CRITICAL ENERGY INFRASTRUCTURE SURVIVABILITY, INHERENT LIMITATIONS, OBSTACLES, AND MITIGATION STRATEGIES

F. Sheldon,* T. Potok,* A. Krings,** and P. Oman**

Abstract

Information systems now form the backbone of nearly every government and private system, from targeting weapons to conducting financial transactions. 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 a nation. The blackout of August 14, 2003, affected, in the U.S. alone, eight states and fifty million people and could cost up to $5 billion.[1] The DOE/NERC interim reports[2] indicate the outage progressed as a chain of relatively minor events consistent with previous cascading outages caused by a domino reaction. The increasing use of embedded distributed systems to manage and control our technologically complex society makes knowing the vulnerability of such systems essential to improving their intrinsic reliability/survivability. Our discussion employs the power transmission grid.

Key Words

Infrastructure vulnerability, reliability, cyber-security, software agent Petri net models

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, environmental insult, etc.). Structured models allow the system reliability to be derived from determined reliabilities of its components. A complex embedded system is composed of numerous 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 an understanding of the likelihood of failures occurring in a system and can provide deterministic insight to developers about inherent (and defined) "weaknesses" in the system components and among systems [1, 2].

[1] N. Gibbs, Lights Out, *Time Magazine*, pp. 24–39, Aug. 25, 2003.

[2] The DOE/NERC reports are at http://reports.energy.gov/ and ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/Blackout Summary-Draft-6b.pdf.

* Applied Software Engineering Research, Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA; e-mail: {SheldonFT, PotokTE}@ornl.gov

** Department of Computer Science, University of Idaho, Moscow, ID 83844 USA; e-mail: {Krings, Oman}@cs.uidaho.edu

(paper no. 434-801)

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. The information technology that supports such infrastructures has enabled society to be simultaneously more complex, effective, efficient, and, unfortunately, more vulnerable to cyber threats.

Understanding the grid's inherent weaknesses begins with understanding its physical behaviour. The vast system

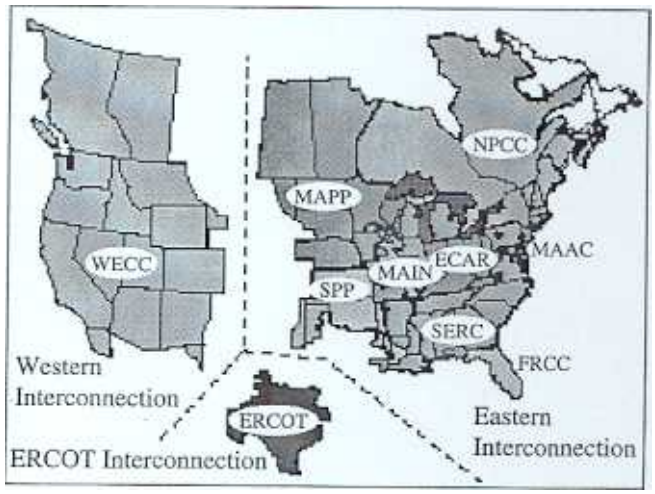

Figure 1. NERC interconnections.

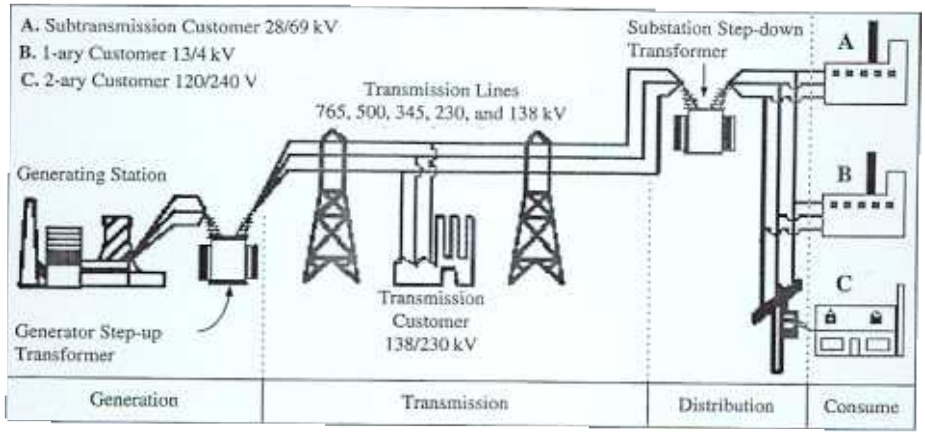

Figure 2. Basic structure of the electric system.

