Evolving the 'DNA blueprint' of eNetwork Middleware to Control Resilient and Efficient Cyber-Physical Ecosystems

Mihaela Ulieru
Canada Research Chair
Director, Adaptive Risk Management
(ARM Lab)
Faculty of Computer Science
University of New Brunswick
1-506-458-7277
http://www.cs.unb.ca/∼ulieru/
Ulieru@unb.ca

ABSTRACT

The Internet of the future will be a nervous system for the entire economy, integrating 'opportunistic ecosystems' of single devices / departments / enterprises into a larger and more complex infrastructure which we refer to as 'Cyber-Physical Ecosystem' (CPE). In the CPE, the individual properties or attributes of single entities will be dynamically combined to achieve an emergent desired behavior of the ecosystem. It is extremely hard - if not impossible - to control large scale CPE by building a global logic 'top-down' system able to rapidly adapt to changes by instructing each element what to do at each step. Using the latest knowledge of complexity science, we aim to develop a methodological framework for designing large scale CPE capable of generating resilient and scalable structure from the 'bottom-up' by evolving self-organized basic architectural component 'cells.' These cells will be adaptively crafted through dynamic protocols enabling service composition into novel architectural components. The statistical properties displayed by the underlying network structure of the complex distributed system reveals the appropriate parameters on which efficient reliable operation depends. The parameters will be tuned using the dynamical network model of the CPE co-evolved with an 'eNetwork middleware' embedded into the complex system's fabric similar to how DNA molds the fundamental cells in natural systems such that they can evolve to accommodate gradual or abrupt change in the environment or internal operating conditions. Validation on the state-of-the-art testbed recently deployed in the Adaptive Risk Management Lab at UNB enable proof of concept opening the door to applications that will revolutionize several areas of crucial importance, including: blackout-free electricity generation and distribution, optimization of energy consumption, disaster response through deployment of holistic security ecosystems, pandemic mitigation, networked transportation and manufacturing, and environmental monitoring and sustainability assessment.

Keywords

Control and dynamical systems, Complex Adaptive Systems, autocatalytic agent blueprint, emergence, self-organization, dynamical networks, evolution, design for resilience, large scale interdependent systems and infrastructures

1. INTRODUCTION

With information communication technology (ICT) pervading everyday objects and infrastructures, the 'Future Internet' [20] is envisioned to radically transform from how we know it today – a mere communication highway – into a vast *hybrid network* seamlessly integrating physical mobile and static physical systems to power, control or operate virtually any device, appliance or system/infrastructure. Manipulating the physical world will occur locally but control and observability will be enabled safely and securely across an overlay network that we broadly refer to as an 'eNetwork' [25]. eNetworks will enable the spontaneous creation of collaborative societies of otherwise separate artifacts, referred to as 'cyber-physical ecosystems' (CPE). In such 'opportunistic ecosystems', distributed systems at various levels of resolution, ranging from single devices to spaces, departments and enterprises, are brought together into a larger and more *complex* 'system of systems' in which the individual properties or attributes of single systems are dynamically combined to achieve an emergent desired behavior of the synergetic ecosystem. We refer to such a *large scale complex system of interdependent distributed systems* as *eNetworked CPE*. As future 'nervous system' of an economy driven by interdependent critical infrastructures [3] eNetworks will integrate computing, communication and storage capabilities with the monitoring and control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time [14]. The inherent risk of cascading failures at various levels of resolution in an eNetworked CPE requires eNetworks, as *middleware for complex distributed*

Bionetics '07, December 10–13, 2007, Budapest, Hungary.

