placed to explore new niches.

According to Lucas [6] complex adaptive systems can be recognised by having many autonomous parts, they are able to respond to external changes and form self-maintaining systems with internal feedback paths. The primary objective of internal feedback paths is to allow a system to self-organize and to optimize function. Lucas [6] further states "such systems are well placed to explore new niches, to search their fitness landscape, changing their composition to fit the changing patterns they encounter".

Tesfatsion [18] states "many natural systems, and increasingly many artificial (man-made) systems such as distributed computing systems, large-scale communication networks, artificial neural networks, evolutionary algorithms, large-scale software systems, and economies exhibit characteristics of complex adaptive systems". Within a complex adaptive system, agents themselves can either be classified as passive, reactive, active or adaptive [16].

Passive Agents: Do not participate in a system unless specifically contacted and even then they only act within well defined constraints.

Re-active Agents: may simply be able to 'receive' a message from another agent and 'transmit' a standard response. Others may be able to process input before demonstrating behaviour dependent on the results

of the process. Such behaviour may be guided by 'if-then' decision rules or some more complex decision algorithm.

Active Agents: have properties that allow them to interact with other agents within the system, across system boundaries and within vertical hierarchies.

Adaptive agents are capable of modifying some of their parameters or variable states or, in some instances, their rule set.

According to Melymuka [14] complex adaptive system modelling is different to traditional modelling of systems. While traditional models start with assumptions from historical data, complex adaptive systems start with the world as it is and track the results moving forward.

Holling [11], Walters [21] and Van Winkle et al [20] argue that an adaptive management framework is important and should be studied as it allows the development of dynamic models that attempt to make predictions about the impacts of alternative policies.

For risk management, this serves three functions:

- problem clarification and enhanced communication among managers and other stakeholders;
- policy screening to eliminate options that are most likely incapable of doing much good, because of inadequate scale or type of impact;
- identification of key knowledge gaps that make model predictions suspect.

We argue that these three functions are vital to successful risk management systems.

An adaptive management system also has two elements: a *monitoring* system to measure key indicators and the current status of things, and a *response* system that enables modifying key indicators. Management and monitoring of indicators and making appropriate responses represent the heart of Risk Management.

4 State of the Art – Applications of CAS Agents and Adaptive Risk Management

According to the Complex Adaptive Systems Group [45], complex adaptive systems are 'beginning to find applications in many areas of science and occasionally, even the humanities'. Moreover the Complex Adaptive Systems Group states that 'examples of CAS that exist in nature include immune systems, multicellular organisms, nervous systems, ecologies, societies, etc. Examples of synthetic (man-made) CAS include parallel and distributed computing systems, large-scale communication networks, artificial neural networks, evolutionary algorithms, large software systems, economies, etc'. More recently, Bar-Yam [53] exposes ways to use complex systems research to solve complex problems in: healthcare, education, military conflict, ethnic violence and terrorism, as well as in international development.

Applications of CAS and adaptive agents have been employed to study a variety of phenomena from natural processes such as bee hives and ant colonies to human ones such as cooperative game strategies. Recently, agent-based simulations have been applied to warfare. Woodaman [13] has developed a simulation to model a riot that pits two kinds of tactics against two different kinds of crowds. This simulates complex behaviour by programming reactive agents and active agents with a few rules and letting them interact with one another to manage risk. By optimizing the agents' activities at local level, adaptive agents can be programmed to allow an improvement in the performance of the system of risk management as a whole.

State of the art risk management systems focus on managing change from within the organisation itself with respect to its response to changes in the environment. Rather than try to guess what risks will affect the organisation, organizations have been building in characteristics to their systems that improve their ability to respond to change, similar to how immunity works in natural systems. Three major characteristics of complex adaptive systems can be distinguished: *active monitoring*: ensuring the organization's sensitivity to detect risk, *agility*: ensuring its flexibility to respond to risk and *adaptive learning*: ensuring the capability of the organization's resources to mitigate risk [34].

The media and the public have focussed their attention on the highly visible symbols that could be targets of global terrorism (buildings, bridges, nuclear power stations, etc). However an equally important point of vulnerability, and in some respects perhaps even more important because of its central role in the national economy and its extreme vulnerability, is the national computer infrastructure. In the past ten years, every sector of the U.S. economy and government has moved onto network systems. "Everybody relies on networks, and nothing can operate unless the networks are functioning correctly" [35].

Network systems and systems that provide security over the enterprise have been the most proactive in advocating the adoption of adaptive characteristics. The examples of company developed network and security systems that have incorporated adaptive characteristics as a strategy into their products are numerous. Examples below are provided to highlight some of the advances in adaptability made by applications.

- Symbiot [19] - provides a platform for adaptive enterprise network security that incorporates a risk model that can be used to quantify the threats associated with maintaining network security operations. Their approach accumulates events in real-time from multiple sources and aggregates them into a single point of administration, analysis and management. Within the platform risk metrics are developed that rely on a uniform, portable, standardized measure of threat called a 'risk score'.

- Vernier Networks Inc [31] - has developed an Adaptive Security platform (Fig. 7) to reduce the overall organisational risks for the enterprise network. Their platform allows organizations to define and implement five layers of security aimed at creating a trusted network.

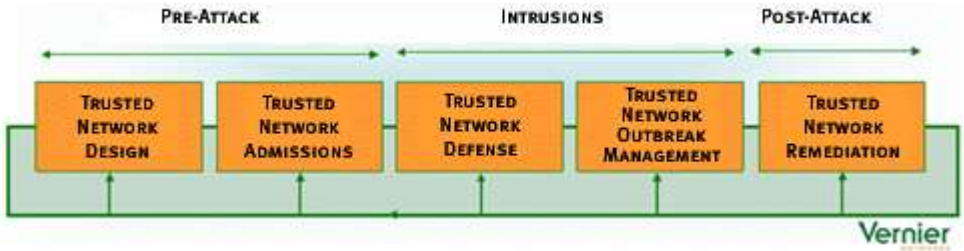


Figure 7: Vernier Networks' Adaptive Security Platform (ASP)

Vernier's system adapts by monitoring pre-attack risks, intrusions and post-attack risks to allow the safety of corporate assets while keeping the organization open for business.

- Hiverworld's [33] continuous adaptive risk management system approach to security challenges (Fig. 8) uses an "appliance" called SWARM.

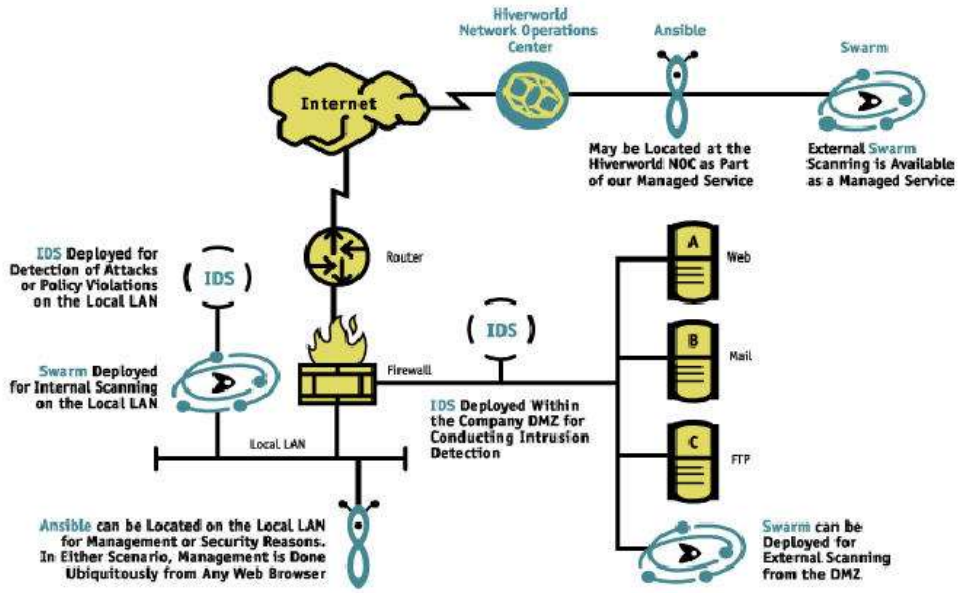


Figure 8: Hiverworld: Continuous Adaptive Risk Management Approach

The 'Swarm' appliance in Hiverworld's solution allows both internal and external intelligent vulnerability scanning that can provide a "hacker's eye" view of the network. Swarm makes use of a vulnerability database, network vulnerability assessment and advanced Scoring System and reflex testing.