of electricity generation, transmission, and distribution that covers the U.S. is essentially a single machine extending into Canada and Mexico in unique ways, probably the world's biggest. This solitary network is physically and administratively subdivided into three "subnets": the Eastern Interconnect, covering portions of the U.S. and Canada east of the Rocky Mountains; the Western Interconnect, covering portions of the U.S., Canada, and Mexican peninsula west of the Rocky Mountains; and the Texas Interconnect run by the Electric Reliability Council of Texas (ERCOT), which covers most of Texas and extends into Mexico (see Fig. 1). Power transmission within each subnet is dominated by AC lines with all generation tightly synchronized to the same 60-Hz cycle (see Fig. 2) [3]. The subnets are joined by DC-links; consequently, coupling is much better controlled between interconnects than within them (i.e., capacity of the transmission lines between the subnets is also far less than within the subnets). Experts widely agree that failures of the power-transmission system are a nearly unavoidable product of a collision between the system physics and the economic regulatory rules. The nation must either physically transform the system to accommodate the new rules, or change the rules to better mesh with the power grid's physical behaviour [4].

2.1 Survival Strategies

The Energy Infrastructure Survivability (EIS), as described here using Generalized Stochastic Petri Nets (GSPNs), is a hierarchical method used to assess and implement survivability mechanisms and mitigate common mode 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. Assessing EIS comprises two phases. First, individual components of the infrastructure are evaluated in isolation to derive individual component survivability (CS, see Figs. 3 and 4). The process identifies feasible *mitigation* mechanisms on a per component basis. In the second phase (see Fig. 5), the CS is introduced into the system-at-large, resulting in a map of the EIS. This approach leverages individual CS models to create

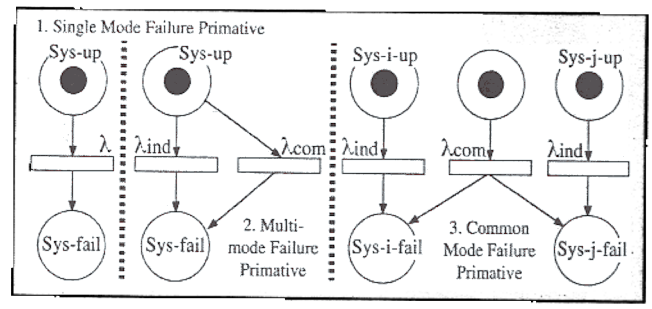

Figure 3. Phase I simple GSPN primitives.

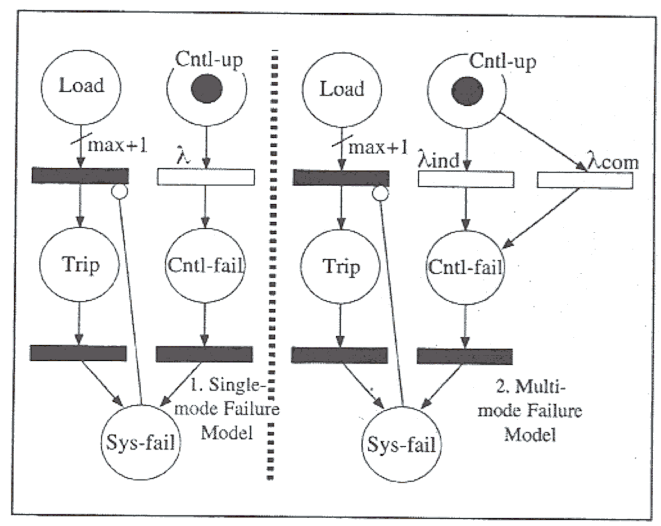

Figure 4. Phase I hybrid primitives.

hierarchical structures with increased system survivability (e.g., against failures due to the complexity of engaging unanticipated component interactions).[3] To codify and systematize this approach, the focus is on models that aid in the process of ensuring system integrity [5] by selecting mit-

[3] We suspect that sources of common mode faults are widespread, so we define modelling primitives that use GSPNs for representing interdependency failures in very simple control systems. This work provides an initial step in creating a framework for analyzing reliability/survivability characteristics of infrastructures with both hardware and software controls (see Section 3.1).

