Assessing Power Substation Network Security and Survivability: A Work in Progress Report[1]

Carol Taylor, Paul Oman, and Axel Krings
Computer Science Department
University of Idaho, Moscow, Idaho 83844
{*ctaylor, oman, krings*}@cs.uidaho.edu

Abstract

This paper reports our experiences with identifying cyber-based threats to the survivability of power substation control networks. Observations from the initial application of vulnerability and hardening assessment techniques have been presented. The paper also discusses the state of the power industry cyber security, which appears to lag behind the state-of-the-practice in both network security and ultra-reliable systems design.

Keywords: Cyber security, electric power security, assessment techniques

1. Introduction

The on-going problem of securing our critical infrastructures from cyber threats is becoming more acute as Americans focus on terrorism and its consequences. As a nation, we have become dependent on the computer networks that support our daily lives and the reliance on these networks have made us more vulnerable to their disruption. As the critical infrastructure industries have become more computerized, the risk of digital disruption from a range of adversaries has increased. The threat groups range from casual hackers seeking a thrill to terrorists out to destroy the American way of life [12]. Our reliance on an increasingly computerized infrastructure is not new and was identified as a problem over five years ago. In 1997, President Clinton formed a group, the President's Commission on Critical Infrastructure Protection (PCCIP) to investigate threats and mitigation strategies for cyber controlled critical networks [16]. This group identified eight critical infrastructure systems whose disruption would have an enormous impact on all of our lives.

One of the most critical infrastructure systems identified was the electric power grid since this system supports all other non-military infrastructures. Power grid vulnerabilities and mitigations were documented in the PCCIP's National Security Telecommunications Advisory Committee (NSTAC) *Electric Power Risk Assessment* report [13]. The PCCIP and NSTAC reports made several recommendations for increasing the security of our 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 [16]. Unfortunately, little progress has been made in securing the electric power grid in the five years since the NSTAC report was published.

Over the past two years we have been studying the vulnerability of the electric power grid to disruption from cyber based attacks. The approach we have taken is to construct a low-level analysis of the grid at the substation level, which was identified in 1997 by NSTAC as one of the most vulnerable parts of the power grid [13]. We have examined the threats, vulnerabilities and mitigation solutions of the distribution substation and its surrounding electronic communication

[1] Portions of this work were funded by grant #60NANB1D0116 from the National Institute of Standards and Technology, U.S. Dept. of Commerce.

network. While physical disruption is a very real part of overall threat to substations, our emphasis in this study was specifically cyber threats. Part of our research objective was to adapt existing vulnerability assessment methods and/or develop new approaches for evaluating substation control networks for cyber security threats. A number of assessment techniques were examined including a modified version of Survivable Systems Analysis (SSA) [6], Probability Risk Assessment (PRA) [7], a prototype expert system [3], and a set of checklists from power industry security standards.

One goal of this paper is to report the results of applying these techniques to the assessment of power substation control networks for cyber based attacks. Another goal is to report on the cyber security challenges still facing the electric power industry five years after the vulnerabilities were documented. Although we focus on electric power networks, our discussion and analyses pertain to all computer controlled complex systems. We present solutions from traditional computer security that should assist real-time networks in surviving a malicious cyber attack. Finally, we examine some of the underlying design issues typical of power substation networks that impact security efforts.

2. Current State of Power Networks

In conducting our research of power system networks we completed several on-site visits to power companies. During those visits, we were able to conduct site assessments and interact with people knowledgeable about the systems that communicate with and control the protective line control devices. While our direct contact was with a limited sample of sites we feel that our on-site experiences were fairly typical of the power industry as a whole. We base this assumption on personal power industry experience, supporting literature, and communication with power industry regulatory agencies. Previous work has presented detailed analysis of the cyber threats that face the electric power industry [14, 15]. In this section, we present and discuss those vulnerabilities that we feel pose the biggest obstacle to securing substation communication and control networks.

