

Autonomic Approach to Survivable Cyber-Secure Infrastructures

Frederick Sheldon, Tom Potok
Applied Software Engineering
Oak Ridge National Lab.¹
Oak Ridge, TN 37831 USA
SheldonFT | PotokTE@ornl.gov

Michael Langston
Dept. Computer Science
University of Tennessee
Knoxville, TN 37996 USA
langston@cs.utk.edu

Axel Krings and Paul Oman
Dept. Computer Science
University of Idaho
Moscow, ID 83844 USA
Krings | Oman@cs.uidaho.edu

Abstract

*Information systems now form the backbone of nearly every government and private system – Web services currently does or will play a major role in supporting access to distributed resources, command and control to exploit the backbone. Increasingly these systems are networked together allowing for distributed operations, sharing of databases, and redundant capability. Ensuring these networks are secure, robust, and reliable is critical for the strategic and economic well being of the Nation. This paper argues in favor of a biologically inspired approach to creating survivable cyber-secure infrastructures (SCI). Our discussion employs the power transmission grid. **Keywords** Infrastructure Vulnerability, Reliability, Cyber-Security, Software Agent, Autonomic Computing Paradigm*

1 Introduction

Survivability of a system can be expressed as a combination of *reliability, availability, security, and human safety*. Each critical infrastructure (component) will stress a different combination of these four facets to ensure the proper operation of the entire system(s) in the face of threats from within (malfunctioning components, normal but complex system interrelationships that engender common failures) and threats from without (malicious attacks, and environmental insult, etc.). Structured models allow the system reliability to be derived from the reliabilities of its components. The probability that the system-of-systems survives depends explicitly on each of the constituent components and their interrelationships as well as system-of-systems relationships. Reliability analysis can provide insight to developers about inherent (and defined) components and/or (intra-)system “weaknesses” [1-4]. Naturally, as the software/system complexity increase, the reliability analysis task becomes more difficult.

In the face of ever increasing computing complexity and pervasiveness, at the core of autonomic systems (AS), is

introspection and self-management. AS strive to (transparently) provide users with a machine/system that runs at peak performance 24x7. Like their biological complement, AS maintain and adjust their function in the context of changing components, workloads, stress, and external conditions and in the context of hardware/software failures, random or malicious [5, 6].

1.1 Biologically Inspired Survivability (BIS)

The next generation of high performance dynamic and adaptive nonlinear networks, of which power systems are an application, will be designed and upgraded with interdisciplinary knowledge for achieving improved survivability, security, reliability, reconfigurability and efficiency. Furthermore, there is an urgent need for the development of innovative methods and conceptual frameworks for analysis, planning, and operation of complex, efficient, and secure electric power networks².

SCI represents the combination of performance and reliability modeling, and survivability analysis germane to future (fourth-generation) power distribution and electronic information infrastructure applications including communication, network-centric distributed command and control as they relate to electrical energy generation, storage/distribution, and electrical machinery and equipment. Two important themes form the basis for increasing robustness in large-scale networked information systems. First *cognitive immunity* promises improved, cost effective technologies for the detection, quantification and recovery from vulnerabilities/faults:³ Such cognition is

² The continued security of electric power networks can be compromised not only by technical breakdowns, but also by deliberate sabotage, misguided economic incentives, regulatory difficulties, the shortage of energy production and transmission facilities, as well as the lack of appropriately trained engineers, scientists and operations personnel.

³ The term “fault” is used consistent with “fault-tolerant design” models, and does not *necessarily* refer to short circuits like “bolted faults.” During the Aug. 10, 1996 west coast cascading failures one contributing cause was McNary generator exciter circuits erroneously detecting a “phase imbalance” that was actually a drop in frequency. Frequency oscillations also contributed to voltage swings which were erroneously interpreted as “switch onto fault” logic by several protective relays that (subsequently) tripped offline. Theoretically, a fault is a discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition (ANSI). Generally, a fault is an

¹ This manuscript has been authored by UT-Battelle, a contractor of the U.S. Government (USG) under Department of Energy (DOE) Contract DE-AC05-00OR22725. The USG retains a non-exclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

truly context dependent. For example, to establish immunity in the power distribution and electronic information (PDEI) infrastructure, we must:

- Assess the state-of-practice of (remote) real-time vulnerability/fault detection for SCI.
- Use existing models of SCI vulnerability/fault detection to develop an improved numerical simulation model for nominal/transient flows.
- Based on the new numerical model, develop and test a real-time detector that can promptly locate and accurately quantify vulnerabilities/faults.
- Simulate a real-time network of detectors and evaluate the effects of signal strength and noise on vulnerability/fault detectability.
- Explore the use of the numerical model, driven by real-time data, within a secure communications infrastructure to define the parameters of a survivable SCI including Supervisory Control and Data Acquisition (SCADA) system.

The second theme, *self-healing*, provides biologically-inspired response strategies and proactive automatic contingency planning for the PDEI infrastructure including automated data acquisition, secure system monitoring, and control techniques between source/sink and control centers.

- Determine the similarities between energy control (e.g., electric power grid control) and information networks for adaptation to SCI control systems,
- Assess the state-of-the-practice with respect to the application of Information Security (InfoSec) principles within existing SCI control and information networks,
- Adapt or develop procedures for Common Mode Failure Analysis (CMFA) and Security/Survivability Systems Analysis (S/SSA) from the electric power domain to application within SCI and information networks in general (e.g., Internet) [7],
- Identify areas within SCI control and information networks where existing InfoSec technologies can be applied, but are heretofore absent,
- Identify SCI specific vulnerabilities for which new InfoSec technologies and devices must be developed or adapted.