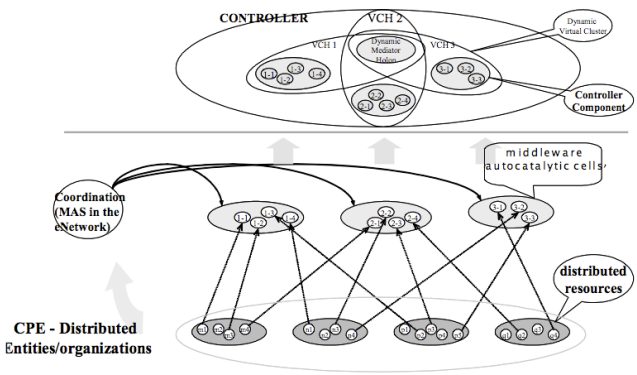

Figure 1: Resource grouping by emerging agents clusters (from [23])

systems, to be designed to enable the deployment of CPE that embed intrinsic robustness and resilience [24]. CPE technologies are envisioned to dramatically evolve over the next years and new properties, issues, interdependencies and vulnerabilities will occur that cannot be envisioned today. To avoid today's solutions becoming tomorrow's problems, a primary requirement for the design of eNetworked CPE is to embed in their fabric *'evolve-ability'* [5] – the ability of a system to seamlessly accommodate unexpected (either gradual or abrupt) change by developing new characteristics or properties that the system did not previously display.

2. STATE-OF-THE-ART

CPE can be modeled as Complex Adaptive Systems (CAS) [15] using the Multi-Agent Systems (MAS) paradigm [19] to build a collective intelligence operating across multitudes of components at various scales that interact intensely with each-other. As a network of agents linked via the Internet the MAS enables the flow of command and control to coordinate desired behavior and performance across the CPE. The MAS paradigm works on top of the Internet protocol to accommodate the processing needs associated with large scale distributed applications unmanageable via centralized processing, thus reducing the computational complexity required at the application layer by distributing it over the eNetwork [24]. One can look at this as a way in which the Internet 'evolved' towards becoming an eNetwork by enriching its architecture with more sophisticated communication and coordination modules to undertake the computational effort required by distributed applications. This 'evolution' [28] is characterized by a spiral of increasing complexity created to suppress unwanted sensitivities/vulnerabilities while taking advantage of new opportunities for increased productivity, performance, or throughput. Complexity here is regarded as *collective behavior* resulting from interaction between parts, which cannot be anticipated because it is not implicitly contained in the behavior of the individual parts at a particular scale of observation. Emerging properties of the collective behavior are novel with respect to the individual parts of the system [11].

When crafting MAS to model complex adaptive systems it is important to recognize that the architectural blueprint (also referred to as 'agent class structure' [26] of the individual agents determines the particular collective behavior, Fig. 1. Using information and uncertainty theory to model the loose coupling between parts we proved [23] that the system self-organizes in a mediated nested hierarchy to minimize the entropy measuring the information exchange across the distributed system to reach equilibrium in an optimal interaction between the parts that achieves the system's objectives most efficiently. To accommodate change in performance requirements and/or environmental conditions system's evolution is enabled by interaction ('mating') with external agents/holons (via automatic composition of service/protocol building blocks). As a rule, the 'basic' agents ('cells') responsible for the emergence of most of the complex collective behavior have *autocatalytic* properties [12]. (The dynamics of a quantity is said to be auto-catalytic if the time variations of that quantity are proportional – via stochastic factors – to its current value [16]). Autocatalyticality ensures that the behavior of the entire system is dominated by the elements with the highest autocatalytic growth rate rather than by the typical or average element. 'Autocatalytic agents' are those un-typical cases (with accidentally exceptional advantageous properties) that enabled the 'emergence' of life [12] (nuclei from nucleons, molecules from atoms, DNA from simple molecules, humans from apes). Most surprisingly, our deepening understanding from genomics and molecular biology has revealed that at the network and protocol level, cells and organisms are strikingly similar to technological networks, despite having completely different material substrates, evolution, and development/construction [9] [25]. As a common denominator, the autocatalytic character linking the microscopic interactions to the macroscopic 'emergent' properties is mathematically phrased via the 'unifying language' of power laws [2] (by taking the logarithm of the variables, random changes proportional to the present value become random additive changes). This brings auto-catalytic dynamics within the realm of statistical mechanics and its powerful methods can be applied efficiently using the concept of *dynamical network* as the unifying tool [18]. The 'elementary' agents within the complex system are modeled as the nodes of the dynamical network and the elementary interactions between them as the links of the network. The dynamics of the complex system is represented by (transitive) operations on the individual links and nodes, while global features of the network correspond to the collective properties of the system that it represents: (quasi)disconnected network components correspond to (almost-)independent emergent objects; scaling properties of the network correspond to power laws. The tools needed to understand complex systems and model them as dynamical networks are currently 'under construction' [18] on a foundation that includes random graph theory and multi-grid and cluster algorithms to which, most recently, robust control was added [8]. Robustness here means that the network resists failure of its nodes as a result of either random or targeted node removal. In this work we set the foundation for a new approach to designing for *'evolve-ability'* [4] the middleware deploying eNetworked CPE, with the eNetwork 'DNA structure' (encapsulated in its architectural blueprint) as the underlying *control mechanism* for inducing robust and efficient behavior within the CPE. Using the paradigms of complexity science and associated computational models of dynamical networks, we