5. Holonic Risk Management Framework

An assessment of the implementation of risk management in contemporary systems leads to conclude that a novel implementation to fully exploit available software and hardware is required. According to Buttram [47] 'historically computer systems and networks have been described using biological analogies likening computing systems to living organisms'. In this respect the analogy shares a number of like characteristics that can be used for comparison. Another useful analogy is to liken computing systems to ecologies. The proposed framework draws on both of these analogies.

At the macroscopic level the framework will incorporate mechanisms from ecology to allow the system to be adaptive to risks externally. At the microscopic level the framework will incorporate mechanisms analogous to the human immune system allowing the system to be adaptive to risks internally. A stepwise development of the framework is shown below, with a final functional view of the Adaptive Risk Management (ARMS) framework in figure 21.

5.1 Holarchies and Holonic Risk Management Ecology

Learnthat.com [48] defines an ecosystem as 'a system whose members benefit from each other's participation via symbiotic relationships (positive sum relationships). It is a term that originated from biology, and refers to self-sustaining systems'.

In response to the need for modelling the complexity of interactions in large scale distributed systems, agent technology has emerged (from the AI distributed intelligence task force) as a paradigm for structuring, designing and building software systems that require complex interactions between autonomous distributed (software) components [55]. While the object-oriented paradigm models systems focusing on the structural, static characteristics of their parts which are defined through encapsulation and inheritance, the agent paradigm models systems focusing on the underlining dynamics defined by the

interactions between their parts. In contrast to the passive way in which objects communicate by invoking methods in one another in a way controlled externally by the user (e.g. from a 'main' program), agents are capable to initiate communication and decide (like a human) when and how to respond to external stimuli (e.g. manifested upon them as requests from other agents). From this perspective the agent paradigm extends the object paradigm in that agents can be regarded as proactive objects [56] that have an internal mechanism which governs their behaviour enabling them to initiate action as well as to respond to the outside environment in an autonomous way. With this in mind one can define:

- an intelligent agent as a *software entity* which exhibits, in some significant measure, autonomy, intelligence, and environmental awareness, and which interacts with its environment to achieve internal goals;
- a multi-agent system (MAS) as a software system in which program modules (the individual agents) are given autonomy and intelligence and an underlining coordination mechanism (implementing rules for collaboration, like for holarchies) which enables collaboration between such modules (agents) to attain system objectives

We build on the results obtained by Ulieru [57], [58] in the design of adaptive information infrastructures. More precisely we will embrace the holonic framework for our system's design.

In his seminal book [59] Stuart Kaufmann postulates that life emerged in the Universe through collective autocatalytic processes fuelled by self-organization and natural selection.
As result of the process of evolution driven by *power laws* and *autocatalicity*, emergence endows the dynamics of composite systems with properties unidentifiable in their individual parts. The phenomenon of emergence involves on one side *self-organization* of the dynamical systems such that the synergetic effects can occur and on the other side interaction with other systems from which the synergetic properties can *evolve* in a new context.

In industrial systems a holonic organization is created (see Fig. 9, [60]) as a nested hierarchy, referred to as *holarchy*, of collaborative entities (e.g. resources, people, departments, sections or enterprises) linked through an information infrastructure that defines several levels of resolution [61]. Each entity is a *holon* and is modeled by a software agent [62] with *holonic* properties—that is, the software agent may be composed of other agents behaving in a similar way, but performing different functions at lower levels of resolution.

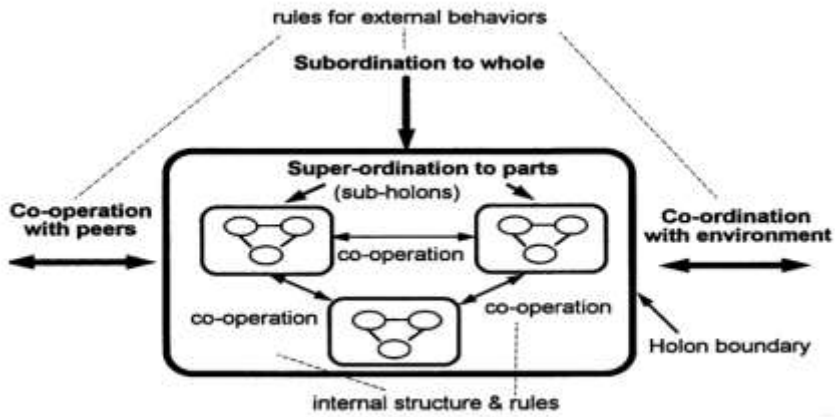


Fig. 9: Generic model of a holarchy (from [60])

The flow of information and matter across a holonic organization defines several levels of granularity (Fig. 9) across which we emulate the mechanism of emergence to enable the dynamic creation, refinement and optimization of flexible ad-hoc AIIs as coordination backbones for the distributed

organization, capable to bring together the best resources available (within reach) depending on the needs of the particular crisis to be addressed.

As such, the phenomenon of emergence involves two distinct steps, namely:

- *Self-organization* of the dynamical systems such that the synergetic effects can occur
- Interaction with other systems from which the synergetic properties can *evolve*

We integrate emergence into the holonic paradigm [63] to create, refine and optimize AIIs. Self-organization is achieved by minimizing the entropy measuring the fuzzy information spread across the multi-agent system [64]. This will cluster the resources (agents), ensuring interaction between the system's parts to reach its objectives timely, efficiently and effectively. Evolution is enabled by interaction with external systems (agents); for example, via a genetic search in cyberspace that mimics mating with most fit partners in natural evolution [65] or by means of dynamic discovery services [66]. In essence of our formalism is provided below.

Holons are autonomous and self-reliant units, they can make decisions on their own without consulting 'higher' levels of control. Simultaneously, holons are subject to higher levels of control. This combination makes a holon a stable form that survives disturbances, can act in the absence of data, and still functions for the functionality of the bigger whole. The holonic risk management framework is initially developed from the holonic risk management ecology as shown in Fig. 10. The *risk management holarchy* as a high level of control is the primary foundation building block of the Holonic Risk Management Ecology. Holarchy's are then developed for Infrastructures requiring protection eg the Emergency response holarchy (Fig. 13) and finally supportive holarchy's are developed to support the infrastructures eg a Holonic Cybersecurity System (Fig. 15) or an e-Health holarchy (Fig. 16) as it will be detailed in the sequel.

