ENERGY INFRASTRUCTURE SURVIVABILITY, INHERENT LIMITATIONS, OBSTACLES AND MITIGATION STRATEGIES

Frederick Sheldon, Tom Potok, Andy Loebl
Applied Software Engineering Research[1]
Oak Ridge National Laboratory
Oak Ridge, TN 37831 USA
SheldonFT | PotokTE | LoeblA@ornl.gov

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

ABSTRACT

The blackout of August 14, 2003 affected 8 states and fifty million people and could cost up to $5 billion[2]. Yet another press release claims it may have cost Ohio manufacturers $1.1 billion, based on a poll of 275 companies. Preliminary reports[3] indicate the outage progressed as a chain of relatively minor events, rather than a single catastrophic failure. This is consistent with previous cascading outages, which were caused by a domino reaction[4]. The increasingly ubiquitous use of embedded systems to manage and control our technologically complex society makes our homeland security even more vulnerable. Therefore, knowing how vulnerable such systems are is essential to improving their intrinsic reliability/survivability (in a deregulated environment knowing these important properties is equally essential to the providers). **Key Words** – Network Vulnerability, Cyber Security, Stochastic Modeling.

1 Introduction

Reliability, the probability that a system will deliver its intended functionality for a specified period and under specific conditions [1, 2], *is one inherently important measure of quality*. 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 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 about 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 [3, 4].

2 Network Vulnerability

Understanding the grid's inherent weaknesses starts with its physical behavior. The vast 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. Power transmission within each subnet is dominated by AC lines with all generation tightly

[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.

[2] N. Gibbs, Lights Out, Time Magazine, pp. 24-39, Aug. 25, 2003

[3] *August 14, 2003 Outage Sequence of Events*, US/Canada Power Outage Task Force, September 12, 2003, (see the NERC web site ftp://www.nerc.com/pub/sys/all_updl/docs/pressrel/BlackoutSummary-Draft-6b.pdf.

[4] Experts widely agree that such failures of the power-transmission system are a nearly unavoidable product of a collision between the physics of the system and the economic rules that now regulate it. To avoid future incidents, 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 behavior (see http://www.tipmagazine.com/tip/INPHFA/vol-9/iss-5/p8.html).

synchronized to the same 60-Hz cycle[5]. These system grids (or subnets) are joined to each other by DC links, so the coupling is much better controlled between the interconnects than within them[6].

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 these infrastructures has enabled society to be simultaneously more complex, more effective and more efficient. Unfortunately, the reliance on these infrastructure networks has made us more vulnerable and the on-going problem of securing critical infrastructures from cyber threats has become more acute.

2.1 Survival and Mitigation Strategies

The Energy Infrastructure Survivability (EIS) Map 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) modeling, simulation, and analysis to understand and enable fundamentally robust and fault-tolerant systems, and (c) systems architecture that can overcome vital limitations. The EIS Map comprises 2 phases. First, individual components of the infrastructure are evaluated in isolation to derive a component survivability map (CSM). The CSM identifies feasible *mitigation* mechanisms on a per component basis. In the second phase, the CSM is extended to the system-at-large, resulting in the EIS Map. Thus, the survivable systems approach leverages individual CSM's to constitute the merging of the component maps with the purpose of creating hierarchical structures with increased system survivability (e.g., against failures due to the complexity of engaging unanticipated component interactions). To codify and systematize this approach the focus is on models that aid in the process of ensuring system integrity [5] by selecting mitigation mechanisms that maximize individual and system wide objectives. In this way, optimization techniques can be added showing how resources can 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 (or 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 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[7]. Moreover, the mathematical model represents the intended/unacceptable behavior of the systems under *all* possible constraints and can be augmented with non-determinism including empirical knowledge (e.g., unanticipated contingencies).