attempt to rephrase concepts from control, communications and software engineering in terms of the construction and verification of barriers that separate acceptable from unacceptable behaviors to propose a breakthrough approach to the **architecting** and **control** of future eNetworked CPE.

3. PROPOSED APPROACH AND ITS ORIGINALITY

3.1 Background and Objectives

Future eNetworked CPE are envisioned as very large scale systems in which a myriad of components have to be able to spontaneously cooperate to accomplish desired tasks ensuring continuity in reliable operating conditions while being able to react to new types of attacks and developing/evolving new (anticipative) defense strategies at the same time. This requires a deep change in how the agents middleware enabling dynamic creation of collaborative CPE clusters is being conceived, designed and managed today – by 'hard-wiring' adaptability into the MAS architectural blueprint, while the blueprint is fixed, impossible to adapt and change by itself [14] [5]. The MAS middleware which controls today's CPE is designed to cover an a-priori anticipated fixed set of scenarios, around a limited range of CPE operating conditions and optimized (in terms of performance) for a particular application. To address the *autonomicity* as major requirement for the future CPE we aim at an evolvable MAS architectural blueprint emerging around desired CPE performance. Adaptation refers to a *micro-evolution*, where systems, at runtime and without any human intervention, modify internal parameters to optimize their operating point (e.g. TPC congestion control [28]). Conversely, evolution leads to the introduction of *new* functionality, not previously engineered in the system. This is generally achieved by means of automatic composition of service/protocol building blocks or automated code generation [5]. The main drive in our undertaking is to design the eNetwork middleware, herewith regarded as the 'controller' of a complex system (the CPE), Fig. 1, as a collective of 'basic autocatalytic agents' (hereafter referred to as 'cells') carrying the 'DNA code' for evolving *resilient* and *efficient* organizational structure in the CPE. Through 'cells' mating protocols and services the middleware architectural blueprint will evolve with new components enabling CPE coordination/control via the dynamic (re)clustering of CPE parts to:

- accommodate (gradual and abrupt) *change* resulting from unanticipated performance requirements and/or unexpected environmental dynamics (*resilience*).
- ensure suitable performance across the overall system's resources (*efficiency*).

The challenge is to prove that systems are robust and efficient at multiple levels of abstraction, including that of embedded code. To address this challenge we focus on architecting the controller to enforce robust efficient CPE behavior, by answering two major questions, as follows.

3.1.1 Architecting the Controller

"How does eNetwork architecture map to CPE behavior?" We aim to find the *basic architectural element* ('autocatalytic agent'/'cell') that could 'grow' (Fig. 2) the components of a middleware architecture acting as controller capable to coordinate efficient and resilient behavior in the CPE, for various kind of CPE (classified e.g. by application or by the kind of devices/plants that make the physical part of the CPE, etc.) When crafting the 'autocatalytic cell' we have to take into account the fact that the new components will need to be 'grown'/'evolved' along the growth gradient of CPE performance requirements – so we will consider the co-evolutionary interdependence between the eNetwork controller and the controlled CPE. The major challenge here pertains to formal software verification of 'evolving code' to ensure **architectural consistency** with CPE robustness and efficiency.

