Survivable Systems Analysis of the North American Power Grid Communications Infrastructure [1,2]

Patrick R. Merry, Axel W. Krings and Paul W. Oman
Computer Science Department
University of Idaho
{patrickm, krings, oman} @cs.uidaho.edu

Abstract

The modern electric power grid is a complex interconnected network of independent physical and electronic devices that utilize myriad technologies for communication between other devices and with centralized control centers. These technologies may be compromised by malicious parties which may, in turn, lead to degraded performance or a failure of the communications infrastructure, ultimately resulting in loss of power grid transmission and/or distribution capabilities. This paper presents a Survivable Systems Analysis (SSA) of the North American power grid communications infrastructure. The SSA is used to identify general classes of inherent and emergent weaknesses within the North American electric power grid and propose appropriate means to mediate them. The analytic technique is applicable to any national or regional power grid, and can be generalized to most wide-area, complex, real-time control infrastructures such as transportation systems, natural gas distribution, and oil pipeline transmission systems.

Keywords: SCADA, Survivability, Power Grid, Survivable Network Analysis, Survivable Systems Analysis

1. Introduction

An electric power grid is a complex interconnected network of power generation, transmission, distribution, control equipment and sensors that is a keystone critical infrastructure which serves as a foundation for other critical infrastructures including health care, telecommunications, transportation and oil and gas distribution [1, 2].

The network of sensors, relays, *intelligent electronic devices* (IED) and various other protective and monitoring equipment is interconnected via a plethora of communications media and protocols creating a heterogeneous, distributed operating environment. Such a complex, wide-area, real-time control system has numerous vulnerabilities, frailties, embedded faults and opportunities for mismatched communications – so much so that it is difficult to establish priorities for when and where to apply security and survivability technologies. Economic constraints generally prohibit a "shot gun" approach of trying to patch all frailties, so design and maintenance engineers must determine where best to allocate their resources.

This paper applies the *Survivable Systems Analysis* (SSA) technique (formerly known as Survivable Network Analysis), developed by Ellison, et al. [3] and refined by Mead, et al. [4], to identify and enumerate general classes of *Intrusion Usage Scenarios* (IUS). The general IUS classes presented here are not intended to be exhaustive. Rather, they are representative examples of scenarios that are technologically feasible and have surfaced during survivability analyses of electric power generation, transmission and distribution facilities conducted by the authors of this paper over the course of eleven on-site studies.

Following a brief system definition and essential capability definition, IUSs are presented and discussed within the scope of common communication infrastructures and system capabilities. Finally, the results of the SSA are presented in the form of a survivability map: A summary of recognition, resistance and recovery attributes for each class of intrusion scenarios.

[1] Funded in part by a grant from NIST
[2] Funded in part by a grant from the U.S. DOT / NIATT

2. Background

Modern power grids are diverse systems of independent generators, transmission, and distribution networks and inter-ties that span large geo-spatial regions. Substation equipment connecting the independently owned generation-to-transmission and transmission-to-distribution facilities is equally diverse. Unfortunately, as the ease of access (i.e. convenience) increases, the susceptibility of the system to accidental and malicious intrusion also increases. As the probability of intrusion increases, the survivability of the system decreases.

During nominal power grid operation and maintenance, a finite number of *normal usage scenarios* (NUS) are observed. In contrast with the expected NUSs are the infinite number of abnormal usage scenarios and, of particular interest, the accidental and malicious IUSs that can be documented via ad hoc or structured methods of engineering analyses.

Addressing the power grid with respect to survivability in the context of malicious acts inherits all difficulties of controlling or modeling such complex systems. In order to avoid addressing all vulnerabilities and possible mitigation techniques for the entire system, we use the SSA approach to narrow the focus. In general, the SSA attempts to identify the essential portions of the system with respect to functionalities. Rather than using the common approach of identifying single possible attacks against specific portions of the system and addressing mitigation strategies in a bottom-up fashion, a top-town approach is taken that first attempts to identify those functionalities, assets or components that are at the core of the system specifications. In this manner, vulnerabilities and mitigation strategies can be focused on the essential portions of the system rather than the entire network. The survivability analysis presented below is modeled after the approaches described in [3] and [4].