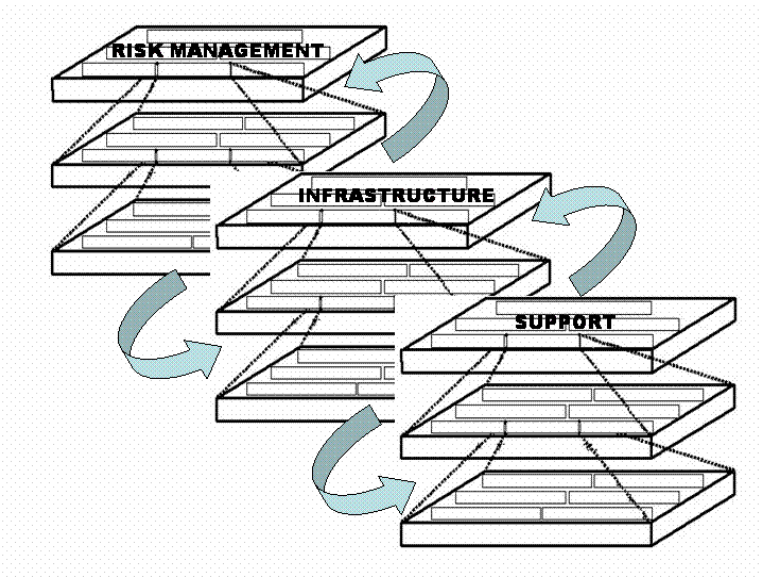


Figure 10: Holonic Risk Management Ecology

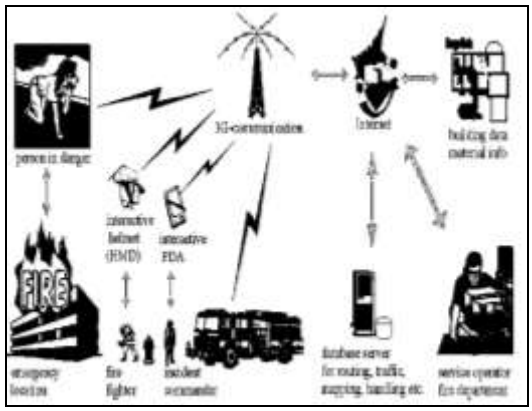
Risk Management

Risk management can only be effectively adopted in an organisation when it has identified and understands its risks. Risk activites focus on inherent and residual risk. In an organisation it is a case of competing risks, i.e. business risk, strategic risk and process risk. Risk metrics, risk drivers and a risk profile must be developed for each category of risk. Risks must then be analysed, mitigated against and controlled all within a guiding set of priority's established according to enterprise objectives.

Figure 11: Risk Management Holarchy

Emergency Response Management (Infrastructure Holarchy)

Rescuing people after an accident or disaster is a time critical operation that requires quick diagnosis, identification of the closest available hospital and knowledge of traffic conditions. AIIs will reduce the duration of a rescue operation by linking participants (see Fig. 12 – from [67]) through a dynamic information system that creates organizational coalitions to deal with disaster relief and ensure harmonious task coordination.



. Figure 12: Fire Emergency Scenario

During an AII-enabled rescue operation (Fig. 12), novel e-Health technologies can be used, e.g. for patient are authentication by a wireless fingerprint sensor that accesses their profile from a remote database which can be accessed via and e-Health (support) holarchy (Fig. 13) [68].

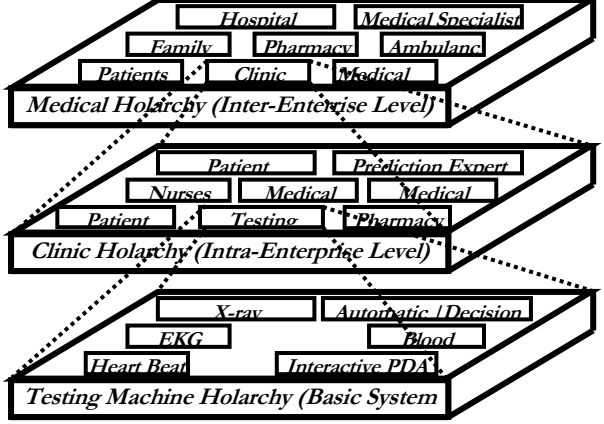
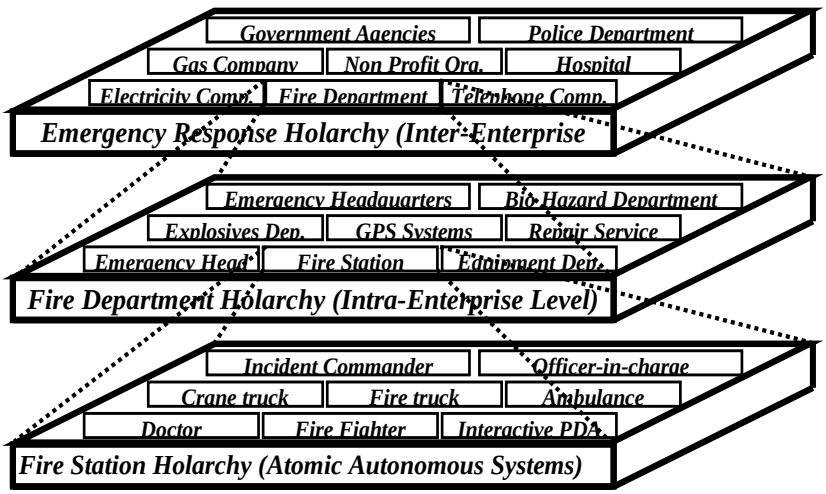


Fig. 13: e-Health Holarchy

Depending on indicators such as blood pressure and the health history of the patient, a first diagnosis will be compiled using automated decision support systems [69]. Electronic logistics support will provide information about the next available and suitable hospital, initiate staff assembly and emergency room preparation, and provide on-the-fly patient check-in.

Planning and scheduling of resources on all levels of the emergency holarchy (Fig. 14) will enable reconfiguration and flexibility by selecting functional units, assigning their locations, and defining their interconnections (e.g. reallocating hospital beds to cope with the victims, rerouting around a fire crew or changing the assignments of a multi-functional defence unit.



unit).

Fig.14: Emergency Response Holarchy (AIIs)

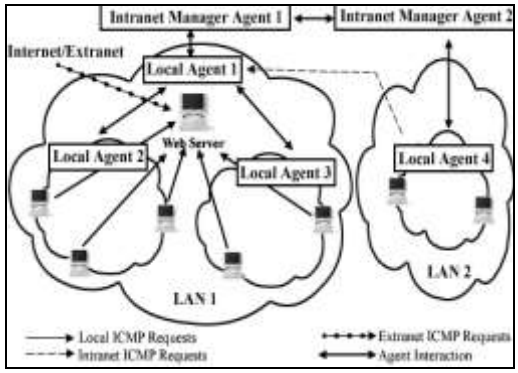
Holonic Cybersecurity System (Support Holarchy)

Information infrastructures are critical to the functioning of society; however, they are vulnerable because of threats and complex interdependencies [70]. New research in this field needs to account for these security issues, which are crucial to future information systems and services. In this context, AIIs provide new dimensions to security:

- *Reliability* of critical infrastructure with survival capabilities, such as power and water distribution.
- *Resilience* based on an anticipative environment that enables operation under continuous threats and attacks.

Most approaches to Cybersecurity focus mainly on system protection against known attacks, leaving it vulnerable to the myriad of creative intrusion-hackers that produce new viruses daily. Few approaches are taking an anticipative view of Cybersecurity systems by emulating the way biological organisms protect themselves [71], [72]. AIIs are networks with moving objects and subjects cloned' as intangible agents in

cyberspace. This vision of security cannot be defined top-down. In this ever-changing environment, security policies must evolve and adapt to suit the circumstances.



. Figure 15: Cybersecurity Scenario (from [72])

To cope with these needs, Ulieru [57] proposed a holonic Cybersecurity model that emulates biological behavior by inducing immunity into the network or system under attack. Organized as a holarchy (see Fig. 15) distributed throughout the network, the framework (Fig. 16) consists of a hybrid mixture of static and mobile agents behaving like a *Cyberorganism* that reacts to attacks in the same way the immune system reacts to protect biological organisms. The AII will anticipate attacks by activating specialized agents seeking the presence of intruders into the network, similar to how antibodies fight viruses in biological systems. This mechanism will enable the network to anticipate an attack and eliminate it before it has a disastrous effect. Computational intelligence techniques will endow the AIIs with learning and discovery capabilities. The AII will behave like an artificial ant colony 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 network. Every command post in the security holarchy (Fig. 16) is alerted, triggering fighter agents that specialize in eliminating attackers.