1.2 Ensuring System Integrity

To codify and systematize BIS the focus should be on requirements, models and tools that aid in the process of ensuring system integrity [8] by selecting the mitigation mechanisms that maximize the individual and system wide objectives (see Fig. 1). In this way, optimization techniques can be added showing how resources (i.e., cost), can be spent on individual solutions, and how this affects the overall survivability. An advantage of this approach, especially in the first phase, would be that SCI

“accidental or abnormal physical” condition that *may* cause a functional unit(s) to fail to perform its required function (when and if encountered). Faults can be classified in terms of criticality indicating the severity of the failure consequences. Error analysis is the process of investigating an observed fault with the purpose of tracing the fault to its source (diagnosis).

implementations in the long haul could be targeted easier, as it is a bottom-up approach[9]. In fact, the applicability of the proposed technology/ methodology to multiple energy sectors in the infrastructure scope is broad because the degree of impact (i.e., to improve or sustain energy assurance) on the energy infrastructure is determined at the component level [10, 11].

2 Network Vulnerability

As a society, we have become dependent on the computer infrastructure networks (including energy grids, pipelines, transportation systems/ thoroughfares and facilities) that sustain our daily lives. *Network-centric infrastructure* demands robust systems that can respond automatically and dynamically to both accidental and deliberate faults. Adaptation of fault-tolerant computing techniques has made computing and information systems intrusion-tolerant and more *survivable*, but even with these advancements, a system will inevitably exhaust all resources in the face of a determined cyber adversary. Computing and information systems also have a tendency to become more fragile and susceptible to accidental faults and errors over time if manually applied maintenance or restoration routines are not administered regularly. This project seeks to address these deficiencies by creating a new generation of security and survivability technologies. These “fourth-generation” technologies will bring attributes of human cognition to bear on the problem of reconstituting systems that suffer the accumulated effects of imperfect software, human error, and accidental hardware faults, or the effects of a cyber attack. Vulnerabilities addressed include mobile/malicious code, denial-of-service attacks, and misuse and malicious insider threats, as well as accidental faults introduced by human error and the problems associated with software and hardware aging [12, 13].

The overarching goals in light of, for example, the threat posed by a blackout similar to the one that occurred on August 14 2004, is to implement systems that *always* provide critical functionality and show a *positive* trend in reliability, that exceed initial operating capability and approach a theoretical optimal performance level in the long run. Desired capabilities include self-optimization, self-diagnosis, and self-healing, architecture/methodology for systems that support self-awareness and reflection in order to achieve these capabilities.

2.1 Survival Strategy

SCI is a strategy intended to meet the critical need for fourth generation survivability and security mechanisms that complement first-generation security mechanisms (trusted computing bases, encryption, authentication and access control), second-generation security mechanisms (boundary controllers, intrusion detection systems, public key infrastructure, biometrics), and third-generation security and survivability mechanisms (real-time execution monitors, error detection and damage prevention, error compensation and repair). New fourth generation technologies will draw on biological metaphors (so-called

artificial biology) such as software that survives because it possesses biological properties of redundancy and regeneration (i.e., parts die off without affecting the whole), natural diversity and immune systems to achieve robustness and adaptability, the structure of organisms and ecosystems to achieve scalability, and human cognitive attributes (reasoning, learning and introspection) to achieve the capacity to predict, diagnose, heal and improve the ability to provide service.

2.2 Hierarchical Evaluation

The SCI strategy uses a hierarchical method to evaluate and implement survivability mechanisms and mitigate failures associated with three important areas of energy assurance: (a) securing cyber assets, (b) modelling, and analysis to understand and enable fundamentally robust and fault-tolerant systems, and (c) systems architecture that can overcome vital limitations. Infrastructure Evaluation comprises 2 phases. First, individual components of the infrastructure are evaluated in isolation to derive individual component survivability (CS). The process identifies feasible *mitigation* mechanisms on a per component basis. In the second phase, the CS is composed into the system-at-large. This approach leverages individual CS models to create hierarchical structures with increased system survivability (e.g., against failures due to the complexity of engaging unanticipated component interactions)⁴. To codify and systematize this approach the focus is on models that aid in the process of ensuring system integrity [15] by selecting mitigation mechanisms that maximize individual and system wide objectives. In this way, optimization techniques can be added showing how resources may be spent on individual solutions, and consequently, how such strategies affect the overall survivability. Naturally, individual component survivability alone is not the means for understanding the survivability of the whole system-of-systems. However, using a bottom up compositional approach enables a model-based notational language to be used to provide a complete and unambiguous description of the system.

2.3 Networks of Control

Industries that use and develop critical infrastructure have become more computerized, and the risk of digital disruption from a range of adversaries has increased [7]. The societal common ground has proven essential to our digital economy, but has become fragile and operated at its margins of efficiency without reinvestment for many years. Assessment and mitigation strategies are needed to support implementing/configuring optimally redundant (backup) systems, low-cost data collection methodologies, identification of critically vulnerable nodes and

⁴ The sources of common mode faults are widespread. See [14] A. Krings and P. Oman, A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures, *HICSS-36 Minitrack on Secure and Survivable Software Systems*, Hawaii, 2003, 334a-44. for modelling primitives that represent interdependency failures in very simple control systems (i.e., an initial step in creating a framework for analyzing reliability/survivability characteristics of infrastructures with both hardware and software controls).

communication pathways, detecting intruders or abnormal operations, mechanisms for distributed intelligent adaptive control to effect more flexible and adaptive systems.