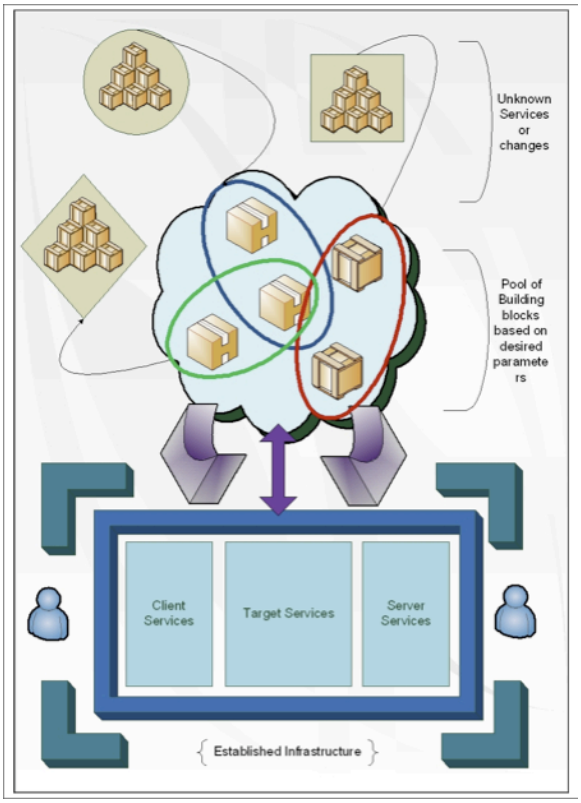

Figure 2: Evolution of architectural components in the eNetwork middleware (controller)

3.1.2 CPE Control for Robustness and Efficiency

"How can the eNetwork be used to control interdependent complex systems and processes (such as e.g. energy production, distribution and consumption)?" We aim to define a strategy to 'emerge bottom-up' the appropriate architectural blueprints (identified in the **Architecting** part) that can implement the necessary regulatory feedback and dynamics to stop cascading failures in the CPE (thus achieving robustness), while considering the abstraction of 'barriers' in the state space of a system's dynamics. For this we first need to define a CPE as a complex dynamical system and using its associated dynamical network model to identify those parameters in charge with the CPE efficient and resilient behavior to design the control loops which can tune desired behavior to stabilize the CPE under abrupt disturbance. The main conceptual objective is to guarantee that a clearly defined set of CPE "bad behaviors" is empty.

(For example, in the case of robustness analysis of linear systems that set can correspond to a particular combination of uncertain parameters producing a large performance index. In protocol verification the bad behavior can be associated, for instance, to a deadlock condition.) To investigate the interdependencies between the middleware communication networks that controls the flows through the CPE we need first to model this 'middleware controller' itself as a complex network of agents managing these flows through the CPE (power, transportation, finances, and other flows). The understanding of the complex controller network and its interactions with the CPE will enable to identify and model vulnerable hubs which need to be enforced. The dynamical network model of the controller hints towards parameters that can strengthen certain 'hubs' via barriers emerged 'bottom-up' thus keeping the CPE safe over a broad range of dynamics. The major challenge here is to rephrase **robust control** in terms of the construction and verification of barriers that separate acceptable from unacceptable behaviors (which typically involve a cascading failure event.) Thus, by modeling the controller as a complex MAS, we can match the parameters revealed by its associated dynamical network to the CPE complex system parameters and appropriately craft the control loops enforcing resilient and efficient CPE behavior.

3.2 Architecting the Controller by Mapping eNetwork Architecture to CPE Behavior

We are searching for the 'DNA structure' of a 'cell' that can evolve the eNetwork architectural blueprint to enable resilient and efficient CPE behavior.

We take note of the 'mutual evolutionary influence[1]' between the two interwoven networks within the fabric of an eNetworked CPE (Fig. 1):

- the dynamical network structure encapsulating the behavior of the complex CPE (system part) – which hints to parameters that can be tuned to ensure desired performance in the CPE;
- the complex network of agents in the eNetwork middleware (controller part), which (as MAS [19]) coordinates the various flows (of information, materials, money, etc.) across the CPE. As a complex system itself, the (MAS) controller displays itself a dynamical network structure, which hints to the parameters that can be used to tune desired performance in the CPE.