2.2 Networks of Computer 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. Our reliance on an increasingly complex technologically based society and infrastructure is not a new development[8] In 1997 President Clinton formed the President's Commission on Critical Infrastructure Protection (PCCIP) to investigate threats and mitigation strategies for cyber controlled and other critical networks. This group identified eight critical infrastructure systems whose disruption would have an enormous impact. The most *critical* infrastructure identified was the electric power grid. Power grid vulnerabilities and mitigations were documented in the PCCIP's National Security Telecommunications Advisory Committee (NSTAC) *Electric Power Risk Assessment* report. The PCCIP and NSTAC made several recommendations for increasing the security of the electric infrastructures. Their suggestions included a broad program of education and awareness including sharing of information between government and industry and cooperatively developing risk assessment methods. Unfortunately, and perhaps 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 was published. 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

[5] Technically speaking, this is not exactly true. There exist an important third high-volume component of DC lines that is also easier to manage and stabilize while still conducting high volumes of electricity from generation sources. The more controllable interconnects among these three is DC.

[6] The capacity of the transmission lines between the subnets is also far less.

[7] Z is classified as a model-based specification language that is equipped with an underlying theory that enables non-determinism to be removed mechanically from abstract formulations to result in more concrete specifications. In combination with natural language, it can be used to produce a formal specification.

[8] Charles Perrow in his 1984 book entitled; Normal Accidents attempts to analytically address system accidents as multiple failures that interact in unanticipated ways.

generation and distribution industry is accepting a new market-based model for the future, concerns regarding how investment in the infrastructure will be incentivized remain an open issue. Under regulatory control, investors were guaranteed (i.e., via amortization and interest returns on utility bonds) a return on long-term infrastructure investments. However, in a market-based situation where profit dominates over the common good of the consumer (e.g., Enron), it's unclear just what will happen to incentivize modernization (e.g., perhaps decentralized [distributed] energy promising reliability and self-sufficiency). In any case, what was formerly a natural "common ground" economic process (i.e., infrastructure modernization begets a return on investment) for the industry is now a "profit driven" economic process where modernization does not realize a profit to the funding authority. This is especially true because the amortization cycle time on power plants and grid infrastructures is so long as compared to typical profit horizons.

This infrastructure is now the 'common ground' which has proven essential to our digital economy, but which 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 communication pathways, detecting intruders or abnormal operations, mechanisms for non-centralized intelligent and adaptive control to effect more flexible and adaptive systems. The new Federal Energy Regulatory Commission (FERC) model discourages *any* investment that does not show a profit to the investor in a reasonable period of time. Costs due to collateral losses from the August 2003 blackout include GDP losses that are not easily accounted for by Return On Investment (ROI) models. Also, estimates of repair and disruption costs are not <u>all</u> countable (e.g., loss of life, endangerment of people, etc.) are also not accounted for by ROI models.

3 Long Term Reliability and Survivability

Subsequent to the attacks of September 11, 2001, concern about the security and reliability of the nation's critical infrastructures *increased sharply*. A comprehensive and coordinated approach to ensure their 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, processing, pipeline transmission, and distribution. Under the direction of the DOE's Office of Energy Assurance (OEA), the National Energy Technology Laboratory (NETL) is working with state, local government, industry, academia, and other national laboratories to develop a comprehensive and defensible strategy to develop and deploy technologies, with emphasis on technologies that can help assure the long term reliability and stability of the energy infrastructure.

3.1 Common Mode Failures

It is now apparent that Critical EIs (CEIs) 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 [7], we describe the August 10, 1996 cascading blackout, and use that description to identify and analyze common mode faults leading to the cascading failure. We suspect that sources of common mode faults in real-time control systems are widespread and many, so we define modeling primitives that allow us to use Generalized Stochastic Petri Nets (GSPN) for representing interdependency failures in very simple control systems. As such, this work has provided an initial step toward creating a framework for modeling and analyzing reliability and survivability characteristics of critical infrastructures with both hardware and software controls.

