Managing Secure Survivable Critical Infrastructures To Avoid Vulnerabilities

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

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 the Nation. The blackout of August 14, 2003 affected 8 states and fifty million people and could cost up to $5 billion[2]. The DOE/NERC interim reports[3] indicate the outage progressed as a chain of relatively minor events consistent with previous cascading outages caused by a domino reaction[4]. 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.

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 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 [1, 2].

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 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 synchronized to the same 60-Hz cycle (see Fig. 1). 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).

---

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

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

[4] 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 behavior (see http://www.tipmagazine.com/tip/INPHFA/vol-9/iss-5/p8.html).

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) modeling, and analysis to understand and enable fundamentally robust and fault-tolerant systems, and (c) systems architecture that can overcome vital limitations. Assessing EIS comprises 2 phases. First, individual components of the infrastructure are evaluated in isolation to derive individual component survivability (CS, see Figs. 2 and 3). The process identifies feasible *mitigation* mechanisms on a per component basis. In the second phase (see Fig. 4), the CS is composed into the system-at-large, resulting in a map of the EIS. 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)[5]. To codify and systematize this approach the focus is on models that aid in the process of ensuring system integrity [3] 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 critical infrastructure survivability.

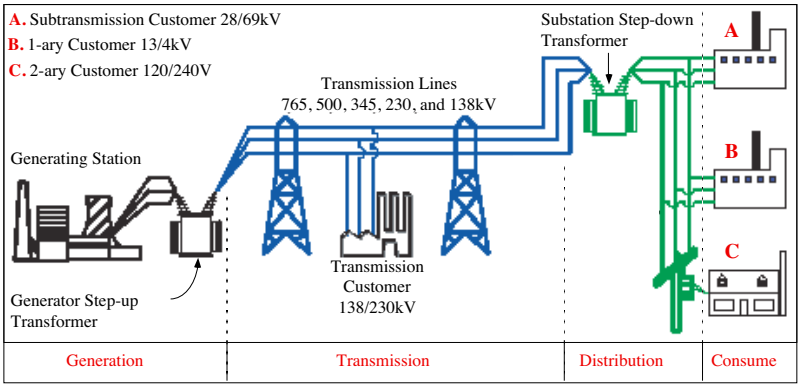

Figure 1. Basic structure of the Electric System

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 [4]), 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[6]. 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.

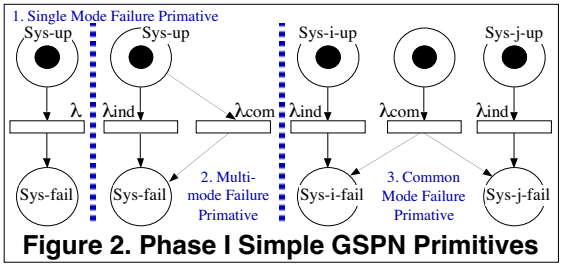

Figure 2. Phase I Simple GSPN Primitives

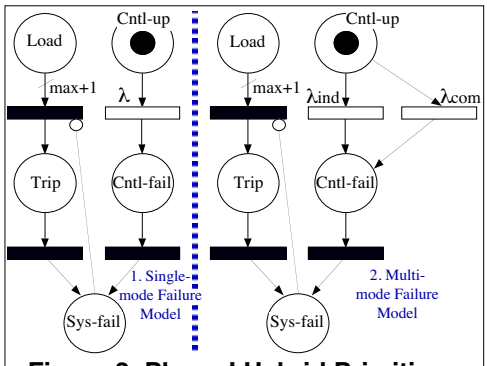

Figure 3. Phase I Hybrid Primitives

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[7]. In 1997 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. The. 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 including sharing of information between government and industry and

[5] We suspect that sources of common mode faults are widespread, so we define modeling 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 paragraph 3.1).

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

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

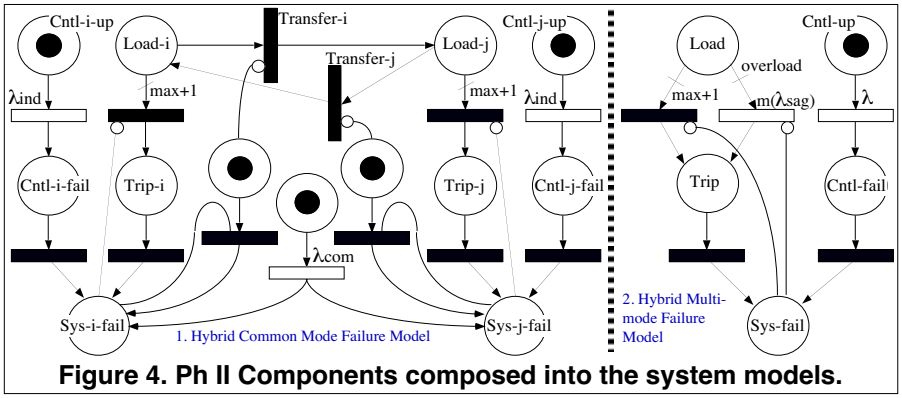

Figure 4. Ph II Components composed into the system models.