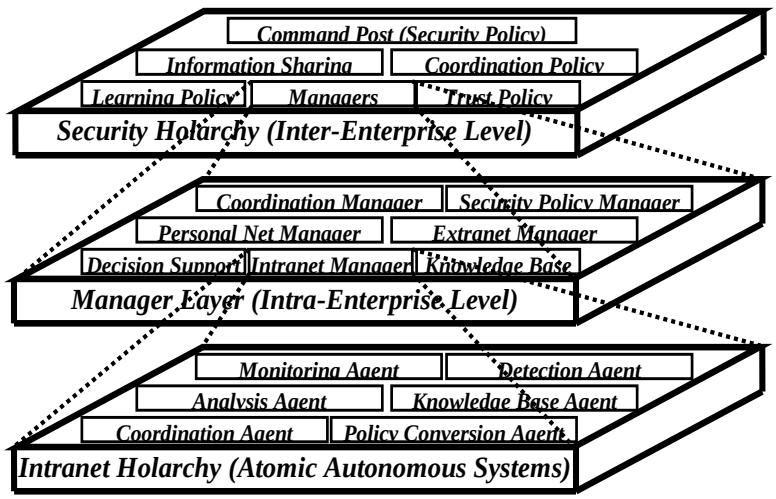


Fig. 16: Cybersecurity Holarchy (AII)

5.3. Human Immune System Analogy and Risk Management Agents

The adaptive human immune system is more complex [49] and has the ability both to recognize different 'antigens' by a group of proteins across its cell surface (chemical fingerprint) and to retain a memory of them so that the next time the antigen invades the fighting response is quicker. Figure 17 [50] below

shows the process of search, detection and cleansing of viruses as they invade the human immune system.

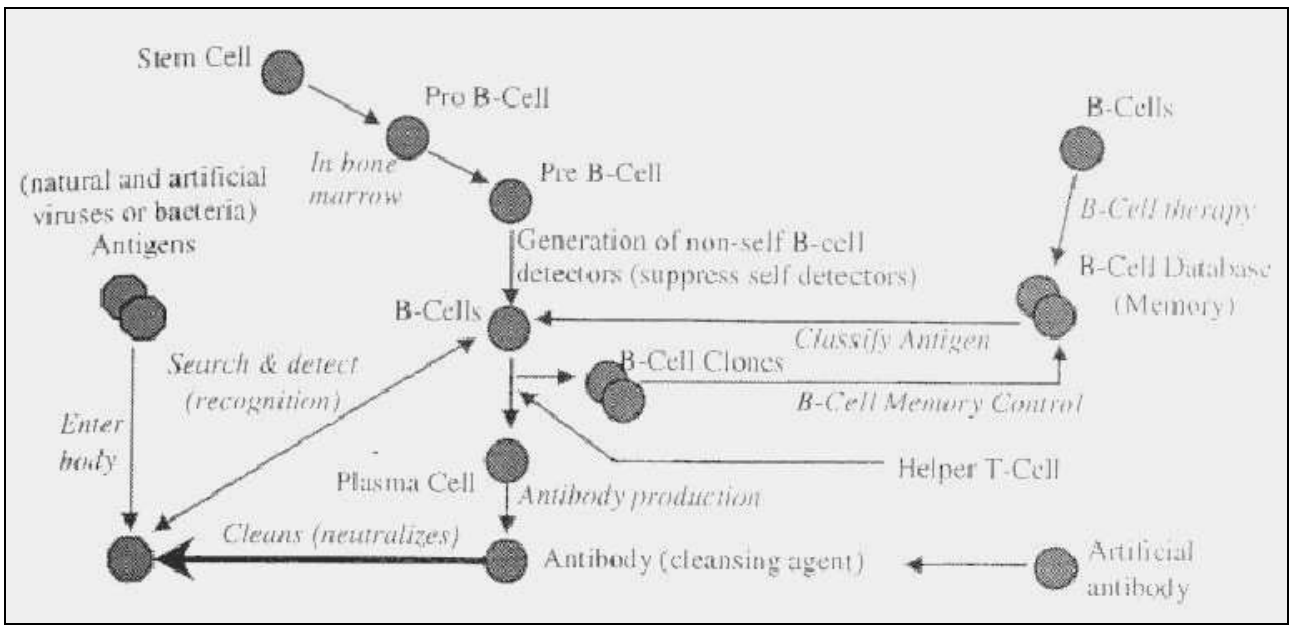


Figure 17: Extracellular Biological IS Model [50]

Risk management agents within the Risk Management Holarchy will search, detect and update identified risks to a risk database in a similar process as virus signatures are added to the human immune system memory, as shown in figure 18 below.

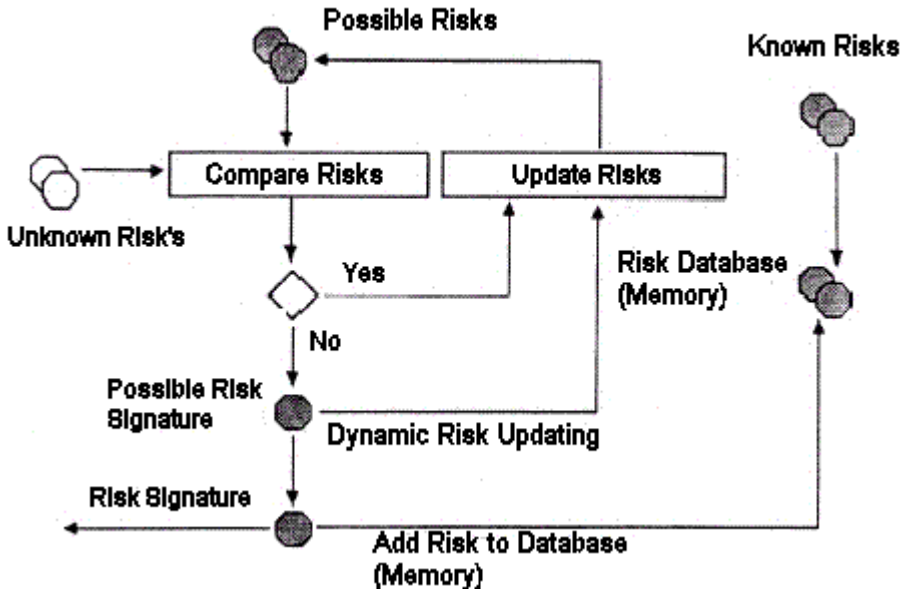


Figure 18: Risk Agent Determination of Risks – Adapted from Hoar [50]

5.3.1 Inter-Agent Communication within the Risk Management Holarchy

The inter-agent communication at the basic agent level is presented in Fig. 19. It shows the modeling of the software agent with holonic properties. The risk management software agent is composed of other

agents eg the identification agent, the control agent, the planning agent and the analysis agent performing different functions.