Fault-tolerant systems deal with accidental faults and errors while intrusion-tolerant systems cope with malicious, intentional faults caused by an intelligent adversary. Combining fault- and intrusion-tolerance technologies produces very robust and survivable systems, but these techniques depend upon resources that may eventually be depleted beyond the point required to maintain critical system functionality. A biologically inspired approach will reconstitute and reconfigure these resources in such a manner that the systems are better protected in the process, reliability is continually improved as vulnerabilities and software bugs are discovered and fixed autonomously, and the ability to provide critical services is never lost.

3 Autonomic Framework

The autonomic (AC) computing approach was outlined in 2001 by Paul Horn Sr. VP of Research at IBM, a corporate-wide initiative in response to what their customers feel are the major impediments to more widespread deployment of computing in the workplace. Customers are concerned with the total cost of ownership (TCO) and believe that configuration management (i.e., installing software and patches, setting various performance parameters, etc) is a significant contributor to TCO.

Ideally, systems would be self-managing; work well out of the box and continue to work well as the computing environment changes (due to failure-induced outages, changes in load characteristics, addition of server capacity). New applications may be easier to deploy if existing ones can automatically adjust and if the appropriate building blocks exist to support the construction of new applications in ways that can adapt themselves. The essential theme for AC systems therefore is self-management and cognition consisting of the following four pillars [5]:

- *Self-configuration* –Automated configuration of components and systems follows high-level policies. Rest of system adjusts automatically and seamlessly.
- *Self-optimization* –Components and systems continually seek opportunities to improve their own performance and efficiency.
- *Self-healing* –System automatically detects, diagnoses, and repairs localized software and hardware problems.
- *Self-protection* –System automatically defends against malicious attacks or cascading failures. It uses early warning to anticipate and prevent system wide failures.

Therefore, the higher-order cognitive processes of reflection and self-awareness are key to creating systems that are not fragile in the presence of unforeseen inputs. Moreover, these systems will have the capacity to reason, learn, and respond intelligently to things never encountered before. However, to realize the challenge many factors must be considered (see Fig. 1).

3.1 Cognitive Cyber Defense

To achieve SCI a hierarchical method may be used to assess and implement survivability mechanisms and

mitigate vulnerabilities as well as all classes of failures. (1) Hardening cyber assets using a framework for SCI survivability, (2) providing robustness and fault-tolerance through modeling, simulation, and analysis, and (3) overcoming fundamental limitations for increased reliability via effective systems architecture and the application/development of the autonomic computing paradigm mentioned above [16]. Survivability assessment comprises 2 phases: First individual components of the infrastructure are evaluated in isolation to derive various components survivability. This phase identifies feasible *mitigation* mechanisms on a per component basis. In the second phase, a mapping from component survivability is extended to the overall system at large resulting in better comprehension that can:

- Enhance control system dependability due to fault tolerance and system integrity strategies (i.e., using autonomic computing paradigm),
- Support a modular/scaleable approach to critical systems automation, and energy/information distribution,
- Improved ability to sustain operational capability post attack,
- Support modeling and simulation of damage phenomenology in support of more intelligent sensors, and
- Provide an optimized technology assessment approach that can be used to select system architectures and define the elements of systems and their control to enable, improved system survivability (e.g., using segregated system zones and autonomic computing paradigm).

3.2 Common Mode Failures

Critical energy infrastructures and essential utilities have been optimized for reliability under the assumption of a benign operating environment. Consequently, they are susceptible to cascading failures induced by relatively minor events such as weather phenomena, accidental damage to system components, and/or cyber attack. In contrast, survivable complex control structures should and could be designed to lose sizable portions of the system and still maintain essential control functions [7]. For example, in [14], the Aug. 10, 1996 cascading blackout is studied to identify and analyze common mode faults leading to the cascading failure. Strategies are needed to define independent, survivable software control systems for automated regulation of critical infrastructures like electric power, telecom, and emergency communications systems.

3.3 Cyber Security

Several mitigating factors contribute to the difficulty of implementing cyber security in power substation control networks. First, is the geographic distribution of these networks, spanning hundreds of miles with network components located in isolated remote locations as well as the sheer number of devices connected to a single network open to compromise. The enormity of access points greatly increases the risk of cyber attack against electronic equipment in a substation [17].