Increase in CPE performance requirements results in higher workflow traffic across the CPE, which in turn increases the coordination demands at the middleware. To cope with these demands new architectural components are added to the middleware (Fig. 2) and by this the eNetwork co-evolves by undertaking new responsibilities to match the continuous development spiral of new CPE applications. ICT-enabled critical infrastructures (today's CPE, Fig. 3 [10]) co-evolved with the Internet by 'patching' it in a piecemeal fashion [28] [3] [24], and by analyzing them we expect to be able to extract *patterns of middleware architectural growth* correlated to the dynamics of the supported complex applications.

[1] *Coevolution* is the 'mutual evolutionary influence' between two species manifested as change in the genetic composition of one in response to a genetic change in the other [12].

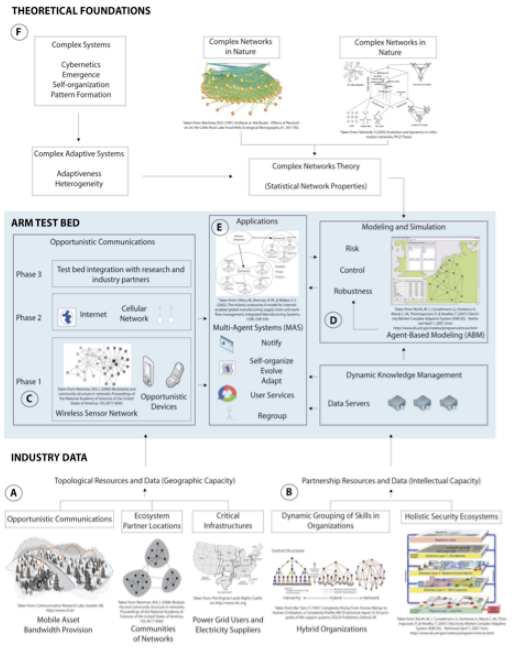

Figure 4: Adaptive Risk Management Lab Testbed (from [27])

Based on these patterns we can develop a library of middleware architectural blueprints for the controller middleware correlated with various behaviors to be enforced in the controlled CPEs as well as a repository of elementary 'cells' that can 'mix-and-match' into architectural components to evolve the various architectures.

To date there is no theory or practice correlating the dynamical network structure reflecting the behavior of a complex distributed system (CPE) with the architecture of the middleware controller (agents network) that coordinates it. We first need to analyze several middleware architectures relative to the dynamical network structure of the CPE deployed on various applications (including the projects in the CFI Lab, Fig. 4 [27] [21]) and extract *patterns* correlating the middleware architectural blueprint to CPE behavior. Based on this we will then define the blueprint ('DNA structure') of a 'cell' that could collectively emerge appropriate architectural components for the middleware blueprints identified [17], Fig. 5.

3.3 Using the eNetwork to Control Large Scale CPE

We investigate how to evolve the appropriate components in the eNetwork architectural blueprint that can reconfigure the CPE around optimal performance requirements with automatic de-coupling of emerging vulnerable hubs.

It is extremely hard – if not impossible – to control a large scale eNetworked CPE by building a global logic 'top-down' system able to rapidly adapt to changes adequately by instructing each element what to do at each step. The communication network infrastructure (eNetwork middleware) for such large scale systems must be regarded in a broader context, of the overall network that can be analysed statistically as a system (whole ensemble of interlinked nodes) [8] to determine global parameters by which to tune the flows