3. An Example SSA on Portions of the North American Power Grid

We now present an example SSA based on recent visitations to control centers, generation plants and transmission and distribution substations comprising portions of the North American electric power grid. While our analyses are specific to a particular power grid, we believe our results can be generalized to most industrialized power grids and possibly other energy infrastructures (e.g. oil and natural gas systems).

3.1. Determination of Essential Functionalities

The first steps in the SSA process are identifying the mission requirements, network architecture, essential services and essential components.

Mission Requirements Definition

To better understand where weaknesses in the communications infrastructure of the power grid may be discovered and exploited, it is useful to first describe how the system should operate in a benign, steady state environment. The following normal usage scenarios present examples of typical usage and behavior of the components and subsystems within the power grid communications network. The identification of these usage scenarios serves as the foundation for isolating functionalities of the system that may be deemed essential to the operation of the system. Eight normal usage scenarios are presented:

- NUS 1: A SCADA system is polled for the status of the equipment it is monitoring. The SCADA system reports the current operating conditions over the network operator's wide area network (WAN), analog modem, broadband Internet connection, wireless network or satellite link.
- NUS 2: A field technician logs onto a locally attached terminal to gain access to a substation controller.
- NUS 3: A SCADA system, in report by exception mode, sends an unsolicited report to a supervisory control system that an anomalous condition has been detected.
- NUS 4: A technician connects to a remote terminal unit (RTU) at a substation by dialing into an analog modem attached to the publicly switched telephone network.
- NUS 5: In response to an anomalous phase angle condition, an intelligent electronic device (IED) trips a breaker that disconnects one or more pieces of "downstream" equipment, protecting it from damage.
- NUS 6: Sensors detect a sudden drop in line voltage and signal a power generation facility to increase power output to meet demand.
- NUS 7: In order to perform physical maintenance on substation equipment, a technician logs into an RTU to de-energize a piece of equipment. An electronic "red tag" is

created in the system to prevent other users from energizing the equipment while maintenance is ongoing.

- NUS 8: During an unscheduled disruption, remote technicians connect to an RTU to ascertain the status of substation equipment and/or to operate breakers and re-closers.

Architecture Definition

The power grid instrumentation, control, generation, transmission, distribution and protective equipment are interconnected to each other or to an RTU within a substation that, in turn, is connected to a larger supervisory control system [6]. Exacerbating the complexity of the power grid communications network is the lack of a single entity responsible for oversight and coordination and the lack of uniform communication standards (there are efforts underway to rectify this through the development of the Utilities Communication Architecture, or UCA [6]). This has led to any number of competing communications protocols and ad hoc standards being adopted by equipment manufactures and, in turn, being deployed by electric power utilities [7, 6].

Protocols employed in the power grid communications infrastructure range from the ubiquitous Ethernet and EIA232 (RS-232) protocols to protocols unique to the industry (e.g. DNP, Foundation Fieldbus, Profibus) to vendor specific protocols (e.g. Modbus, Seri-Bus) [6]. These protocols can be deployed over fiber, leased line, twisted pair, satellite, wireless or microwave media [2, 8].

The possible combinations of equipment, protocols and communications media are many and diverse. This poses several challenges to the electric power industry, with implications for the security of the communications infrastructure. Common functionalities of typical substation components include:

- IEDs operate circuit re-closers and similar equipment.
- SCADA systems receive input from attached sensors and relay data to supervisory control systems. SCADA systems may communicate with supervisory control systems via LAN, WAN, microware, radio frequency, publicly switched telephone networks or satellite.
- SCADA systems receive remote commands from supervisory control systems. These instructions are relayed to substation controllers.
- The substation controller is the primary interface to the local IEDs, controlling and coordinating their operation.
- Analog (i.e. dial-up) modems may be connected to a substation controller and/or directly to one or more IEDs.
- Local terminals may be connected to substation equipment (e.g. IEDs, the substation controller, SCADA components) via any one of a number of protocols including: Ethernet, UCA, EIA232, ControlNet or a proprietary protocol.