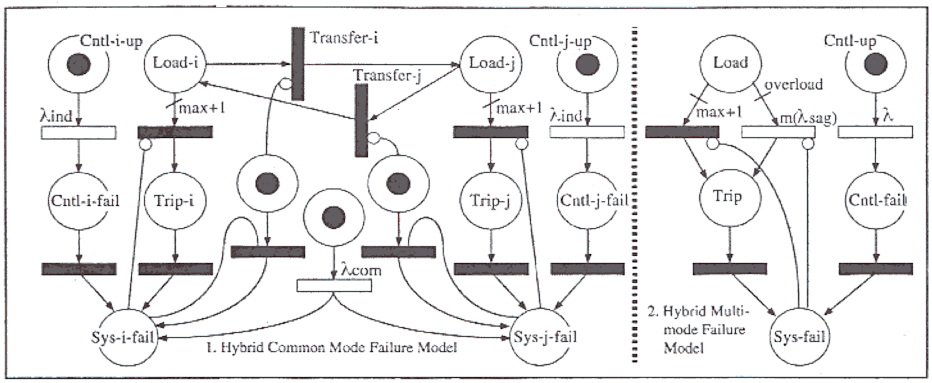

Figure 5. Phase II components composed into system models.

igation 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 critical infrastructure 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. For example, the physical system is represented as a collection of state variables and their values along with some operations that change its state. In such approaches (e.g., the Z notation [6]), a mathematically based language (i.e., employing set theory and logic) provides a powerful structuring mechanism that can be used to construct system models from smaller subsystem/component models. In Z, schemas are composed into hierarchical structures that model physical systems, including their physical properties, protocols, networks, communications, computers, and software as well as their dependent interrelationships.[4] Moreover, the mathematical model represents the intended/unacceptable behaviour of the systems under *all* possible constraints and can be augmented with nondeterminism including empirical knowledge.

2.2 Networks of Control

As the industries that use and develop critical infrastructure have become more computerized, the risk of digital disruption from a range of adversaries has increased. The threats range from casual hackers seeking a thrill to terrorists out to destroy our societal technological mainstays, from failures due to the normal complexity of systems and their interconnections to natural calamities.[5] In 1997, the U.S. president Clinton formed the President's Commission on Critical Infrastructure Protection (PCCIP). This group identified eight critical infrastructure systems whose disruption would have an enormous impact. Power grid vulnerabilities and mitigations were documented in the PCCIP's National Security Telecommunications Advisory Committee (NSTAC) *Electric Power Risk Assessment* report, which made several recommendations for increasing security. Their suggestions included a broad program of education and awareness, among them sharing of information between government and industry and cooperatively developing risk assessment methods. Unfortunately, and partly due to the reorganization of the industry towards a more competitive model, little progress has been made in securing the electric power grid in the five years since the NSTAC report. Funding is needed to develop and deploy technologies and methodologies for designing systems that are less vulnerable to compromise through means such as improved cyber assurance and are more self-healing and resilient. Given that the electrical generation and distribution industry is accepting a new market-based model for the future, how investment in our *common ground* infrastructure will be encouraged through incentives remains an open issue [7]. The common ground has proven essential to our digital economy, but has become fragile and has been 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 communication pathways, detecting intruders or abnormal operations, and mechanisms for distributed intelligent adaptive control to effect more flexible and adaptive systems.

3. Long-Term Reliability and Survivability

Subsequent to the attacks of September 11, 2001, concern about the security and reliability of the United States' critical infrastructures increased sharply. A comprehensive and coordinated approach to ensure national security became necessary. The energy infrastructure (EI) underpins all other infrastructures: telecommunication, transportation, banking, manufacturing, plus essential services such as food, water, and health. The EI is comprised of the generation, transmission, and distribution of electricity and oil and natural gas production, storage, refining,

[4] Z, a model-based specification language used in combination with natural languages, is equipped with an underlying theory that enables nondeterminism to be removed mechanically from abstract formulations to result in more concrete "formal" specifications.

[5] C. Perrow (in *Normal Accidents* [1984]) analytically addresses system accidents as multiple failures that interact in unanticipated ways.

processing, pipeline transmission, and distribution.