Our approach uses intelligent software agents (SAs) [18,

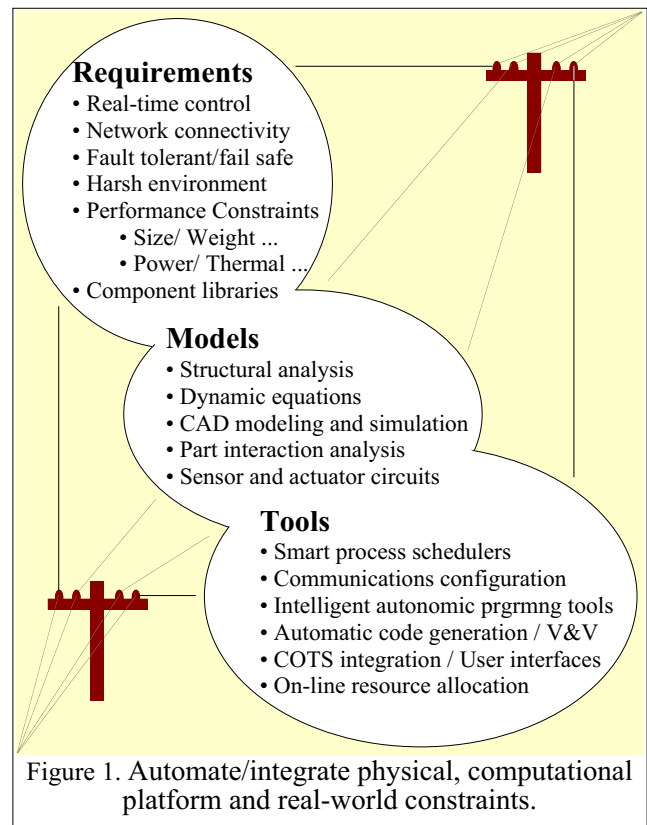


Figure 1. Automate/integrate physical, computational platform and real-world constraints.

19 2003] (each modeled as an individual component) to deploy new and user-friendly data collection and management capabilities which possess inherent resiliency to failures in control networks [7, 20 2003] as well as maintenance/evolution properties that promote low cost of ownership [7, 21]. SAs enable secure, robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber attack etc., [22, 23], as well as intelligent adaptive control [24].

3.4 Inherent Obstacles

The diversity of equipment and protocols used in the communication and control of power systems is staggering [7]. The diversity and lack of interoperability in these communication protocols create obstacles for anyone attempting to establish secure communication to and from a substation (or among substations in a network of heterogeneous protocols and devices). In addition to the diversity of electronic control equipment is the variety of communications media used to access this equipment. It is not uncommon to find commercial telephone lines, wireless, microwave, private fiber, and Internet connections within substation control networks [25].

3.5 Mitigation Strategies

Previous work in this area has presented details of both threats and mitigation mechanisms for substation communication networks [25]. In [26], the most important mitigation actions that would reduce the threat of cyber intrusion are highlighted. The greatest reduction can be achieved by enacting a program of cyber security education combined with an enforced security policy. Combined,

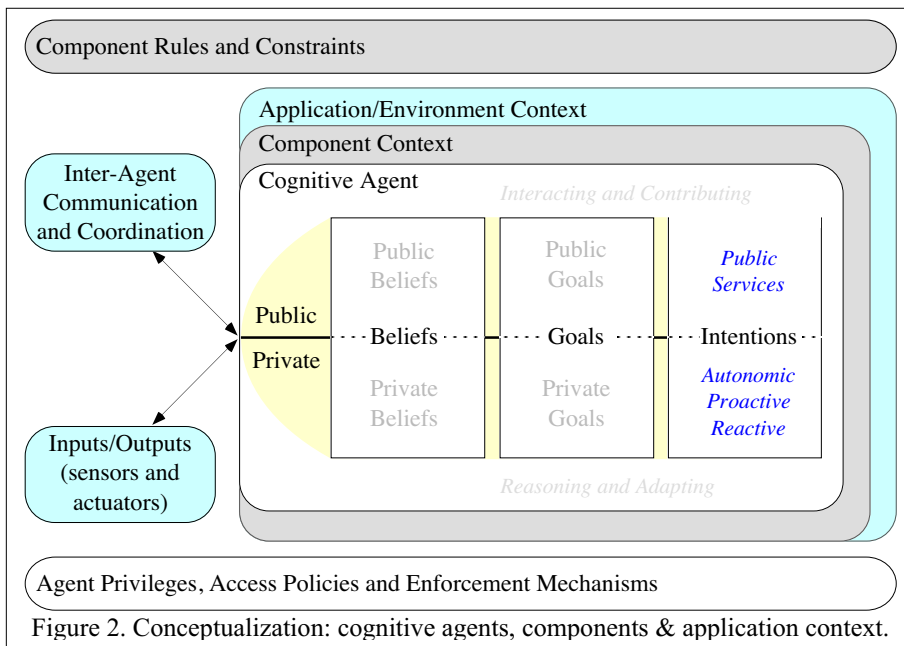


Figure 2. Conceptualization: cognitive agents, components & application context.

these two strategies will have the greatest impact because of the lag in cyber security knowledge within the industry. Education and enforcement will assist with counteracting both external and insider threats⁵.

4 Software Agents

Adaptive/intelligent software agents [27-29] can be used to deploy new and user-friendly data collection, and inherent resiliency to failures in responsive decision networks [30] as well as software maintenance/ evolution properties that promote low cost of ownership [21, 31] (see [6] for a discussion of fundamental [dis-]advantages). Using software agents can enable secure and robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber attack etc. [31-33], distributed intelligent adaptive control [34], and characterization of damage and failure mechanisms (see Fig. 2).

Cognitive systems may comprise 3 types of processes: a) *reactive*, timely response to external stimuli, b) *deliberative*, learning and reasoning, c) *reflective*, continuously monitor/adapt based on introspection.