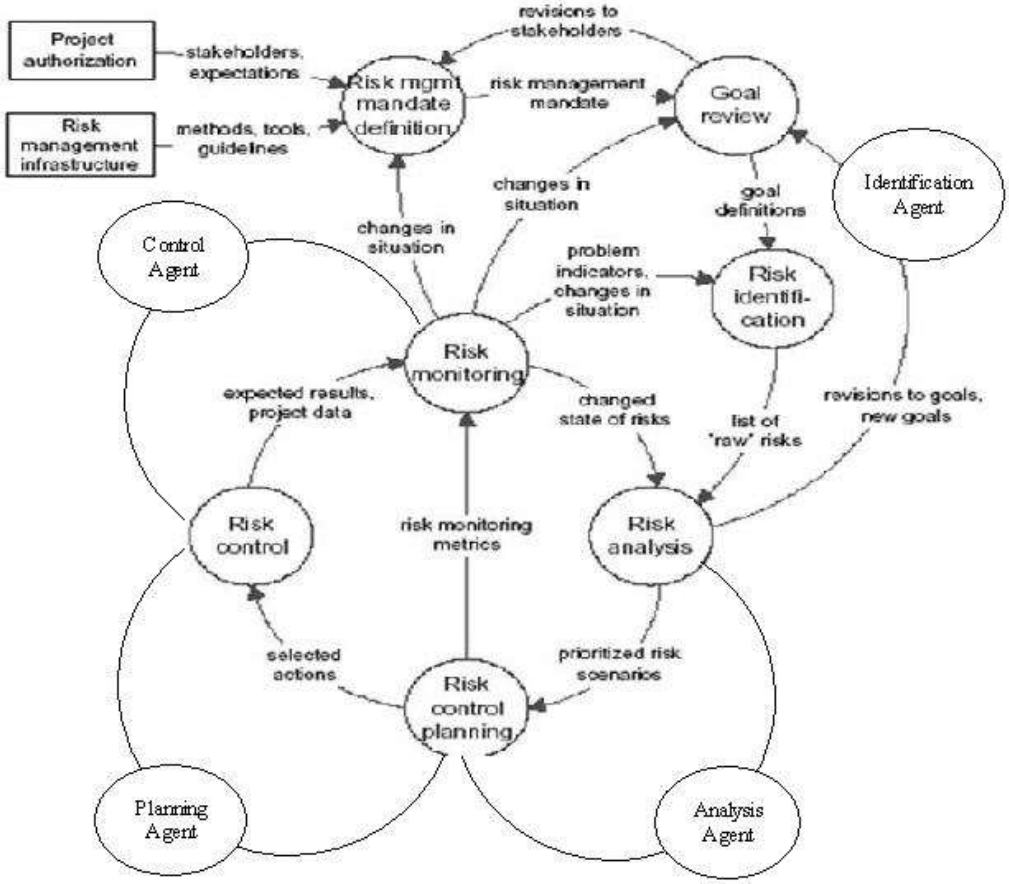


Fig. 19: Inter-Agent Communication – Adapted from Kontio [12]

5.3.2 Internal Structure of the Agents within in the Risk Management Holarchy

Internally the agents have a structure as presented in Fig. 20. This structure originated from work completed on the resilience project and from the theory of "panarchy" that allows an adaptive system to evolve [36].

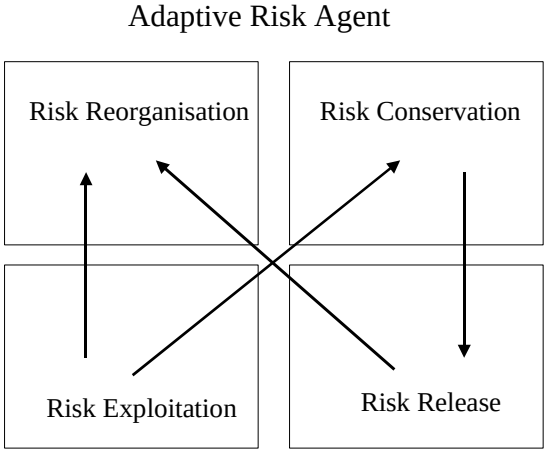


Fig. 20: Internal Structure of the Agents in the Risk Management Holarchy (adapted from Gunderson and Holling [36])

According to Gunderson and Holling [36] any viable framework to understand complex systems behavior would have to meet the following criteria:

- to be as simple as possible but no simpler than necessary for understanding and communication
- to be dynamic and prescriptive, not static and descriptive (e.g., connect to policies and actions; evaluate alternative futures)
- to embrace uncertainty and unpredictability.

It is anticipated that agents with this structure in place will progress through a number of stages as identified by Gunderson and Holling [36]:

Stage 1 - *Exploitation* : Initially holons will be expected to be at an exploitation stage as determined by weak feedback loops, so its behavior is prone to high variation, and the evolutionary path it follows is undetermined.

Stage 2 - *Conservation* : agents at this stage will exhibit strong feedback loops that tend to maintain stability and allow self-consolidating behavior .

Stage 3 - *Release* : agents at this stage will be able to release resources following a disturbance which breaks feedback loops and causes the system to collapse

Stage 4 – *Reorganization* : agents at this stage are able to direct the flows of those resources through the establishment or reestablishment of interactions, including feedback loops, among components.

5.3.3 Agents Properties and Measures within the Risk Management Holarchy

According to Goldspink [16] "for anything interesting to happen in an agent-based system there is a need to include active agents". Active agents have properties that allow them to interact with other agents. The action potential of an active agent can vary markedly". A simple active agent may be able to 'receive' a message from another and 'transmit' a standard response. Others may be able to process input before demonstrating behavior dependent on the results of the process.

As identified by Moore [32] Fig. 21, five measures are required for risk management in each phase of the cycle. The 'active' agents in the holon will utilize these measures to inform the holon:

- Identify – Ability to predict problems
- Analyse – Ability to predict impact
- Plan – Ability to implement planned actions
- Track – Ability to maintain management focus on risk mitigation actions
- Control – Ability to reduce risk exposure

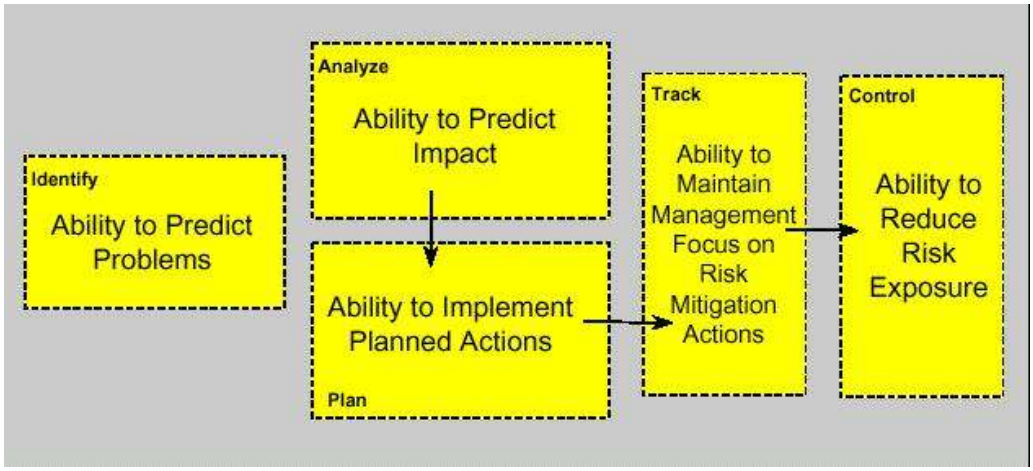


Figure 21: Measures of Risk (Moore [32])

5.4. Architectural View of ARMS

The proposed Adaptive Risk Management (ARMS) framework consists of the Holonic Risk Management Ecology (Fig. 10) and the configuration of the Risk Management Agents behavior as it interacts with the ecology, as illustrated in Fig. 21.