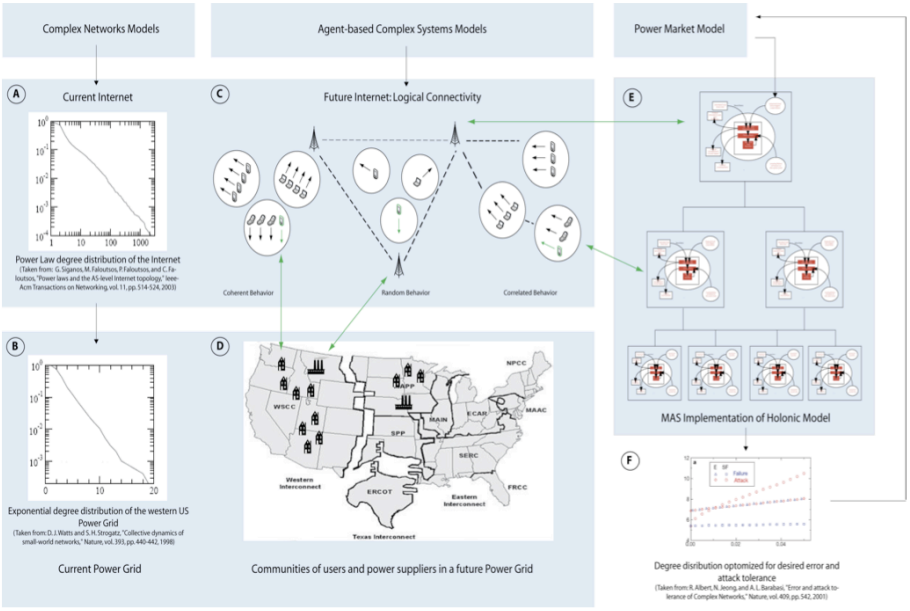

Figure 3: CPE power grid controlled by the eNetwork (from [10])

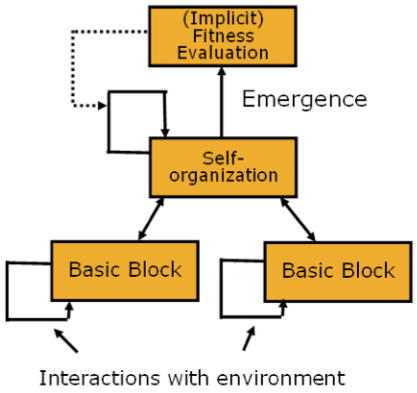

Figure 5: 'Bottom-up' emergence of architectural components (from [17])

throughout the system (ensemble) vs. micromanaging the traffic on individual links and nodes. Based on statistical analysis of the dynamical networks [18] modeling the CPE (complex system) and its controller middleware respectively, we can synthesize growing of coordination components in the middleware to tune efficient operation and resilience within the CPE. The dynamical network model of the CPE reveals the parameters that *can/should be tuned* while the dynamical network model of the controller middleware reveals those parameters by *which to tune* desired CPE behavior/performance and using the correlation patterns previously identified (Section 3.2) we can design interaction protocols linking middleware components via feedback mechanisms to ensure optimal workflow across the CPE. At the same time the dynamical network models enable identification and evaluation of interdependencies between CPE and its controller (Fig. 1) which point to vulnerabilities to cascading failures. The abstraction of 'barriers' in the state space of CPE network dynamics hints one side to the parameters by which resilience to such failures can be tuned and on the other side to the middleware architectural components containing the protocols needed for tuning the identified parameters.

3.4 Evolve the eNetwork (controller) to grow barriers to attacks in the CPE (complex system)

We start with the recent observation [9] that most advanced biological and technological systems have evolved driven by the need to enforce barriers to attacks [25]. Most genes code for sensors, actuators and the complex regulatory networks that **control** them, and thus confer to the cell **robustness** rather than the mere basic functionality required for survival in ideal circumstances. Likewise the Internet is enabled by protocols specifying control strategies for managing the flow of packets. They create barriers to cascading failures because of router outages and congestion [8]. Thus robustness involves complex regulatory feedback and dynamics to stop cascading failures. Analyzing the collective behavior of the CPE regarded as a *statistical ensemble* we can envision appropriate protocols encoded in 'cells' that collectively can compose ('mate') protocols to act 'at the right place at the right time' on the overall system according to changing operating conditions. This 'mating' of the 'basic autocatalytic agents/cells' will evolve protocols that will grow ('emerge') architectural components specifying control strategies for managing the workflow across the CPE while creating barriers to occurring cascading failures. Various 'mating' methods exist, among which: automatic composition of service/protocol building blocks, e.g. like in the BioNets approach [4] in which evolutionary services are associated to *user-situated living organisms*; automated

code generation [29] e.g. via *Artificial Chemical Computing (ACC)* [13] [7], Artificial Immune Systems [6]; *Evolutionary Algorithms* [1]; or swarm intelligence [22]. By thorough analysis the most appropriate to compose the basic architectural cells identified at Section 3.2 to automatically generate ('bottom-up emerge'/'grow') the components of the middleware blueprint that stop cascading failures for various classes of CPE will be selected (or other methods will be developed as necessary).