4.1 Cognitive Agent Architecture

Based on the BDI model [35, 36] the *Beliefs* of an agent can consist of private and public beliefs. Private beliefs represent local agent state information, which form the main basis for reasoning and reactive behavior. Public beliefs include (distributed) information about the context/environment and are the basis for reflective processes. The *Desires* are goals, where private goals govern the deliberative activities while the public goals direct the reflective processes as they describe the overall cognitive system goals. *Intentions* (services) consist of reactive, pro-active, autonomic and public plans. Reactive plans deal with timely responses to inputs and changes in

the environment. Proactive plans form the core of the deliberative process, and represent the planning and reasoning processes. The autonomic plans represent the reflective process, including monitoring the agent's performance to achieve robust and secure behavior. The robustness will include, at a minimum, fail-safe plans to respond to unexpected events. An agent may make available its Public Services to other agents in the system. Agents in cognitive systems are autonomous and situated. Thus each agent is implemented with one or more active processes (or threads). For simple reactive agents (with very limited deliberative or reflective processes), a single thread is adequate to respond reactively to external stimuli. Complex agents may have separate threads for reactive, proactive

and autonomic plans⁶.

4.2 Modeling and Optimization

In addition, as an extension to the SCI, we identify how specific SCI communication protocols and mechanisms [27] can be modeled and mapped onto fault-models for understanding the impacts of common mode failures and usage profiles, including load scheduling [37-39], to identify weak points (assisting risk assessment and mitigation) in the system [14, 40, 41]. For example, there are cost effective ways to apply survivability methods [33, 42] based on redundancy and dissimilarities to the communication networks controlling the SCI. This provides several advantages: 1) the result uses a transformation model [43-45] to map the specific protocol and/or application to a graph and/or Petri Net(s) [46]; 2) interesting optimization criteria can be applied to facilitate survivability based on redundancy, while investigating the degree of independence required to achieve certain objectives (e.g., defining minimal cut sets of fault trees associated with any hazard); 3) isolation of the critical subsystems, which constitute a graph, and using agreement solutions to augment the graph to achieve the required survivability (robustness). Thus, different graphs may be derived that contain the original critical subsystems and are augmented by edges and/or vertices that allow the use of agreement algorithms. In this way, critical systems decisions are decentralized and invulnerable to malicious attacks, as long as the threshold of faulty components dictated by the agreement algorithms is not violated. Moreover, the whole field of system fault diagnosis, which

⁵ FERC (Federal Energy Regulatory Commission) adopted NERC (North American Energy Reliability Council) security policies as standard.

⁶ Cognitive agent systems specification is defined by a Cognitive Multi-Agent Modeling Language (CMAML) and formally described using denotational semantics [6]. The key concepts of the language are Agent, Belief, Goal, Plan, KQML Performative, FIPA Performative and Blackboard [ICA02Kavi].

originated from the PMC model (Preparata, Metz and Chien), can be applied [47, 48]. The fundamental question is "Who tests whom, and how is the test implemented to identify faulty components?" In this vein, we can address (i.e., specify) how to derive "diagnostics" that would determine if the system is robust along with a measure of confidence (i.e., determine the effectiveness, see [32-34, 42, 49, 50]).

4.3 Exemplar

Consider the need for secure web services in the context of compute-intensive applications. A natural place to focus basic research efforts is on computational problems that are hard to solve but easy to check. NP -complete problems are prime examples. Such a problem cannot be solved in polynomial time (assuming $P \neq NP$), and yet is easy to check, in the case of a "yes" instance due to its membership in NP . Within this class, let us further restrict our attention to problems that are FPT (Fixed-Parameter Tractable) [51].

A problem of size n , and parameterized by k , is FPT if it can be decided in $O(f(k)n^c)$ time, where f is an arbitrary function and c is a constant independent of both n and k . Algorithms for FPT generally operate in two stages. The first stage, termed "kernelization," is aimed at condensing an arbitrarily difficult instance into its combinatorial kernel or core. The goal is to make the kernel's size some small function of the relevant parameter (e.g., see [52]). The second stage, known as "branching," is used to explore the search space of the kernel efficiently. It is branching that requires the vast majority of time, space and communication (e.g., see [53]). By kernelizing sequentially, but branching across the web, we achieve:

- *Verifiability.* Membership in NP means that we can usually expect to be able to check a candidate solution quickly. This is a critical feature, ensuring that a faulty or malicious processor cannot invalidate or subvert our computation.
- *Security.* We break the search space into disjoint sections and distribute them out to different processing elements. Each element knows only its share of the given instance, which is of course advantageous should the problem be sensitive. Even if two or more elements are untrustworthy and work in collusion, they cannot deduce the entire instance. Any attempt to exploit intercepted transmissions is similarly thwarted, thereby containing damage from intrusion. Strong concealment of the total problem is a natural part of this method.
- *Scalability.* As a computation, an FPT-based approach scales wonderfully. Branching translates to a most flexible form of partitioning. There are no *a priori* lower or upper bounds on the degree of parallelism that can be utilized. Furthermore, almost any architectural model will do, from tightly coupled parallel systems to widely distributed grids. This process can be viewed as something akin to a real-time, secure version of `seti@home` or `folding@home`.
- *Robustness.* The kernelization-plus-branching algorithm design paradigm requires no explicit communication

between remote processing elements. If a limited number of elements or links fail or become unreliable, we are able to add, delete or shift branching segments around at will, thereby ensuring at worst a graceful form of degradation and preventing catastrophic failure.