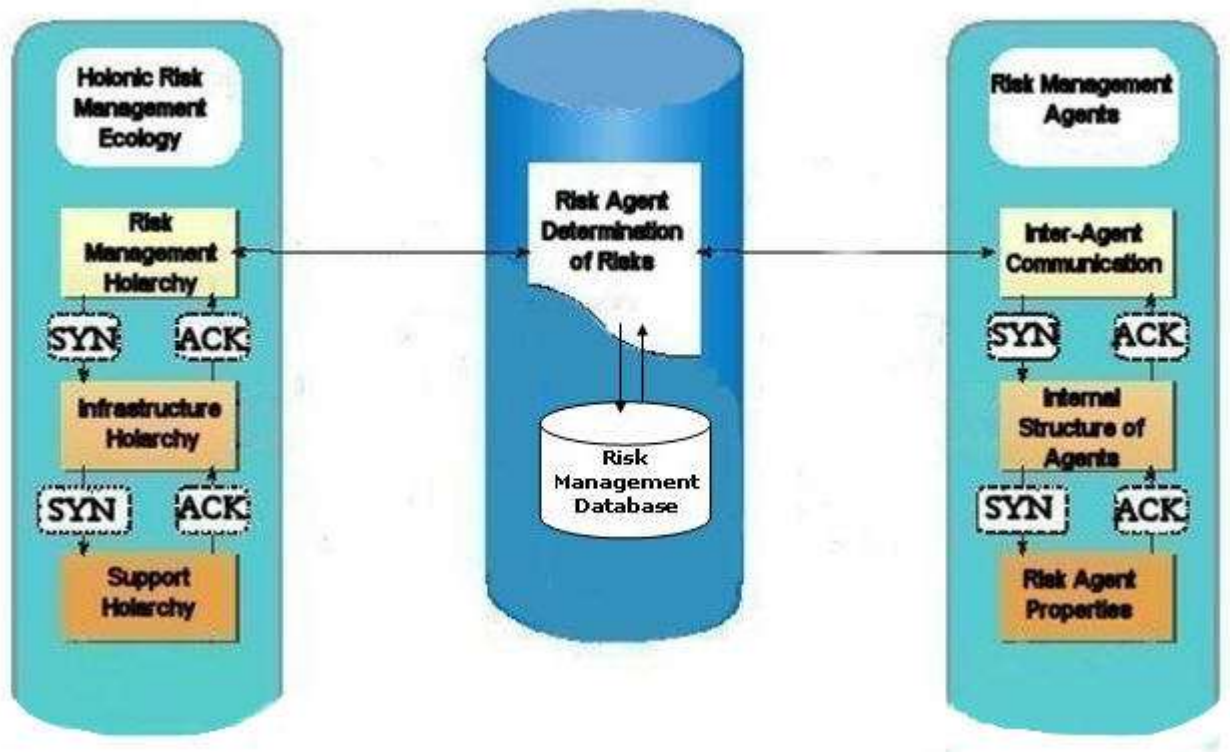


Fig. 21: Architectural View of ARMS

From this perspective, ARMS consists of 3 distinct sections (depicted from left to right):

- Holonic Risk Management Ecology: comprising the interaction of the Risk Management Holarchy, the Infrastructure Holarchy and the Support Holarchy.

- Risk Agent Determination of Risks: this represents the AI component incorporating detection and updating of identified risks to a risk database in a similar process as virus signatures are added to the human immune system memory.

- Risk Management Agents: comprising the Inter-Agent Communication, the Internal Structure of the Agents and the Risk Agent Properties.

In order to facilitate communication between the components of ARMS, a connection protocol must be employed to establish a connection (handshake) - connection establishment, data transfer and connection termination. Precise ARMS communication protocols have not been identified but in a typical TCP connection one end opens a socket and listens passively for a connection from the other. The client-side of a connection initiates an active open by sending an initial SYN segment to the server as part of the 3-way handshake. The server-side should respond to a valid SYN request with a SYN/ACK. Finally, the client-side should respond to the server with an ACK, completing the 3-way handshake and connection establishment phase. An example can be found in [51]. Our future work will focus on undertaking an analysis to explore protocols that could be implemented in the proposed architecture.

5.5. Functional View of ARMS

A functional view of ARMS (Fig. 22) reveals the cyclic nature of the risk management process (left part of the figure), which is a continuous, incremental improvement process, as well as the interaction between the risk, infrastructure and support holarchies. As we zoom into the holarchic functionality, the adaptation mechanism is revealed (in the right part of the figure), as another distinct cyclic process in which the various functions of the systems are performed by the adaptive risk agents, which in turn continually evolve (lower, left part of Fig. 22) by learning from each experience/new risk encountered, which maintaining consistency with the knowledge already available.

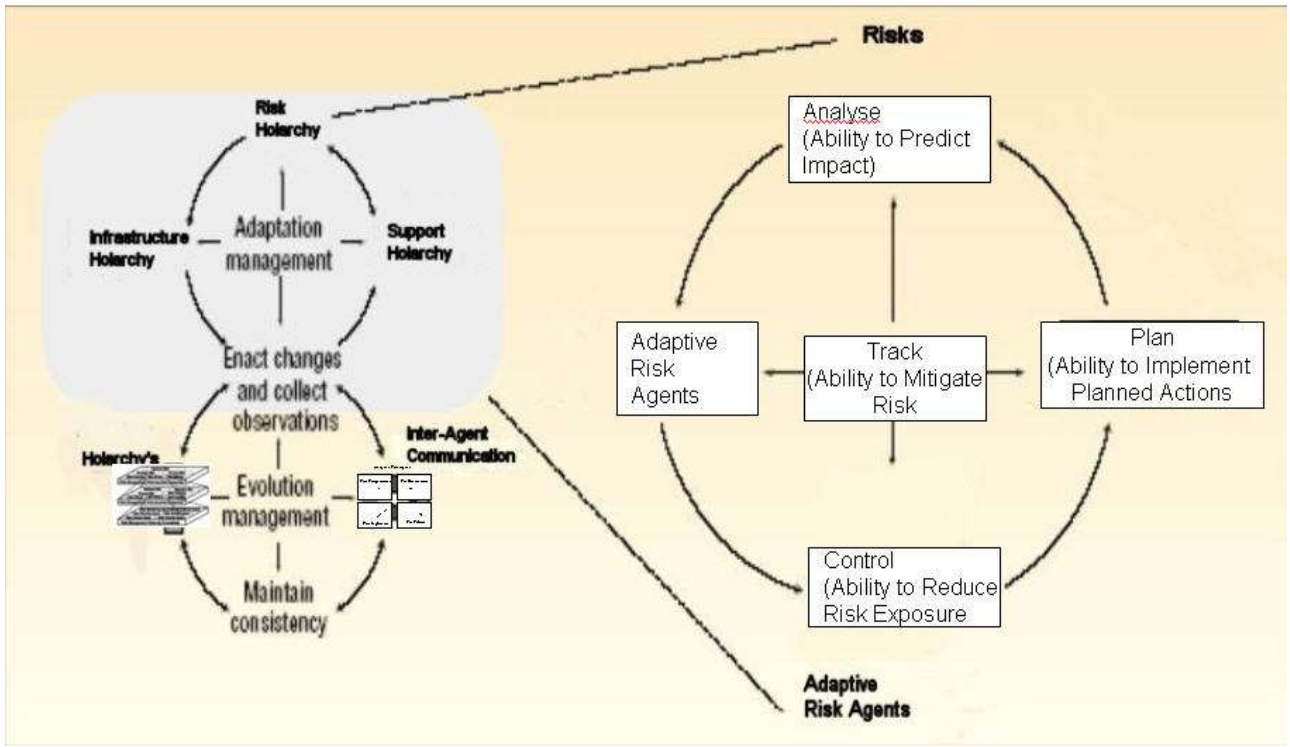


Fig. 22: Functional View of ARMS

This functional view naturally reveals the ecological view of ARMS which is illustrated in the sequel.

5.6. Ecological View of ARMS

Figure 23 reveals an ecomap of ARMS as a way of mapping the ARMS system in relation to its world. The internal structure of the system consists of the holarchies (risk, infrastructure and support), inter-agent communication, adaptive agents and adaptive agents properties. Here on easily identifies how biological behaviour is mirrored by ARMS ecology through e.g. the evolutionary aspect happening through ARMS interaction with the outside world, as well as to new threats continuously coming from the external environment. In addition ARMS adaptability to the requirements of e.g. a new enterprise that solicits ARMS support is depicted.