3.1 Common Mode Failures

It is now apparent that critical EIs and essential utilities have been optimized for reliability in benign operating environments. As such, 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. Strategies are needed to define independent, survivable software control systems for automated regulation of critical infrastructures like electric power, telecommunications, and emergency communications systems. For example, in [8], the August 10, 1996, cascading blackout is studied to identify and analyze common mode faults leading to the cascading failure.

3.2 Cyber Security

Power substation control networks exhibit a number of factors that contribute to the difficulty of implementing cyber security. Foremost is the geographic distribution of these networks, spanning hundreds of miles with network components located in isolated remote locations. A related concern is the sheer number of devices connected to a single network (i.e., thousands of accessible devices may be open to compromise). The sheer size and the number of access points greatly increases the risk of cyber attack against electronic equipment in a substation [9].

Our approach would use intelligent software agents (SAs) [10–12] (each modelled as an individual component) to deploy new and user-friendly data collection and management capabilities that possess inherent resiliency to failures in control networks [13, 14] as well as maintenance/evolution properties that promote low cost of ownership [14, 15]. SAs enable secure, robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber attack, and so on [16, 17], as well as intelligent adaptive control [18].

3.3 Inherent Obstacles

The diversity of equipment and protocols used in the communication and control of power systems is staggering.[6] 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, the variety of communications media used is to access this equipment. It is not uncommon to find commercial telephone lines, wireless, microwave, private fiber, and Internet connections within substation control networks [19].

3.4 Mitigation Strategies

Previous work in this area has presented details of both threats and mitigation mechanisms for substation communication networks [19, 20]. In [21], 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, 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 threats [22].[7]

4. Summary and Conclusion

An important advantage here is that EI implementations can be targeted more easily, as they involve a bottom-up approach. The applicability of the approach to multiple energy sectors within the infrastructure scope is broad because the degree of impact (i.e., to improve or sustain energy assurance) on the EI is determined at the component level [21, 23]. In addition, as an extension to the EIS approach, we may identify how specific EI communication protocols and mechanisms [10] can be modelled and mapped onto fault-models for understanding the impacts of common mode failures and usage profiles, including load scheduling [1, 24], to identify weak points (assisting risk assessment/mitigation) in the system [8, 25, 26].

Moreover, there are cost-effective ways to apply survivability methods [17, 27] based on redundancy and dissimilarities to the communication networks controlling the EI. This provides several advantages: (1) the result would use a transformation model [8, 25] to map the specific protocol and/or application to a graph and/or Petri net(s) [28]; (2) interesting optimization criteria can be applied to facilitate survivability based on redundancy and 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 (4) using agreement solutions to augment the graph to achieve the required survivability (e.g., 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 become less vulnerable to malicious attack(s), given that the threshold of faults dictated by the agreement algorithms is not violated.

[6] Substation control systems/protocols include proprietary SCADA (Supervisory Control And Data Acquisition) protocols or Ethernet, EIA232/485, Utility Communication Architecture, ControlNet, Vendor propriety protocol, Internet, V.32, V.34, WAP, WEP, DNP, Modbus, Profibus, and Fieldbus. These protocols connect protective Intelligent Electronic Devices to controllers (e.g., programmable logic controllers, remote terminal units, local PCs, and SCADA devices).

[7] FERC (Federal Energy Regulatory Commission) adopted NERC (North American Energy Reliability Council) security policies as standard (education/compliance audits presumably will follow).

Table 1
1988–2003 CERT/CC Statistics: Yearly Computer Security Incidents Reported

	1988–1989		1990–1999										2000–2003			
Year	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03
Incidents	6	132	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	52,658	82,094	137,529

Total incidents reported (1988–2003): 319,992; ***Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.*** **Please see http://www.cert.org for specific details.**

The CERT/CC publishes statistics for (1) Number of incidents reported, (2) Vulnerabilities reported, (3) Security alerts published, (4) Security notes published (5) Mail messages handled, and (6) Hotline calls received. The present CERT Coordination Center grew from a small computer security incident response team formed at the SEI (Software Engineering Institute) by the Defense Advanced Research Projects Agency (DARPA) in 1988. The small team grew quickly and expanded its activities. Now, the Networked Systems Survivability Program manages the CERT/CC. The manager of that program reports to the director of the Software Engineering Institute (a non-academic unit of Carnegie Mellon Univ.).