2.1 Current Vulnerabilities

The greatest vulnerability of the power substation control networks is the lack of cyber security awareness within the power industry. This problem was identified in the original PCCIP reports as a barrier to securing the electric power grid [13, 16]. On the surface, this appears to be a problem easily solved with a little awareness training in cyber security practices. However, this problem is much larger than it first appears, and is not immediately solvable. Lack of security awareness can be found at all levels of the industry from developers of systems and software that control the power grid to the operators of the power control systems and the power engineers themselves [15]. Table 1 shows a checklist of the known vulnerabilities documented in [13] that still exist and have been observed in recent assessment visitations conducted by the authors of this paper. It can be seen that all prior vulnerabilities still exist, and new ones, associated with emerging technologies and business needs, have come to bear.

Table 1. Power Grid Vulnerabilities

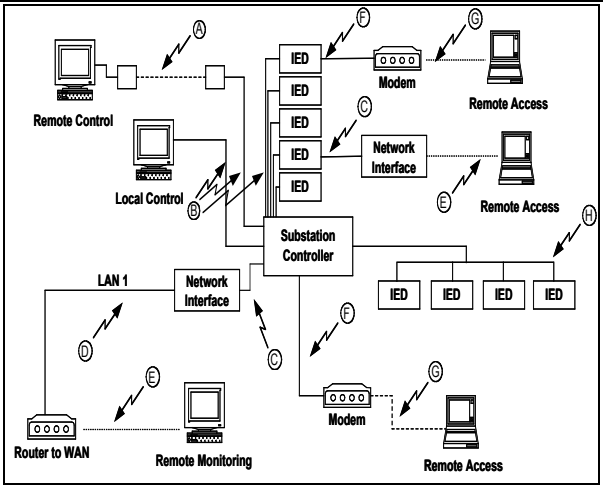
Documented Vulnerability	1997 NSTAC	2002 Visits
Weak Passwords Used	✓	✓
Default Passwords Not Changed	✓	✓
Passwords Posted Visibly	✓	✓
Shared Logins	✓	✓
Inconsistent or Non-existent Warning Banners	✓	✓
Personnel Unaware of Hacking Threat	✓	✓
Non-existent Security Policies	✓	✓
Unsecured Modem Access	✓	✓
IT Network Interconnectivity	✓	✓
Non-existent or Inadequate Intrusion Detection	✓	✓
Internet Connectivity	Non-existent	✓
Wireless Networks	Non-existent	✓
Commercialization of Utility Telecomms	Non-existent	✓

While recognition of the need for power system cyber security appears to be growing, it is increasing at a slow rate. There still appears to be a general lack of urgency in the attitude of power industry executives towards solving computer security problems [4]. There are many reasons and contributing factors for this industry complacency. Power industry deregulation has created competition, forcing power companies to trim development and work closer to their margins without extra resources [12]. As a consequence, new threats, like cyber security, require additional resources and have a lower priority compared to established business needs. Cyber control of power systems is relatively new in an industry that dates back to the 1900's. Executives that make company decisions are business oriented and lack the technical background to understand the risks and consequences of a cyber-generated attack [4].

2.2 Current Challenges

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 it greatly increases the risk of cyber attack against electronic equipment in a substation [12].

Another challenge to the power industry is the diversity of equipment and protocols used in the communication and control of power systems. Figure 1 presents a high-level diagram of electronic equipment typically used in a substation control system along with the protocols used by these devices. 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. In addition to the diversity of electronic control equipment is the variety of communications media to access this equipment. It is not uncommon to find commercial telephone lines, wireless, microwave, private fiber, and Internet connections within substation control networks [14].



A. Proprietary SCADA protocol or Ethernet
B. Proprietary, EIA232, EIA485, Ethernet, UCA, or ControlNet
C. Vendor Proprietary Protocol
D. Ethernet
E. Local Ethernet or Internet
F. EIA-232
G. V.32, V.34, WAP, or WEP
H. DNP, Modbus, Profibus, Fieldbus

Figure 1. Example Substation Protocols

3. Mitigation Strategies

Previous work has presented details of both threats and mitigation mechanisms for substation communication networks [14,15]. Table 2 highlights the most important mitigation actions that would reduce the threat of cyber intrusion. 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. 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 due to the insider's knowledge of electric power system operations [4]..