5 Summary and Conclusions

Agent-based computing combined with vision of autonomic computing represents an important new paradigm both for Artificial Intelligence and, more generally, Computer Science. It has the potential to significantly improve the theory and the practice of modeling, designing, and implementing SCI systems. Yet, to date, there has been little systematic analysis of what makes the agent-based approach such an appealing and powerful computational model. Moreover, even less effort has been devoted to discussing the inherent disadvantages that stem from adopting an agent-oriented view. Here both sets of issues are explored. The standpoint of this paper has been the role of agent-based software in solving complex, real-world problems of security and. In particular, it was argued that the development of robust, cyber defensible survivable software systems requires autonomous agents that can complete their objectives while situated in a dynamic and uncertain environment, that can engage in rich, high-level social interactions, and that can operate within flexible organizational structures.

Some people claim that agent-based computing (ABC) can significantly improve our ability to model, design and build complex, distributed software systems. Indeed, a high degree of correspondence exists between the requirements of complex system development paradigms and the key concepts and notions of agent-based computing. The ABC approach will likely succeed as a mainstream software engineering (SE) paradigm because it is a logical evolution from contemporary SE approaches to and because it is well suited to developing software for open systems. In contrast, ABC has the characteristic of unpredictable interactions. The strong possibility of emergent (nondeterministic) behavior in the wrong context is an inherent drawback. However, one important countermeasure is that long-term means of addressing these problems, a social level characterization of agent-based systems was advocated as a promising point of departure. Agent-based computing should be seen in its broader context as a general-purpose model of computation that naturally encompasses autonomic distributed and concurrent systems

6 References

- [1] F. T. Sheldon and K. Jerath, Assessing the Effect of Failure Severity, Coincident Failures and Usage-Profiles on the Reliability of Embedded Control Systems, *To Appear ACM Symposium on Applied Computing*, Nicosia Cyprus, 2004.
- [2] F. T. Sheldon and S. A. Greiner, Composing, Analyzing and Validating Software Models to Assess the Performability of Competing Design Candidates, *Annals of Software Engineering (On Software Reliability, Testing and Maturity)*, vol. 8, 1999.
- [3] F. T. Sheldon, S. Greiner, and M. Benzinger, Specification, safety and reliability analysis using Stochastic Petri Net models,

10th Int. Wkshp on Software Specification and Design, San Diego, CA, 2000, 123-132.

[4] F. T. Sheldon, K. Jerath, and S. A. Greiner, Examining Coincident Failures and Usage-Profiles in Reliability Analysis of an Embedded Vehicle Sub-System, *Proc Ninth Int'l Conf. on Analytical and Stochastic Modeling Techniques [ASMT 2002]*, Darmstadt Germany, June 3-5, 2002, 558-563.

[5] J. O. Kephart and D. M. Chess, The Vision of Autonomic Computing, *IEEE Computer Magazine*, 2003, 41-50.

[6] N. R. Jennings, On Agent-based Software Engineering, *Artificial Intelligence*, vol. 117 (2), 2000, 277-96.

[7] F. Sheldon, T. Potok, A. Krings, and P. Oman, Critical Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies, *Int'l Jr. Power and Energy Systems (Spec. Theme Blackout)*, 2004, To Appear.

[8] F. T. Sheldon and H. Y. Kim, Testing Software Requirements with Z and Statecharts Applied to an Embedded Control System, *To Appear: Software Quality Journal*, 2004.

[9] A. W. Krings, W. S. Harrison, N. Hanebutte, C. S. Taylor, M. McQueen, and S. Matthews, An Agent Supported Bottom-Up Approach to Computer and Network Survivability, *Int'l Conf. Dependable Systems and Networks (Supplement of to DSN-2001)*, Goteborg Sweden, 2001, B70-71.

[10] C. Taylor, P. Oman, and A. Krings, Assessing Power Substation Network Security and Survivability: A Work in Progress Report, *Proc. Int'l Conf. on Security and Management (SAM'03)*, Las Vegas, 2003.

[11] H. Y. Kim, Jerath, K. and Sheldon, F.T., "Assessment of High Integrity Components for Completeness, Consistency, Fault-Tolerance and Reliability," in *Component-Based Software Quality: Methods and Techniques*, vol. LNCS 2693, A. Vallecillo, Ed. (Heidelberg: Springer-Verlag, 2003) 259-86.

[12] B. Liscouski and W. J. S. Elliott, "Causes of the August 14 Blackout in the United States and Canada," NRCAN/USDOE (US-Canada Power System Outage Task Force), Wash. DC, Interim Report, Nov. 2003.

[13] E. J. Lerner, "What's wrong with the Electric Grid?" *The Industrial Physicist*, Vol. 9, Issue 5, (Accessed: Nov. 1, 2003) <http://www.tipmagazine.com> Last Updated: Jan. 2004.

[14] A. Krings and P. Oman, A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures, *HICSS-36 Minitrack on Secure Survivable SW Sys*, Hawaii, 2003, 334a-44.

[15] F. T. Sheldon and H. Y. Kim, Validation of Guidance Control Software Requirements for Reliability and Fault-Tolerance, *IEEE Proc. RAMS*, Seattle, Jan. 2002, 312-318.

[16] C. Tristram, From Artificial Intelligence to Artificial Biology? *Technology Review*, vol. 106 (9), 2003, 40.