4.1 Cyber Security Is a Vulnerability

Malicious acts targeting computers have reached epidemic proportions. All *critical* infrastructures in the U.S. have computer-automated controls (energy, finance, telecommunications, water, transportation, health care). Table 1 gives an accounting of the yearly increase in reported computer security incidents as recorded by the CERT/CC [29]. These data are illustrated in Fig. 6, showing the dramatic increase, and are contrasted against known causes of power outages (reported by NERC). Roughly 11% of all outages have unknown causes. Eliminating cyber security vulnerabilities may prevent such outages.

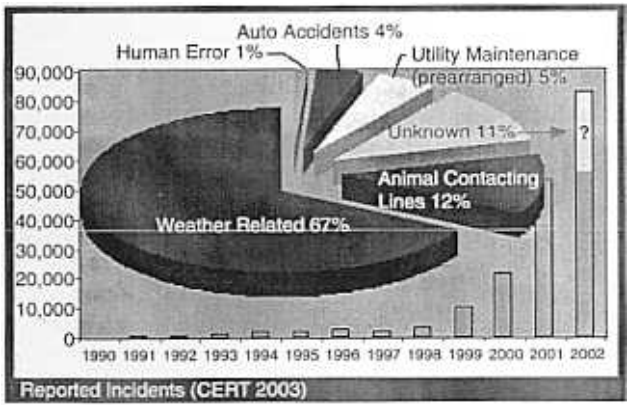

Figure 6. What causes power outages (cyber security)?

On August 15, 2003, the U.S.'s President Bush and Canada's Prime Minister Chrétien directed that a joint task force be established to investigate the causes of the August 14 blackout and how to reduce the possibility of future outages. The task force created three working groups to assist in the first phase of the investigation, an Electric System Working Group, a Nuclear Working Group, and a Security Working Group (SWG), with the purpose of overseeing and reviewing investigations of the conditions and events in their respective areas and determining whether they may have caused or affected the blackout. The objective of the SWG was to determine what role, if any, a malicious cyber event may have played in causing or contributing to the outage. Analysis to date provides no evidence that malicious actors are responsible for or contributed to the outage. The SWG acknowledges reports of al-Qaeda claims of responsibility, yet those claims are not consistent with findings to date [3]. No evidence exists suggesting that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. SWG analysis has brought to light certain concerns with respect to the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some operators to view adequately the status of electric systems outside their immediate control. Further data collection and analysis is being undertaken to test these findings and to examine more fully the cyber security aspects of the power outage. The outcome of the Electric System Working Group (ESWG) root cause analysis will serve to focus this work, as the significant cyber events are identified and examined from a security perspective.

5. List of Acronyms

DOE—United States Department of Energy
NERC—North American Electric Reliability Council
EIS—Energy Infrastructure (EI) Survivability
GSPN—Generalized Stochastic Petri Nets
WECC—Western Electricity Coordinating Council
ERCOT—Electric Reliability Council of Texas
MAPP—Mid-Continent Area Power Pool
SPP—Southwest Power Pool
MAIN—Mid-America Interconnected Network
NPCC—Northeast Power Coordination Council
ECAR—East Central Area Reliability Coordination Agreement
SERC—Southeast Electric Reliability Council
MAAC—Mid-Atlantic Area Council
FRCC—Florida Reliability Coordinating Council

Acknowledgement

The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce

the published form of this contribution, or allow others to do so, for U.S. Government purposes.

References

[1] F.T. Sheldon, K. Jerath, & S.A. Greiner, Examining coincident failures and usage-profiles in reliability analysis of an embedded vehicle sub-system, *Proc. 9th Int. Conf. on Analytical and Stochastic Modeling Techniques (ASMT 2002)*, Darmstadt Germany, June 3–5, 2002, 558–563.

[2] F.T. Sheldon, S. Greiner, & M. Benzinger, Specification, safety and reliability analysis using stochastic Petri net models, *10th Int. Workshop on Software Specification and Design*, San Diego, CA, 2000, 123–132.

[3] B. Liscouski & 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), Washington, DC, Interim Report, November 2003.