3.2 Cyber Security

Power substation control networks exhibit a number of factors that contribute to the difficulty of implementing cyber security. Foremost among the challenges facing the power industry is the geographic distribution of these networks, spanning hundreds of miles with network components located in isolated, physically remote spots. A related security concern is the sheer number of devices connected to a single network. There could be thousands of accessible devices that would be open to compromise should an intruder gain access. The sheer size of the network and the number of access points contained within greatly increases the risk of cyber attack against electronic equipment in a substation [8].

3.3 Inherent Limitations and Obstacles

Another challenge to the power industry is the diversity of equipment and protocols used in the communication and control of power systems. Substation control systems, along with the protocols used by these systems, include proprietary SCADA (Supervisory Control And Data Acquisition) protocol or Ethernet, EIA232/485, UCA (Utility Communication Architecture), ControlNet, Vendor propriety protocol, Internet, V.32, V.34, WAP, WEP, DNP, Modbus, Profibus, and Fieldbus. These protocols are used to connect the protective Intelligent Electronic Devices (IEDs) to the control equipment like the Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), communication processors, local

PC's, and SCADA devices. 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 [9].

3.4 Mitigation Strategies

Previous work in this area has presented details of both threats and mitigation mechanisms for substation communication networks [9, 10]. In [11], the most important mitigation actions that would reduce the threat of cyber intrusion are highlighted. The greatest reduction from the threat of cyber intrusion can be achieved by enacting a program of cyber security education and training combined with an enforced security policy[9]. We believe these two strategies will have the greatest impact on securing power networks because of the lag in cyber security knowledge within the industry. The education along with the enforcement will assist with counteracting both external and insider threats. The insider threat is considered to be more serious and potentially more damaging due to the insider's knowledge of electric power system operations [12].

4 Conclusions

The advantage of the EIS Map approach, especially in the first phase, is that EI implementations in the long haul can be targeted easier, as it is a bottom-up approach. In fact, the applicability of our proposed technology/ methodology demonstration 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 EI is determined at the component level [11, 13]. Furthermore, semi-intelligent software agents [14-16] may be used to deploy new and user-friendly data collection and management capabilities, thereby increasing the likelihood of successful commercialization due to their inherent resiliency to failures in control networks [17, 18] as well as software maintenance/evolution properties that promote low cost of ownership [18, 19]. Using software agents enables secure and robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber attack etc., [20, 21], as well as intelligent adaptive control [22]. In addition, as an extension to the EIS Map, we may identify how specific EI communication protocols and mechanisms [14] can be modeled and mapped onto fault-models for understanding the impacts of common mode failures and usage profiles, including load scheduling [3, 23, 24], to identify weak points (assisting risk assessment/mitigation) in the system [7, 25, 26].

Moreover, there are cost effective ways to apply survivability methods [21, 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 [7, 25] to map the specific protocol and/or application to a graph and/or Petri Net(s) [2], (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 (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 invulnerable to malicious attacks, as long as the threshold of faulty components dictated by the agreement algorithms is not violated.

The whole field of system fault diagnosis, which originated from the Preparata, Metz and Chien (PMC) model can be applied. The fundamental question is, "Who tests who, and how is the test implemented to identify faulty components?" In this vein, "diagnostics" are specified which determine if the system is robust.

5 A Comparative Epilogue

In the early 1980's, the automobile industry was obsessed with automation. While engaged in implementing automation at one Ford plant, an interesting irony was discovered. The initial step that was undertaken as the foundation for automation was to document the assembly line and refine its processes to yield an automation process that was sufficient to save manufacturing costs equal to the anticipated investment in robotics and systems. But the refinement process was effective enough to increase production without the billions of dollars needed for building and installing the automated systems. Consequently, Ford stopped when the analysis was complete and never proceeded with the automation transformation step. The same might be said for the electrical systems grid – merely documenting its components and systems may enlighten the industry with respect to what needs to be changed. That is, the documentation step may shed sufficient light on grid vulnerabilities that wholesale and drastic alterations are deemed unnecessary.