[17] NERC, *An Approach to Action for the Electricity Sector, Ver. 1* (Princeton, NJ: N. American Electric Reliability Council, 2001).

[18] T. E. Potok, M. T. Elmore, J. W. Reed, and F. T. Sheldon, VIPAR: Advanced Information Agents Discovering Knowledge in an Open and Changing Environment, *Proc. 7th World Multiconf. On Systemics, Cybernetics and Informatics Spec. Session on Agent-Based Computing*, Orlando, July 27-30, 2003, 28-33.

[19] F. T. Sheldon, M. T. Elmore, and T. E. Potok, An Ontology-Based Software Agent System Case Study, *IEEE Proc. Int'l Conf. on Information Technology: Coding & Computing*, Las Vegas, Apr. 28-30, 2003, 500-06.

[20] T. E. Potok, L. Phillips, R. Pollock, A. Loebl, and F. T. Sheldon, Suitability of Agent-Based Systems for Command and Control in Fault-tolerant, Safety-critical Responsive Decision Networks, *ISCA 16th Int'l Conf. on Parallel and Distributed Computer Systems (PDCS)*, Reno, Aug. 13-25, 2003, 283-290.

[21] F. T. Sheldon, K. Jerath, and H. Chung, Metrics for Maintainability of Class Inheritance Hierarchies, *Jr. of Software Maintenance and Evolution*, vol. 14 (3), 2002, 147-160.

[22] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman, Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack, *ACM Wkshp on Scientific Aspects of Cyber Terrorism*, Wash. DC, Nov. 2002.

[23] C. Taylor, A. Krings, and J. Alves-Foss, Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening, *Proc. ACM Wkshp on Scientific Aspects of Cyber Terrorism*, Wash. DC, Nov. 2002.

[24] C. Taylor, A. Krings, W. S. Harrison, N. Hanebutte, and M. McQueen, Considering Attack Complexity: Layered Intrusion Tolerance, *DSN 2002 Wkshp on Intrusion Tolerance*, June 2002.

[25] P. Oman, E. Schweitzer, and J. Roberts, Protecting the Grid From Cyber Attack, Part II: Safeguarding IEDS, Substations and SCADA Systems, *Utility Automation*, vol. 7 (1), 2002, 25-32.

[26] C. Taylor, P. Oman, and A. Krings, Assessing Power Substation Network Security and Survivability: A Work in Progress Report, *Proc. Int'l Conf. on Security and Management (SAM'03)*, Las Vegas, 2003, 281-287.

[27] Z. Zhou, Sheldon, F.T. and Potok, T.E., Orlando, July 31 - Aug. 2, 2003, Modeling with Stochastic Message Sequence Charts, *IIS Proc. Int'l. Conf. on Computer, Communication and Control Technology*, Orlando, FL, 2003.

[28] F. T. Sheldon, M. T. Elmore, and T. E. Potok, An Ontology-Based Software Agent System Case Study, *Int'l Conf on Information Technology Coding and Computing (ITCC)*, Las Vegas, Nevada, USA, 2003.

[29] T. Potok, Elmore, M., Reed, J. and Sheldon, F.T., VIPAR: Advanced Information Agents Discovering Knowledge in an Open and Changing Environment, *SCI 2003 Proc. 7th World MultiConf on Systemics, Cybernetics and Informatics (Special Session on Agent-Based Computing)*, Orlando, 2003.

[30] F. T. Sheldon, T. Potok, and K. Kavi, Multi-Agent Systems for Knowledge Management and Decision Networks, *Informatica*, vol. 28 (SI Agent Based Computing), 2004, To Appear.

[31] T. E. Potok, Phillips, L., Pollock, R., Loebl, A. and Sheldon, F.T., Suitability of Agent-Based Systems for Command and Control in Fault-tolerant, Safety-critical Responsive Decision Networks, *ISCA 16th Int'l Conf. on Parallel and Distributed Computer Systems (PDCS)*, Reno NV, 2003.

[32] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman, Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack, *ACM Wkshp on Scientific Aspects of Cyber Terrorism (SACT)*, Wash. DC, 2002.

[33] C. Taylor, A. Krings, and J. Alves-Foss, Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening, *Proc. ACM Wkshp on Scientific Aspects of Cyber Terrorism, (SACT)*, Wash. DC, 2002.

[34] C. Taylor, A. Krings, W. S. Harrison, N. Hanebutte, and M. McQueen, Considering Attack Complexity: Layered Intrusion Tolerance, *Int'l Conf on Dependable Systems and Networks (Wkshp on Intrusion Tolerance)*, 2002.

[35] A. S. Rao and M. P. Georgeff, BDI Agents: From theory to practice, *Int'l Conf. on Multi-Agent Sys*, San Fran., 1995, 312-319.

[36] K. M. Kavi, M. Aborizka, and D. Kung, A framework for the design of intelligent agent based real-time systems, *Proc. 5th Int'l Conf. on Algorithms and Architectures for Parallel Processing*, Beijing, 2002, 196-200.

[37] A. Krings, W. Harrison, A. Azadmanesh, and M. McQueen, Scheduling Issues in Survivability Applications using Hybrid Fault Models, *To Appear Parallel Processing Letters*, 2004.