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, concerns regarding how investment in our *common ground* infrastructure will be incentivized remain an open issue [5]. The 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 communication pathways, detecting intruders or abnormal operations, 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 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.

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 [6], the Aug. 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 [7].

Our approach would use intelligent software agents (SAs) [8-10] (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 [11, 12] as well as maintenance/evolution properties that promote low cost of ownership [12, 13]. SAs enable secure, robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber attack etc., [14, 15], as well as intelligent adaptive control [16].

3.3 Inherent Obstacles

The diversity of equipment and protocols used in the communication and control of power systems is staggering[8]. 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 [17].

3.4 Mitigation Strategies

Previous work in this area has presented details of both threats and mitigation mechanisms for substation

[8] 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 PC's, and SCADA devices.

communication networks [17, 18]. In [19], 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[20][9].

4 Summary and Conclusions

An important advantage here is that EI implementations can be targeted easier, as it is a bottom-up approach. The approach applicability 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 [19, 21]. In addition, as an extension to the EIS approach, we may identify how specific EI communication protocols and mechanisms [8] can be modeled and mapped onto fault-models for understanding the impacts of common mode failures and usage profiles, including load scheduling [1, 22], to identify weak points (assisting risk assessment/mitigation) in the system [6, 23, 24].

Moreover, there are cost effective ways to apply survivability methods [15, 25] based on redundancy and dissimilarities to the communication networks controlling the EI. This provides *several advantages*: (1) the result would use a transformation model [6, 23] to map the specific protocol and/or application to a graph and/or Petri Net(s) [26], (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 less vulnerable to malicious attack(s), given the threshold of faults dictated by the agreement algorithms is not violated.

5 References

[1] F. T. Sheldon, K. Jerath, and S. A. Greiner, Examining Coincident Failures and Usage-Profiles in Reliability Analysis of an Embedded Vehicle Sub-System, ASMT02, pp. 558-563.

[2] F. T. Sheldon, S. Greiner, and M. Benzinger, Specification, safety and reliability analysis using Stochastic Petri Net models, ACM IWSSD, San Diego, 2000, pp. 123-132.

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

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

[5] F. Sheldon, et al., Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies, IASTED Int'l Conference PowerCon, New York, NY, 2003.

[6] A. Krings and P. Oman, A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures, HICSS-36 Minitrack on Secure/Survivable Software Systems, Hawaii, 2003.

[7] NERC, An Approach to Action for the Electricity Sector, Ver. 1 (Princeton, NJ: NERC, 2001).

[8] Z. Zhou, et. al., Modeling with Stochastic Message Sequence Charts, IIIS Proc. CCCT, Orlando, July 2003.

[9] T. Potok, et al., VIPAR: Advanced Information Agents Discovering Knowledge in an Open and Changing Environment, Proc. SCI, Agent-Based Computing, Orlando, July 2003.

[10] F. T. Sheldon, et. al., An Ontology-Based Software Agent System Case Study, IEEE ITCC, Las Vegas, 2003, pp. 500-06.

[11] T. E. Potok, et al., Suitability of Agent-Based Systems for Command and Control in Fault-tolerant, Safety-critical Responsive Decision Networks, ISCA PDCS, Reno, Aug, 2003.

[12] F. T. Sheldon, et. al., Multi-Agent Systems for Knowledge Management and Decision Networks, Jr. Informatica, 2004.

[13] F. Sheldon, K. Jerath, and H. Chung, Metrics for Maintainability of Class Inheritance Hierarchies, Jr. SME (J. Wiley and Sons), vol. 14 (3), pp. 147-160, 2002.

[14] D. Conte de Leon, et al., Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack, ACM SACT, Wash. DC, Nov. 2002.

[15] C. Taylor, et. al., Risk Analysis & Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening, ACM SACT, Wash. DC, Nov. 2002.

[16] C. Taylor, et al., Considering Attack Complexity: Layered Intrusion Tolerance, IEEE Proc. DSN , June 2002.

[17] 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, pp. 25-32.

[18] P. Oman, et al., Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electronic Power Systems, TAM Conf. for PRE, College Station, TX, 2002.

[19] C. Taylor, P. Oman, and A. Krings, Assessing Power Substation Network Security and Survivability: Progress Rpt., Proc. Int'l Conf. on Security and Management, Las Vegas, 2003.

[20] DOE, "Vulnerability Assessment and Survey program: Lessons learned and Best Practices," U.S. DOE Sept. 28, 2001.

[21] H.Y. Kim, et. al, "Assessment of High Integrity Components for Completeness, Consistency, Fault-Tolerance and Reliability," in Component-Based Software Quality: Methods & Techniques, Eds: M. Cechich, A. Vallecillo, LNCS 2693, 2003, pp. 259-86.

[22] A. W. Krings, et al., The Impact of Hybrid Fault Models on Scheduling for Survivability, Wkshp on Scheduling in Computer- and Manufacturing Systems, Seminar 02231, Rpt. 343, Schloss Dagstuhl, June 2002.

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

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

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

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

[9] FERC adopted NERC (North American Energy Reliability Council) security policies as standard (education/compliance audits may follow).