[4] E.J. Lerner, What's wrong with the electric grid? *The Industrial Physicist*, *9*(5), http://www.tipmagazine.com (Accessed: November 1, 2003).

[5] F.T. Sheldon & H.Y. Kim, Validation of guidance control software requirements for reliability and fault-tolerance, *IEEE Proc. Reliability and Maintainability Symp.*, Seattle, WA, January 2002, 312–318.

[6] J. Jacky, *The way of Z: Practical programming with formal methods* (Cambridge: Cambridge University Press, 1997).

[7] F.T. Sheldon, T.E. Potok, A. Loebl, A.W. Krings, & P. Oman, Energy infrastructure survivability, inherent limitations, obstacles and mitigation strategies, *IASTED Int. Conf. PowerCon*, New York, NY, 2003, 49–53.

[8] A.W. Krings & P.W. Oman, A simple GSPN for modeling common mode failures in critical infrastructures, *HICSS-36 Minitrack on Secure and Survivable Software Systems*, Big Island, Hawaii, paper STSSS02, January 2003 (10 pages).

[9] NERC, *An approach to action for the electricity sector, Version 1* (Princeton, NJ: North American Electric Reliability Council, 2001).

[10] Z. Zhou, F.T. Sheldon, & T.E. Potok, Modeling with stochastic message sequence charts, *IIIS Proc. Int. Conf. on Computer, Communication and Control Technology*, Orlando, FL, July 31–August 2, 2003 (8 pages). Available at www.csm.ornl.gov/~sheldon/pubs.html

[11] T.E. Potok, M.T. Elmore, J.W. Reed, & 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, FL, *9*, July 27–30, 2003, 28–33.

[12] F.T. Sheldon, M.T. Elmore, & T.E. Potok, An ontology-based software agent system case study, *IEEE Proc. Int. Conf. on Information Technology: Coding & Computing*, Las Vegas, NV, April 28–30, 2003, 500–506.

[13] T.E. Potok *et al.*, Suitability of agent-based systems for command and control in fault-tolerant, safety-critical responsive decision networks, *ISCA 16th Int. Conf. on Parallel and Distributed Computer Systems (PDCS)*, Reno, NV, August 13–25, 2003, 283–290.

[14] F.T. Sheldon, T.E. Potok, & K.M. Kavi, Multi-agent systems for knowledge management and decision networks, *Informatica*, *28* (Special Issue on Agent Based Computing), 2004 (to appear).

[15] F.T. Sheldon, K. Jerath, & H. Chung, Metrics for maintainability of class inheritance hierarchies, *Journal of SW Maintenance and Evolution*, *14*(3), 2002, 147–160.

[16] D. Conte de Leon, J. Alves-Foss, A.W. Krings, & P. Oman, Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack, *ACM Workshop on Scientific Aspects of Cyber Terrorism (SACT)*, Washington DC, November 2002, paper #6 (10 pages). Available at www.cs.uidaho.edu/~krings/publications.html

[17] C. Taylor, A. Krings, & J. Alves-Foss, Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening, *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism (SACT)*, Washington DC, November 2002, paper #7 (9 pages). Available at www.cs.uidaho.edu/~krings/publications.html

[18] C. Taylor, A.W. Krings, W.S. Harrison, N. Hanebutte, & M. McQueen, Considering attack complexity: Layered intrusion tolerance, *Proc. DSN 2002 Workshop on Intrusion Tolerance, International Conference on Dependable Systems and Networks (DSN)*, Washington DC, 23–26 June 2002 (5 pages). Available at www.cs.uidaho.edu/~krings/publications.html

[19] P. Oman, E. Schweitzer, & J. Roberts, Protecting the grid from cyber attack, part 2: Safeguarding IEDS, substations and SCADA systems, *Utility Automation*, *7*(1), 2002, 25–32.

[20] P. Oman, A. Risley, J. Roberts, & E. Schweitzer, Attack and defend tools for remotely accessible control and protection equipment in electronic power systems, *Texas A&M Conf. for Protective Relay Engineers*, College Station, TX, 2002, paper #14 (26 pages). Available at www.selinc.com/techpprs.htm

[21] C. Taylor, P. Oman, & A. Krings, Assessing power substation network security and survivability: A work in progress report, *Proc. Int. Conf. on Security and Management (SAM '03)*, Las Vegas, NV, 2003, 281–287.