4. CONCLUSIONS

We proposed a methodological framework for **architecting** the elementary 'agents'/'cells' capable of collectively generating ('emerging') new components in the middleware, thus modifying its architectural blueprint, to tune (**control**) dynamic adaptation of the CPE to gradual or abrupt change in performance requirements or environmental conditions. Addressing this involves the undertaking of the grand challenge of formal and algorithmic verification of the correctness and robustness of scalable network protocols and embedded software for control of large scale distributed systems which we currently tackle in the ARM Lab [27] [21]. **To date there is no theory or practice for designing systems that emerge architectural components to enforce barriers to cascading failures.** On the **architecting** side, we proposed (in Section 3.2) a strategy to identify the architectural (eNetwork middleware) pattern ('blueprint') enforcing barriers to attacks in various kinds of CPE and the basic 'cell' structure that would generate ('emerge') such barriers via a bottom-up 'cell' combination enabling 'mix-and-match evolution' of protocols. Cell 'mating' generates new composite protocols, which restructure (evolve) the architecture into an (emerging) blueprint of new components. To guarantee system's functional correctness we must concomitantly develop formal software verification methods to ensure architectural consistency with CPE robustness and efficiency. On the **control** side we have to map the parameters identified in Section 3.2 to the architectural blueprints of the middleware enforcing barriers to attacks (found in the architecting process) in order to identify a strategy to generate ('emerge') barriers to attacks in the eNetwork middleware by tuning appropriate parameters to implement the necessary regulatory feedback and dynamics to stop cascading failures in the CPE.

The proposed approach frontally bootstraps through the latest advances in five disciplines (while further pushing the boundaries of each) as follows:

- **Systems engineering** – new approach to **control** hybrid interdependent multidimensional networked systems of systems with cascading effects;
- **Software engineering** – new approach to **architect** the middleware coordinating large scale complex systems exhibiting emergent performance;
- **Communications** – new approach to modeling large scale communication network infrastructures, regarded in a broader context, of the overall network that can be analysed statistically as a system (whole ensemble of interlinked nodes) to determine global parameters by which to tune the flows throughout the system (ensemble) rather than by analysing the traffic on individual links and nodes.
- **Computing** – development of new techniques and algorithms associated to dynamical networks as models for these complex systems;
- **Complexity science** – development of new techniques and algorithms associated to emergence, self-organization and evolution in complex adaptive systems – where 'evolution' is understood in the broader context of *autocatalytic* processes.

Evolve-able resilient and efficient CPE unleash potential for the seamless integration of technologies unthinkable today within the fabric of our Planet – thus creating an open environment for far reaching societal, economic, industrial and techonologically sustainable growth. CPE will accommodate both gradual and disruptive developments, the influence on our lives of which we cannot completely grasp now, such as the threat of climate change.

5. REFERENCES

[1] W. Banzhaf, P. Nordin, R. Keller, and F. Francone. *Genetic Programming, An Introduction*. Morgan Kaufmann Publishers, 1998.

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

[3] V. Brown, T. Beyeler, and D. Barton. Assessing infrastructure interdependencies: The challenge of risk analysis for cmplex adaptive systems. *Int. J. Critical Infrastructures*, 1 (1):108–117, 2004.

[4] I. Carreras, I. Chlamtac, F. DePellegrini, and D. Miorandi. Bionets: Bio-inspired networking for pervasive communication environments. *IEEE Transactions on Vehicular Technologies*, 55 (6):–, 2006.

[5] I. Carreras, D. Morandi, and I. Chlamtac. From biology to evolve-able, pervasive ict systems. In *Proc IEEE SMC 2007 Conf, Oct. 7–10, Montreal, Canada*, 2007.

[6] L. deCastro and J. Timmis. *Artificial Immune Systems: A New Computational Approach*. Springer, 2002.