- [38] A. W. Krings, W. S. Harrison, M. H. Azadmanesh, and M. McQueen, The Impact of Hybrid Fault Models on Scheduling for Survivability, *Int'l Wkshp on Scheduling in Computer- and Manufacturing Systems (Seminar 02231, Report 343)*, Schloss Dagstuhl, Germany, 2002.
- [39] F. T. Sheldon, K. Jerath, and S. A. Greiner, Examining Coincident Failures and Usage-Profiles in Reliability Analysis of an Embedded Vehicle Sub-System, *9th Int'l Conf. on Analytical and Stochastic Modeling Techniques [ASMT 2002]*, Darmstadt Germany, 2002, 558-563.
- [40] A. Krings and P. Oman, Secure and Survivable Software Systems, *IEEE HICSS-36, Minitrack on Secure and Survivable Software Systems*, Big Island, Hawaii, 2003, 334a.
- [41] W. S. Harrison, A. Krings, N. Hanebutte, and M. McQueen, On the Performance of a Survivability Architecture for Networked Computing Systems, *IEEE Proc. HICSS-35*, Hawaii, 2002, 1-9.
- [42] C. Taylor, A. Krings, W. S. Harrison, and N. Hanebutte, Merging Survivability System Analysis and Probability Risk Assessment for Survivability Analysis, *IEEE DSN 2002 Book of FastAbstracts*, 2002.
- [43] A. W. Krings and M. H. Azadmanesh, A Graph Based Model for Survivability Applications, *To Appear Electronic Journal of Operations Research (EJOR)*, 2004.
- [44] A. Krings and P. Oman, A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures, *HICSS-36 Minitrack on Secure and Survivable Software Systems*, Hawaii, Jan. 2003, 334a-44.
- [45] A. W. Krings, Agent Survivability: An Application for Strong and Weak Chain Constrained Scheduling, *HICSS-37, Minitrack on Security and Survivability in Mobile Agent Based Distributed Systems*, Big Island, Hawaii, Jan. 2004, To Appear.
- [46] F. T. Sheldon, K. M. Kavi, W. W. Everett, R. Brettschneider, J. T. Yu, and R. C. Tausworthe, Reliability Measurement: From Theory to Practice, *IEEE Software*, 1992, 13-20.
- [47] S. Chessa and P. Santi, Comparison based system-level fault diagnosis in ad-hoc networks, *20th IEEE Symp. On Reliable Distributed Systems*, 2001, 257-266.
- [48] F. P. Preparata, G. Metze, and R. T. Chien, On the Connection Assignment Problem of Diagnosable Systems, *IEEE Transactions on Computers*, vol. EC-16, 1967, 848 - 854.
- [49] A. Krings, S. Harrison, N. Hanebutte, C. Taylor, and M. McQueen, Attack Recognition Based on Kernel Attack Signatures, *Int'l Sym. on Information Systems and Engineering (ISE)*, Las Vegas, 2001, 413-419.
- [50] C. Taylor, W. Harrison, A. Krings, N. Hanebutte, and M. McQueen, Low-Level Network Attack Recognition: A Signature-Based Approach, *IEEE Proc. PDCS*, Anaheim, 2001, 570-574.
- [51] R. G. Downey and M. R. Fellows, *Parameterized Complexity* (Springer-Verlag, 1999).
- [52] F. N. Abu-Khzam, R. L. Collins, M. R. Fellows, M. A. Langston, W. H. Suters, and C. T. Symons, Kernelization Algorithms for the Vertex Cover Problem: Theory and Experiments, *Proc. Wkshp on Algorithm Engineering and Experiments (ALENEX)*, 2004, To Appear.
- [53] F. N. Abu-Khzam, M. A. Langston, and P. Shanhag, Scalable Parallel Algorithms for Difficult Combinatorial Problems: A Case Study in Optimization, *Proc., Int'l Conf on Parallel and Distributed Computing and Systems*, 2003, 563-568.

7 Apx: Cyber-Security in the Electric Sector

Excerpt from [12]: The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting the

electric power system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that, although it caused no outages, the infection blocked commands that operated other power utilities. The report, "NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Worm Infection," is available at web site <http://www.nrc.gov/reading-rm/docollections/news/2003/03-108.html>.

This example, among others, highlights the increased vulnerability to disruption via cyber means faced by North America's critical infrastructure sectors, including the energy sector. Of specific concern to the U.S. and Canadian governments are the Supervisory Control and Data Acquisition (SCADA) systems, which contain computers and applications that perform a wide variety of functions across many industries. In electric power, SCADA includes telemetry for status and control, as well as Energy Management Systems (EMS), protective relaying, and automatic generation control. SCADA systems were developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, are now, for a variety of business and operational reasons, either directly or indirectly connected to the global Internet. For example, in some instances, there may be a need for employees to monitor SCADA systems remotely. However, connecting SCADA systems to a remotely accessible computer network can present security risks. These risks include the compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms.

Security has always been a priority for the electricity sector in North America; however, it is a greater priority now than ever before. Electric system operators recognize that the threat environment is changing and that the risks are greater than in the past, and they have taken steps to improve their security postures. NERC's Critical Infrastructure Protection Advisory Group has been examining ways to improve both the physical and cyber security dimensions of the North American power grid. This group includes Canadian and U.S. industry experts in the areas of cyber security, physical security and operational security. The creation of a national SCADA program to improve the physical and cyber security of these control systems is now also under discussion in the United States. The Canadian Electrical Association Critical Infrastructure Working Group is examining similar measures.