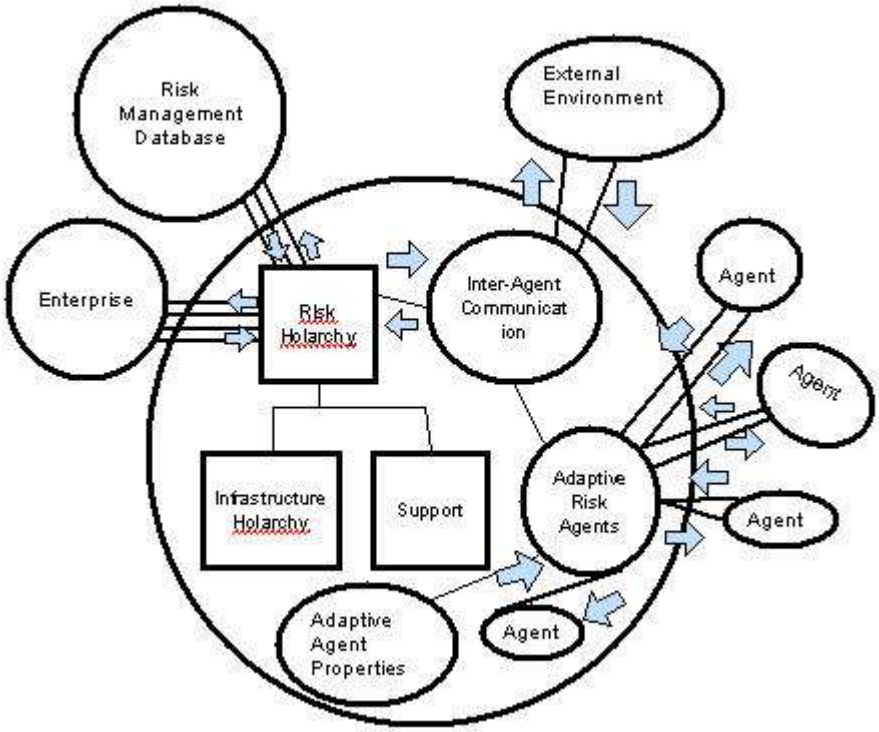


Fig. 23: Functional Ecomap of ARMS

6. CONCLUSIONS

An evolutionary, adaptive risk management system with holonic properties was introduced as a means to respond to emerging needs for safety and security in today's world dynamics. Consisting of three main types of holarchies (Risk, Infrastructure and Support) which dynamically interact through inter-agent communication, the systems is capable to learn, respond and adapt to new situations much like biological organisms adapt and respond to threats in their struggle for survival. Rooted on a solid emergency response management strategy the system acts at several levels to protect critical infrastructure, by e.g. ensuring simultaneously the security of the information infrastructure, on which most of today's critical infrastructure depends. Starting from a deep understanding of the state-of-the art and needs of today's risk management systems, our work is a step forward towards providing autonomic tools much needed to sustain and support mankind in the e-Society age.

7. REFERENCES

[1] Arizona Water Resource (2002), Legislation and Law, Are Laws Adequate for Protecting Sensitive Water Information? http://ag.arizona.edu/AZWATER/awr/julyaugust02/leglaw.html
[2] Department of Defence – Risk Management Plan Template and Guide (2003) - http://www.eitoolkit.com/tools/implementation/Preparation/40_risk_mgmt_plan_template_guide.doc
[3] Crossland, R.,McMahon, C.A. and Sims Williams, J.H (1998), "Survey of Current Practice in Managing Design Risk",ISBN: 0-86292-474-X, University of Bristol, April
[4] Deloitte Touche Tohmatsu (2000), Risk Survey
[5] Deloitte Touche Tohmatsu (2002), Lessons from September 11th, A New Paradigm for Business Continuity Management
[6] Lucas, C (1999) , 'Complex Adaptive Systems - Webs of Delight', http://www.calresco.org/lucas/cas.htm [viewed 2/6/2004]
[7] Foote, D (2002) http://www.infosecuritymag.com/2002/aug/securitymarket.shtml, August, 2002, Information Security
[8] United States General Accounting Office (2002), 'Combating Terrorism - Actions Needed to Guide Services' Antiterrorism Efforts at Installations, http://www.gao.gov/new.items/d0314.pdf [viewed 2/6/2004]

[9] Sandia National Laboratories (2004), 'Critical Infrastructure Surety', http://www.sandia.gov/CIS/capability.htm [viewed 3/7/2004]

[10] Holling, C.S (1995), "What Barriers? What Bridges," in Barriers and Bridges to the Renewal of Ecosystems and Institutions.Edited by L. H. Gunderson, C. S.Holling, and S. S. Light, pp. 3-34. New York: Columbia UniversityPress.

[11] Holling, C. S. (1978),Adaptive environmental assessment and management. John Wiley, New York.

[12]Kontio, J , Getto, G. and Landes. D. (1998),Experiences in improving risk management processes using the concepts of Riskit method, SIGSOFT'98 sixth International Symposium on the Foundations of Software Engineering.

[13] Woodaman, R (2000), Naval Postgraduate School, Monteray California Thesis, 'Agent-Based Simulation of Military Operations other than War Small Unit'.

[14] Melymuka, K (2002), "What If . . . ?", Computerworld, FEBRUARY 04, 2002,

[http://www.computerworld.com/industrytopics/financial/story/0,10801,67916,00.html] Date visited: 17/02/2002

[15] Stoneburner, G. , Goguen. A, and Feringa, A (2001), Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology

[16] Goldspink, C (2000), 'Modelling social systems as complex: Towards a social simulation meta-model' , Journal of Artificial Societies and Social Simulation vol. 3, no. 2, http://jasss.soc.surrey.ac.uk/3/2/1.html

[17] Starnes, R . (2003), Danger money, The challenge of risk management http://www.scmagazine.com/scmagazine/2003_02/feature_4/, feb 2003

[18] Tesfatsion, L (2002), Syllabus of Readings for Complex Adaptive Systems and Agent-Based Computational Economics, [http://www.econ.iastate.edu/tesfatsi/sylalife.htm], date visited 17/02/2002

[19] Symbiot Security [2004], http://symbiot.com [viewed 8/8/2004]

[20] Van Winkle, W. K., Rose, K. A., Shuter, B. J., Jager, H. I., and Holcomb, B. D. (1997). Effects of climatic temperature change on growth, survival, and reproduction of rainbow trout: predictions from a simulation model. Canadian Journal of Fisheries and Aquatic Sciences 54, 2526-2542.

[21] Walters, C.J. (1986). Adaptive management of renewable resources. McMillan, New York.

[22] International Critical Infrastructure Protection Handbook (2001), www.isn.ethz.ch/crn/research/CIIP.cfm

[23] Carnegie Mellon Software Engineering, http://www.sei.cmu.edu [viewed 9/9/2004]

[24] Sesel, J (2003), 'The History of Professional Risk Management', Http::://www.siliconrose.com.au/Articles/HistoryOfRiskManagement.htm [viewed 9/9/2004]

[25] Association of Project Management (UK) (2000) , http://www.apm.org.uk/resources/r.htm [viewed 3/8/2004]

[26] The Sandia National Laboratories Energy, Information and Infrastructure Technology Division (2003), Http://www.sandia.gov/E&E/ep.html [viewed 3/8/2004]

[27] Sifri, G (2002), 'Risk management: Identifying the need 'http://builder.com.com/5100-6315-1050435.html

[28] Risk Management Standard, AS/NZS 4360, www.sai-global.com/NEWSROOM/ TGS/2004-09/RISK-KNIGHT/RISK-KNIGHT.HTM [viewed 28/8/2004]

[29] Newport News Shipbuilding (1998) , http://www.seva.net/~incose/sor-2001/ flyer/sor-trifold-000724.pdf [viewed 3/8/2004]

[30] Standards Australia (2004), Http://ww.standards.com.au [viewed 1/8/2004]

[31] Vernier Networks, Inc , 'Vernier Networks Inc Home Page', http://www.verniernetworks.com [viewed 6/8/2004]

[32] Moore, M (1998), ' Measuring the Effectiveness of Risk Management', http://www.stc-online.org/cd-rom/1998/slides/t1mmoore.PDF [viewed 10/7/2004]

[33] Hiverworld (2004), ' Continuous Adaptive Risk Management' , Http://www.hiverworld.com [Visited 23/10/2003]

[34] McNamee, D (2004), 'Risk Management Today and Tomorrow', http://www.mc2consulting.com/risknz.htm [visited 6/8/2004]

[35] Fernandez, F (2002), 'Secure and Reliable Homeland Security Program', http://guinness.cs.stevens-tech.edu/~dduggan/Local/IAS/DD-May23.doc [visited 3/4/2003]

[36] Gunderson, L. and C.S. Holling (eds). 2002. Panarchy: Understanding Transformations in Human and Natural Systems. Islands Press (pb)