[7] P. Dittrich. Chemical computing. In *Proc. of UPP*, 2004.

[8] J. Doyle, D. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger. The " robust yet fragile" nature of the internet. In *Proceedings of the National Academy of Science USA*, volume 102, 2005.

[9] J. Doyle and M. Csete. Rules of engagement. *Nature*, 446:860, 2007.

[10] S. Grobbelaar and M. Ulieru. Complex Systems as Control Paradigm for Complex Systems. Opening Position Paper at the 1st IEEE Workshop on eNetworks Cyberengineering, IEEE Systems, Man and Cybernetics Conference, October 7–10, Montreal, Canada, 2007.

[11] J. Holland. *Emergence: From Chaos to Order*. Perseus Books, 1998.

[12] S. Kauffman. *Investigations*. Oxford University Press, 2000.

[13] G. Krauss. *Biochemistry in Signal Transduction and Regulation*. Wiley and Sons, 2003.

[14] A. Lee. Computing foundations and practice for cyber-physical systems: A preliminary report. Technical Report UCB/EECS-2007-72, University of California, Berkeley, 2007.

[15] S. Levin. Complex adaptve systems: Exploring the known, the unknown and the unknowable. *Bulletin of the American Mathematical Society*, 40:3–19, 2003.

[16] Y. Louzoun, N. Shnerb, and S. Solomon. Microscopic noise, adaptation and survival in hostile environments. *European Physical Journal B*, 56:141–148, 2007.

[17] D. Miorandi. From Biology to Evolvable Pervasive ICT Systems, Presentation at the IEEE SMC Workshop on Cyberengineering, October 7, Montreal, Canada. Available online at: http://www.smc2007.org/workshops.html, 2007.

[18] M. Newman, A.-L. Barabasi, and D. Watts, editors. *The Structure and Dynamics of Networks*. Princeton University Press, 2006.

[19] M. North and C. Macal. *Managing Business Complexity: Discovering Strategic Solutions with Agent-Based Modeling and Simulations*. Oxford University Press, 2007.

[20] NSF/OECD. Workshop "Social and Economic Factors Shaping the Future of the Internet", Washington DC. http://www.oecd.org/dataoecd/47/28/39034762.pdf, 2007.

[21] M. Sohail and M. Ulieru. Challenges in the deployment of enetworked cyberphysical ecosystems. In *Proceedings IEEE ETFA 2007, Patras, Greece*, pages 804–809, 2007.

[22] J. Suzuki and T. Suda. A middleware platform for a biologically inspired network architecture supporting autonomous and adaptive applications. *IEEE J. Sel. Ar. Comm.*, 23 (2):249–260, 2005.

[23] M. Ulieru. Emerging computing for the industry: Agents, self-organization and holonic systems. In *Proceedings of the IEEE-ICON International Workshop on Industrial Informatics*, pages 215–232, November 2004.

[24] M. Ulieru. Design for resilience of enetworked critical infrastructures. In *Proceedings of the 1st IEEE Int. Conf. on Digital Ecosystems*, pages 540–545, 2007.

[25] M. Ulieru. Foreword to the invited workshop on enetworks cyberengineering: Infrastructures for cyber-physical ecosystems. In *Proceedings IEEE Systems, Man and Cybernetics*, 2007.

[26] M. Ulieru and M. Cobzaru. Building holonic supply chain management systems: An e-logistics application for the telephone manufacturing industry. *IEEE Transactions on Industrial Informatics*, 1 (1):18–31, 2005.

[27] M. Ulieru and S. Grobbelaar. Engineering industrial ecosystems in a networked world. In *Proceedings of the 5th IEEE Industrial Informatics Confercence*, pages 5–17, 2007.

[28] W. Willinger and J. Doyle. Robustness and the internet: Design and evolution. In E. Jen, editor, *Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies*, Santa Fe Institute Studies on the Sciences of Complexity. Oxford University Press, 2002.

[29] L. Yamamoto. Framework for distributed on-line evolution of protocols and services. Technical report, BIONETS (IST-2004-2.3.4 FP6-027748) Deliverable (D1.2.1), 2006.