6 References

[1] M. A. Vouk, Software reliability engineering, *IEEE Annual RAMS*, Los Angeles, CA, 2000.

[2] F. T. Sheldon, et al., Reliability Measurement: From Theory to Practice, *IEEE Software*, July 1992, pp. 13-20.

[9] FERC has adopted the security policies of the NERC (North American Energy Reliability Council) as its Standard. Education presumably will follow, as will audits for compliance.

[3] 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, pp. 558-563.

[4] F. T. Sheldon, S. Greiner, and M. Benzinger, Specification, safety and reliability analysis using Stochastic Petri Net models, *10th ACM Int. Wkshp on Software Specification and Design*, San Diego, CA, 2000, pp. 123-132.

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

[6] J. Jacky, *The way of Z: Practical Programming with Formal Methods* (Cambridge U. Press, 1997).

[7] 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.

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

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

[10] P. Oman, et al., Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electronic Power Systems, *TX A&M Conf. for Protective Relay Engineering*, College Station, 2002.

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

[12] DOE, Vulnerability Assessment and Survey program: Lessons learned and Best Practices, *U.S. Dept. of Energy Assurance*, Sept. 28, 2001.

[13] H. Kim, K. Jerath, and F. Sheldon, Assessment of High Integrity Components for Completeness, Consistency, Fault-Tolerance and Reliability, in *Component-Based Software Quality: Methods and Techniques*, M. P. A. Cechich, and A. Vallecillo, Eds. Heidelburg: Springer LNCS 2693, 2003, pp. 259-86.

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

[15] T. Potok, et al., VIPAR: Advanced Information Agents Discovering Knowledge in an Open and Changing Environment, *Proc. 7th World Mulitconf. On Systemics, Cybernetics and Informatics: Agent-Based Computing*, Orlando, July 27-30, 2003.

[16] F. T. Sheldon, M. T. Elmore, and T. E. Potok, An Ontology-Based Software Agent System Case Study, *IEEE Conf. on Info Technology: Coding & Cmptng*, Las Vegas, Apr. 28-30, 2003, pp. 500-06.

[17] 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'l Conf. PDCS*, Reno NV, Aug. 13-25, 2003.

[18] F. T. Sheldon, T. E. Potok, and K. M. Kavi, Multi-Agent Systems for Knowledge Management and Decision Networks, *Informatica*, *28*(Special Issue on Agent Based Comp.), 2004, pp. Pending.

[19] F. T. Sheldon, K. Jerath, and H. Chung, Metrics for Maintainability of Class Inheritance Hierarchies, *Jr. of SW Maint. and Evolution (John Wiley, London)*, *14*(3), May 2002, pp. 147-160.

[20] D. Conte de Leon, et al., Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack, *ACM Wkshp Sci Aspects of Cyber Terror*, Wash DC, Nov. 2002.

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

[22] C. Taylor, et al., Considering Attack Complexity: Layered Intrusion Tolerance, *Proc. DSN 2002 Wkshp on Intrusion Tolerance*, Jun. 2002.

[23] A. Krings, et al., Scheduling Issues in Survivability Applications using Hybrid Fault Models, *Parallel Processing Ltrs*, 2003 (to appear).

[24] A. Krings, et al., 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, June 2-6 2002.

[25] A. Krings and P. Oman, Secure and Survivable Software Systems, *IEEE Proc. HICSS-36, Minitrack on Secure and Survivable Software Systems*, Big Island, Hawaii, Jan. 2003, pp. 334a.

[26] W. S. Harrison, et al., On the Performance of a Survivability Architecture for Networked Computing Systems, *IEEE Proc. HICSS-35*, Big Island, Hawaii, Jan. 2002, pp. 1-9.

[27] C. Taylor, et al., Merging Survivability System Analysis and Probability Risk Assessment for Survivability Analysis, IEEE DSN 2002 Book of Fast Abstracts, June 2002.