Table 2. Mitigation Actions

Action	Explanation
Cyber Security Education	Education creates employee cyber awareness; Employees assist with cyber security.
Enforcement of Cyber Security Policy	Policy enforcement should accompany education; A security policy is critical for cyber security.
Authentication Enforcement	Strong password policy; multi-factor authentication.
Enact Encryption	Communication data should be encrypted – encrypting modem or VPN device.
Firewalls, Virus Scanners, Intrusion Detection Systems	Network security devices for both corporate and power control networks will help reduce cyber threats.
Keep SCADA control and Corporate networks separate	Connecting critical SCADA control networks increases risk of intruder access.

Security policies mandating authentication, access restriction, and activity logging will have a fairly large impact on insider and intruder risks. Ideally, these types of mechanisms will be part of a larger security policy. Encrypting data sent over public telephone lines either through Virtual Private Network (VPN) or Public Key Infrastructure (PKI) technology will help insure privacy and prevent eavesdropping (e.g., sniffing) of important information. Similarly, implementing firewalls on corporate and SCADA networks plus using virus scanners and Intrusion Detection Systems (IDS) will assist in securing power system networks [15]. Finally, we note that SCADA networks should be kept isolated from corporate networks to eliminate the possibility of outsiders penetrating the corporate network and migrating to the more critical power communication and control networks [14].

4. Survivability and Vulnerability Assessment

Over the past two years we have explored a number of methods for determining the vulnerabilities and assessing the threats to power control networks. These techniques included standards-based checklists, a combined SSA/PRA approach, and an expert system analysis. Each technique will be described along with its usefulness in assessing the vulnerabilities and ultimate survivability of power control networks.

4.1 Standards Checklists

Prior to undertaking several on-site industry visits, we compiled checklists derived from industry standards and guidelines [8, 9, 10]. The standards documented recognized methods for electric power substation physical and electronic security, including secure communications. The lists proved useful in conducting the on-site security evaluations with managers, power engineers, network administrators, and control system operators. The checklists are currently under revision to enhance their usefulness for industry personnel to conduct self-assessment of substation network security.

While checklists are a useful place to begin a vulnerability assessment of power system cyber threats, they have a number of limitations. For example, the checklists require a certain level of knowledge and computer security expertise in the person performing the assessment, but as discussed before, this is frequently not the case in the electric power industry. In contrast, the checklists could be designed to be general, but would then miss important aspects of a network specific problem. In summary, we found checklists to be a good starting point, but not adequate for a thorough security assessment.

4.2 Survivability System Analysis / Probability Risk Assessment

Survivability System Analysis (SSA) is a relatively recent approach to the assessment and hardening of computer systems. SSA is particularly suitable for assessing unbounded networks with ill-defined boundaries and non-centralized control [6], such as power substation networks connected to corporate networks and/or connected to the Internet. These system interconnections greatly increase network boundaries. SSA emphasizes survivability, the continued operation of the essential services of a system in spite of deliberate compromise or natural failure of some components. Survivability

is defined as the capability of a system to complete its mission in a given time frame under the constraints of accident or attack. A key concept in survivable systems is the identification of essential services critical to the organization's mission that must be preserved over less critical services [6].

As a technique for assessing power system vulnerabilities to cyber related threats, SSA offers several advantages. Given the size and distributed nature of these networks it is infeasible to place the entire network under the same level of protection. The emphasis on the preservation of essential services as opposed to all services allows a power company to allocate their security resources where they are most needed. Another advantage of SSA is the detailed analysis of threat scenarios to the essential services. SSA requires scrutiny of the threats, identification of essential component vulnerabilities, and proposed mitigations of the vulnerabilities so that recognition, resistance and recovery from each threat is possible [6].