[37] American Society for Training & Development Linking People, Learning and Performance [2004], 'Self Assessment – Checklist', http://www.astd.org/NR/rdonlyres [visited 26/9/2004]

[38] Websters Online Dictionary (2004), 'Defintion: Systematic', http://www.websters-online-dictionary.org/ [visited 26/9/2004]

[39] Hyperdictionary (2004), 'Definition : Systematic', http://www.hyperdictionary.com/dictionary/systematic [visited 26/9/2004]

[40] Fastenersources.com (2004), ASQ Glossary of Terms, http://www.fastenersources.com/definition.html [visited 26/9/2004]

[41] California Performance Review (2004) , 'SO19 911 Emergency Call Center System Improvements, http://www.report.cpr.ca.gov/cprrpt/issrec/stops/it/so19.htm [visited 26/9/2004]

[42] Ward, J (2004), 'Defensive measures' http://www.engineeringnet.co.uk/features%5Ceng11200203.htm [visited 26/9/2004]

[43] Calderone, J (2001), 'Radios Hindered Bravest', Freq of Nature, http://www.freqofnature.com/archives/2001_12_16_newsarchives.html [visited 26/9/2004]

[44] BC Government Information Resource Management Glossary (2004), http://www.cio.gov.bc.ca/other/daf/IRM_Glossary.htm, [visited 26/9/2004]

[45] Complex Adaptive Systems Group (2004) , http://www.cs.iastate.edu/~honavar/cas.html, [visited 26/9/2004]

[46] Resilience Alliance (2004), 'An Immune System Perspective on Ecosystem Management', http://www.ecologyandsociety.org/vol5/iss1/art13/index.html [visited 26/9/2004]

[47] Buttram, R (2004), 'The Biological Analogy and the Future of Information Security', http://www.giac.org/practical/Randy_Buttram_GSEC.doc, [visited 26/9/2004]

[48] Learnthat.com (2004), 'Ecosystem Definition', http://www.learnthat.com/define/view.asp?id=302, [visited 26/9/2004]

[49] Julies-Story (2004),'Human Immune System', http://www.julies-story.org/adrenal/immune-sys.htm, [visited 26/9/2004]

[50] Hoar, R (2004), 'Applications of Immune System Computing', http://pages.cpsc.ucalgary.ca/~jacob/Courses/ Winter2003/CPSC601-73/Slides/07-ISC-Applications.pdf, [visited 26/9/2004]

[51] Mihaela Ulieru and Alexander Grabelkovsky, "Telehealth Approach to Glaucoma Progression Monitoring", *International Journal of Information Theories and Applications* 10(3), 2003, ISSN 1310-0513, pp. 326-330.

[52] Yaneer Bar-Yam, Making Things Work: Solving Complex Problems in a Complex World, Knowledge Magazine Press, 2004, ISBN 0-9656328-1-4

[53] M. Klein, H. Sayama, P. Faratin, and Y. Bar-Yam: A complex systems perspective on how agents can support collaborative design, in *Agent Supported Cooperative Work*, Y. Ye and E.F. Churchill, eds., in press.

[54] Wiegers, K (2004), 'Why Is Process Improvement So Hard?', http://www.processimpact.com/articles/spi_so_hard.html, , [visited 26/9/2004]

[55] Woolridge, M. (Ed.), Foreword to the Proceedings of the Workshop on Agent-Oriented Software Engineering, International Conference Autonomous Agents 2001, Montreal, Canada, May 2001.

[56] Weiss, G. (Editor) – *Multiagent Systems, a Modern Approach to Distributed Artificial Intelligence*, The MIT Press, Cambridge, Massachusetts, 1999.

[57] Ulieru, M., Adaptive Information Infrastructures for the e-Society, Proceedings of the International Workshop on Engineering Self-Organizing Applications, AAMAS 2004, New York, pp.

[58] Ulieru, M., Emerging Computing for the Industry: Agents, Self-Organization and Holonic Systems, Workshop on Industrial Informatics, IECON 2004, November 2-6, 2004, Busan, South Corea.

[59] Stuart Kaufmann, At Home in The Universe: The search for the laws of self organization and complexity, New York: Oxford University Press, 1995

[60] Christensen, James H., Holonic Manufacturing Systems: Initial Architecture and Standards Directions, in *Proceedings of the First European conference on Holonic Manufacturing systems*, European HMS Consortium, Hanover, Germany, 1994.

[61] Mihaela Ulieru, Scott Walker and Robert Brennan, "Holonic Enterprise as a Collaborative Information Ecosystem", Workshop on "Holons: Autonomous and Cooperative Agents for the Industry", Autonomous Agents 2001, Montreal, May 29, 2001, pp. 1-13.

[62] Mihaela Ulieru, "Modeling Holarchies as Multi-Agent Systems to Enable Global Collaboration", Proceedings of the IEEE Computer Society Press – 13th International Conference and Workshop on Database and Expert Systems Applications (DEXA 2002), September 2-6, 2002, Aix-en-Provence, France, pp. 603-608, ISBN 0-7695-1668-8, Order # PRO1668.

[63] Mihaela Ulieru, "A Fuzzy Mathematics Approach to Modeling Emergent Holonic Structures", Invited Chapter in *Geometry, Continua and Microstructures*, pp. 241-255, Academic Press, 2002 – ISBN 973-27-0880-8.

[64] Mihaela Ulieru, Dan Stefanoiu and Douglas Norrie, "Holonic Metamorphic Architectures for Manufacturing: Identifying Holonic Structures in Multi-Agent Systems by Fuzzy Modeling", Invited Chapter in *Handbook of Computational Intelligence in Design and Manufacturing* (Jun Wang & Andrew Kussiak – Editors), CRC Press 2000, ISBN No 0-8493-0592-6, pp. 3-1 – 3-36.

[65] Mihaela Ulieru and Silviu Ionita, "Soft Computing Techniques for the Holonic Enterprise", FLINT 2001, M. Nikravesh and B. Azvine (Eds.), New Directions in Enhancing the Power of the Internet, UC Berkeley Electronics Research Laboratory, Memorandum No. UCB/ERL M01/28, August 2001. pp 182-187.

[66] LARKS: Dynamic Matchmaking Among Heterogeneous Software Agents in Cyberspace, K. Sycara, S. Widoff, M. Klusch and J. Lu, *Autonomous Agents and Multi-Agent Systems*, Volume 5, No. 2, June 2002, Kluwer ISSN 1387-2532.

[67] Mentrup, C., O. Fuhrer: e-Motion: e-Mobile Testbed for Interoperability of Networks in e-Logistics,; Session on Innovative Sectorial Applications, Proc. 1st Int. Conf. on Mobile Business – Evolution Scenarios for Emerging Mobile Commerce Services, July 8-9, 2002 Athens, Greece.

[68] Mihaela Ulieru, "Internet-Enabled Soft Computing Holarchies for e-Health Applications", in *New Directions in Enhancing the Power of the Internet*, (L.A. Zadeh and M. Nikravesh – Editors), pp. 131-166, Springer Verlag, Berlin, 2003.

[69] Mora, T. and Ulieru, M., Agent-Based Decision Support Systems for the Industry, Proceedings of INDIN 2004, Second International Conference on Industrial Informatics, Berlin, Germany, June 24-26, 2004, pp. 391-396.

[70] Tom Berson, Sun Tzu in Cyberspace: The Art of Information Warfare, Keynote Address at the Cybersecurity 2003 Conference, May 20, Foster City, CA, USA.

[71] D. L. Chao and S. Forrest, Information Immune Systems, *International Conference on Artificial Immune Systems* (ICARIS). pp. 132-140 (2002)

[72] N. Foukia, S. Fenet, S. Hassas and J. Hulaas, *"An Intrusion Response Scheme: Tracking the Alert Source using a Stigmergy Paradigm"*, in Proceedings of the 2nd International Workshop on Security of Mobile Multiagent Systems (SEMAS-2002), AAMAS 2002,, Bologna, Italy, July 16, 2002.