[22] DOE, *Vulnerability assessment and survey program: Lessons learned and best practices*, U.S. Department of Energy Assurance, September 28, 2001.

[23] H.Y. Kim, K. Jerath, & F.T. Sheldon, Assessment of high integrity components for completeness, consistency, fault-tolerance and reliability, in *Component-based software quality: Methods and techniques*, ed. M.P.A. Cechich & A. Vallecillo (Heidelburg: Springer, 2003).

[24] A.W. Krings, W.S. Harrison, M.H. Azadmanesh, & M. McQueen, The impact of hybrid fault models on scheduling for survivability, *Int. Workshop on Scheduling in Computer and Manufacturing Systems*, Seminar 02231, Report 343, Schloss Dagstuhl, Germany, June 2–6, 2002. Available at www.dagstuhl.de

[25] A.W. Krings & P.W. Oman, Secure and survivable software systems, *IEEE Proc. HICSS-36, Minitrack on Secure and Survivable Software Systems*, Big Island, Hawaii, paper STSSS00, January 2003.

[26] W.S. Harrison, A.W. Krings, N. Hanebutte, & M. McQueen, On the performance of a survivability architecture for networked computing systems, *IEEE Proc. HICSS-35*, Big Island, Hawaii, 2002, 195–103.

[27] C. Taylor, A. Krings, W.S. Harrison, & N. Hanebutte, Merging survivability system analysis and probability risk assessment for survivability analysis, *IEEE DSN 2002 Book of FastAbstracts*, June 2002.

[28] F.T. Sheldon, K.M. Kavi, W.W. Everett, R. Brettschneider, J.T. Yu, & R.C. Tausworthe, Reliability measurement: From theory to practice, *IEEE Software*, July 1992, 13–20.

[29] CERT/CC, State of the practice of computer security incident response teams, Carnegie-Mellon University, http://www.cert.org (Accessed: January 7, 2004).

Biographies

Frederick T. Sheldon is a research staff member at ORNL. Formerly, he was Assistant Professor at WSU, CU and research staff at DaimlerChrysler (Germany), Lockheed Martin, Raytheon, and NASA Langley/Ames Research Centers. His research is concerned with developing and validating models, methods, and supporting tools for the creation of safe, secure, and correct software/systems. He received his Ph.D. at UT Arlington in 1996 and founded the Software Engineering for Dependable Systems Lab in 1999. He is a Senior Member of the IEEE

and member of ACM, IASTED, AIAA, Tau Beta Pi, and Upsilon Pi Epsilon. He has published in numerous journals and international conferences.

Thomas E. Potok is a leader of the Applied Software Engineering Research Group at the ORNL (http://computing.ornl.gov/cse_home/aser.shtml). He was at IBM's Software Solutions Laboratory in Research Triangle Park for 14 years, where he held various software development and management positions. He is currently a PI on several internal R&D and DoD projects. His B.Sc., M.Sc., and Ph.D. in computer engineering are from NC State University. He is also an adjunct faculty member at the University of Tennessee, a member of the ACM/IEEE Computer Society, and has authored over 40 publications and filed four software patents.

Axel Krings is a Associate Professor of Computer Science and Engineering at the University of Idaho (http://www.cs.uidaho.edu/~krings). Krings has worked in system survivability for the past seven years, with support from DOD, DOE INEEL, and NSA. Prior to joining the faculty at Idaho he was an Assistant Professor at the Technical University of Clausthal, Germany. His research work focuses on complex systems reliability, fault tolerance, and survivability. He has published in numerous journals and international conferences. He earned his M.Sc. and Ph.D. in computer science at the University of Nebraska at Lincoln. He is a Senior Member of the IEEE.

Paul Oman has worked in information security for the past six years, with support from DOD, NSA, NSF, and NIST. He spent the last two years working on security improvements within the electric power industry as Senior Research Engineer at Schweitzer Engineering Labs, Pullman, WA. Prior to joining SEL he was Professor and Chair of Computer Science at the University of Idaho and was awarded the distinction of Hewlett-Packard Engineering Chair during his last seven years there. Dr. Oman has published over 100 papers and technical reports on computer security, computer science education, and SE. He is a past editor of *IEEE Computer* and *Software* journals and serves as a Senior Member in the IEEE.