One problem with SSA is its lack of quantification. Without quantification it is difficult to measure system survivability and determine the success of the system in meeting its survivability objectives. In an effort to add quantification capability to SSA, we have combined Probability Risk Assessment (PRA) with SSA. PRA utilizes probabilities to determine the likelihood that adverse events will occur [7]. Probabilities are calculated from statistical sampling or historical records of the event of interest. In the absence of these sources, risk can be determined through solicitation of expert opinion. A PRA for cyber security threats involves quantification of the risk from these threats and the specification of mitigating actions including costs. Problems with PRA approaches include a lack of historical cyber security data for estimating risk, and the difficulty of analyzing risk for large networks [2].

Our combined approach, Risk Analysis and Probabilistic Survivability Assessment (RAPSA), seeks to leverage the strengths of both approaches [17]. First, SSA is used to partition the system into essential services and those less critical to the mission. In addition to the threat/intrusion scenarios required in SSA, the probability of risks for each intrusion scenario is added from PRA. Tools such as event and fault-tree analysis can help understand how equipment failure impacts the system. The final product of SSA is a survivability map showing detailed threat scenarios and defensive measures for the essential services. In RAPSA we add cost data to the map and shown how trade-offs via decision tree analysis can be used to achieve the best mitigation option for a given cyber threat [17]. The four stages of the RAPSA approach are summarized in Figure 2. The assessment method shows promise and is currently under development for assessing power network security.

Stage 1 – System Self-assessment
An analysis team performs a self-assessment to understand system mission objectives. Partition the system into services that are essential to the mission and those services that are identified.

Stage 2 – Threat Identification
Threats from cyber attacks are enumerated for the essential services identified in the previous step. Intrusion scenarios/ attack stages are outlined for the essential services. Vulnerabilities associated with each intrusion scenario are identified.

Stage 3 – Risk Quantification
Quantify the risks for each intrusion scenario. Event/fault trees will be used where needed to assist with understanding how attacks can be neutralized. Mitigation mechanisms will be proposed.

State 4 – Risk Mitigation Trade-off
Several types of tradeoff analyses are possible such as Partitioned Multi- Objective Risk Method (PMRM) or simple Decision Tree Analysis. Produce survivability map including risks and costs for mitigation strategies.

Figure 2. RAPSA Survivability Assessment

4.3 Expert System Analysis

Our third approach to vulnerability assessment of a power control network is to analyze the individual components using a prototype expert system [3]. As shown in Figures 3 and 4, Prolog was used to model the visibility conditions and implement the shortest path algorithm to find the most vulnerable device in the network [3].

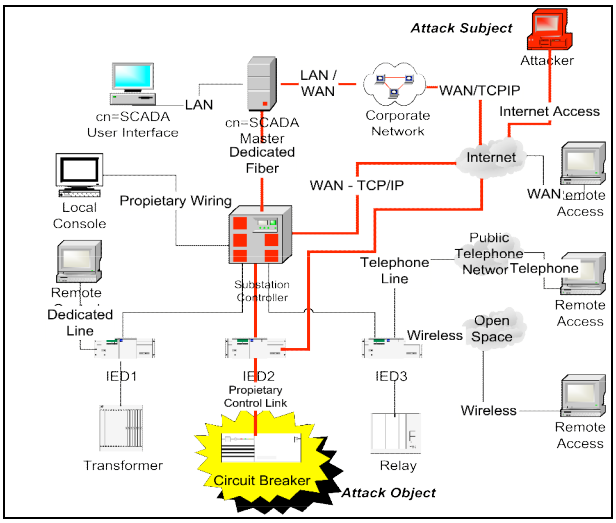


Figure 3. Example Substation Attack

Visibility paths from Internet to CircuitBreaker:

["Internet","SubstationController","IED2", "CircuitBreaker"] with vulnerability level = 10

["Internet","IED2","CircuitBreaker"] with vulnerability level = 7

["Internet","CorporateNetwork","SCADAMaster", "SubstationController","IED2", "CircuitBreaker"] with vulnerability level = 23

Most vulnerable visibility path from Internet to CircuitBreaker:

["Internet","CorporateNetwork","SCADAMaster", "SubstationController","IED2", "CircuitBreaker"] with vulnerability level = 23

Figure 4. Output of Expert System Vulnerability Assessment

A graph is used to model the system and a set of conditions is defined for each device that must be met in order for the device to be "visible" to the attacker. Visibility conditions are represented as edges between the nodes. Vulnerability of a particular device is found by adding up the visibility conditions in the visibility path to the device.

Identification of the vulnerable devices shows where security needs to be applied in order to mitigate the effects of an attack. This approach is currently under consideration for further development and testing with actual substation configurations.

5. Conclusion

In this paper, we have reported on our experiences with identifying cyber-based threats to the survivability of power substation control networks. Observations from the initial application of vulnerability and hardening assessment techniques have been presented. Since this is a work in progress report, these assessment approaches are initial efforts. Hence, it is difficult to tell how useful the appr will be in improving the overall security of power communication and control networks, but preliminary analysis shows they have merit in vulnerability identification and survivability enhancement. In looking at the current state of power industry cyber security, it appears to lag behind the state-of-the-practice in both network security and ultra-reliable systems design. In spite of the national emphasis on terrorism awareness, the power industry as a whole appears to be lacking in cyber security awareness. Unless this complacency changes, the power grid will continue to be susceptible to all forms of cyber-based intrusions and the future may see major disruption of power resulting from a cyber-based attack.

6. References

[1] Behrendt, K. and M. Dood, *Substation Relay Data and Communication*, Technical Report, Schweitzer Engineering Labs, Pullman, WA, 2000. Available from www.selinc.com.

[2] Blakley, B., E. McDermott, and D. Gear, "Information security is information risk management," *NSPW*, Cloudcroft, New Mexico, Sept. 2001.

[3] 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," *First Workshop on Scientific Aspects of Cyber Terrorism*, Washington D.C., November, 2002.

[4] DOE, *Vulnerability Assessment and Survey program: Lessons learned and Best Practices*, U.S. Department of Energy Assurance, September 28, 2001.

[5] Dolezilek, D., "*Case Study of a Large Transmission and Distribution Automation Project*", Technical Report, Schweitzer Engineering Labs, Pullman, WA, 2000. Available from www.selinc.com.

[6] Ellison, R. J., R. C. Linger, T. Longstaff, and N. R. Mead, "Survivable Network Systems Analysis: A Case Study," *IEEE Software*, July/August 1999, pp. 70-77.

[7] Haimes, Y., *Risk Modeling, Assessment, and Management***,** John Wiley and Sons, New York, NY, 1998.

[8] IEC, IEC 61850 TC 57, *Draft Standard for Communication Networks and Systems in Substations*, International Electrotechnical Commission, Geneva, Switzerland, 2002.

[9] IEEE, *IEEE Standard 1402-2000: Guide for Electric Power Substations Physical and Electronic Security*, IEEE Power Engineering Society, New York, NY, April 4, 2000.

[10] IEEE, *IEEE Draft Standard 1525: Draft Standard for Substation Integration, Protection, Control and Data Acquisition Communication*, IEEE Power Engineering Society, New York, NY, 2002.

[11] Krings, A., and P. Oman, "A Simple GSPN for Modeling Common Mode Failures in Critical Infrastructures," *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, Waikola, HI, January 2003.

[12] NERC, *An Approach to Action for the Electricity Sector*, Ver. 1.0, North American Electric Reliability Council, Princeton, NJ, June 2001.

[13] NSTAC, *Electric Power Risk Assessment*, National Security Telecommunications Advisory Committee, Wash. D.C., 1997. Available from www.ncs.gov/n5_hp/Reports/EPRA/electric.html.

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

[15] Oman, P., A. Risley, J. Roberts and E. Schweitzer, "Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electronic Power Systems," *Texas A & M Conference for Protective Relay Engineers*, College Station, TX, 2002.

[16] PCCIP, *Critical Foundations to Protect America's Infrastructures*, report from the President's Commission on Critical Infrastructure Protection, Washington D.C., 1997.

[17] Taylor, C., A. Krings, and J. Alves-Foss, "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An assessment approach for power substation hardening," *First Workshop on Scientific Aspects of Cyber Terrorism*, Washington D.C., November, 2002.