Essential Capabilities and Components

The essential services and assets central to the correct and timely operation of the electric power grid communications infrastructure are exhaustive and vary from one system to another, but all are focused on ensuring that equipment operates as intended under nominal conditions and during times of network distress. A complete list of essential services and assets should be generated for each entity responsible for network operations. Following are examples capturing the essential services of a typical system.

Essential Services

- Remote personnel shall have access to control systems (e.g. via modem, LAN, WAN).
- Local personnel shall have access to control systems (e.g. physical access to control and protective equipment).
- Continued proper functioning of safety equipment (e.g. breakers) is required.
- Accurate and timely exchange of SCADA data is required between the RTU and supervisory control systems.

Essential Assets

- Power generation, transmission and distribution equipment and infrastructure
- SCADA equipment
- Safety and operational equipment (e.g. breakers, re-closers, IEDs, RTUs)
- Communications infrastructure equipment

Once the essential services and assets are identified and documented, the essential components can be better recognized. Within the scope of the SSA, essential components are defined as *"those components that participate in delivery of essential services and preservation of essential assets"* [3]. As such, the essential components in the following list are required in order to preserve the essential assets and services described above.

Essential Components

- Communication channels (e.g. physical, microwave, radio frequency links)
- Communication equipment (e.g. modems, routers, switches)
- Authentication devices, both local and remote (e.g. key-card services, biometrics)
- IEDs responsible for physically operating safety and power distribution equipment.

3.2. Intrusion Scenarios

The next phase of the SSA process involves identifying or defining *intrusion usage scenarios* (IUS). The communication networks that facilitate day-to-day operations of the power grid through remote monitoring, audit and control of widely dispersed physical assets have allowed network operators to remain competitive in an increasingly demanding market [9, 10]. These same communications networks and automated tools have also opened the power grid to possible degradation of services and damage through accidental and malicious actions.

The SSA uses IUSs, which are essentially examples of possible network exploits, to identify the most vulnerable components in a system or network. The following IUSs illustrate how a malicious user may exploit weaknesses in the communications infrastructure to compromise safety, disrupt the distribution of power or damage control equipment. The IUSs have been aggregated into general classes of exploits and are not intended to be comprehensive. They are representative samples of attacks given current communications infrastructure designs and technology. The list is far from exhaustive as there are too many possible intrusion scenarios to list and new potential scenarios may arise every day.

Analog Modems

- IUS 1: A war dialer is used to locate an analog modem attached to an RTU. The potential intruder is able to discern the make and model of the RTU based on the welcome banner on the login screen. This information may assist in successfully cracking the password by applying public domain data mining techniques.
- IUS 2: An individual gains access to a substation RTU by spoofing a dial back modem.

Passwords, Backdoors and Social Engineering

- IUS 3: A malicious insider accesses control systems using common or default passwords shared by all technicians.
- IUS 4: Given weak passwords, an attacker uses a dictionary and/or brute force password attack to access equipment.
- IUS 5: Via the use of a Trojan horse, a malicious user accesses the corporate network and/or captures passwords and data from the compromised computer and network.
- IUS 6: A misplaced or stolen laptop is used to gain access to network assets through the use of installed software or by retrieving passwords from disc.
- IUS 7: An intruder uses social engineering to gather information about network operations and topology to assist in successfully compromising the communications infrastructure.

Wireless Network Access

- IUS 8: Using the 802.11 family of wireless networking protocols, a malicious individual mounts a direct attack on the network. Attempts may be made to access equipment, capture network traffic or crack passwords.

Physical Access and Sniffing

- IUS 9: An attacker accesses a long-haul network line or EIA232 serial line that bypasses physically guarded areas.
- IUS 10: An unauthorized user who gains physical access to the substation or a communications network node may be able to manipulate safety, control and communications devices.
- IUS 11: Having gained access to either the physical network (e.g. LAN, WAN) or to a wireless network, an intruder may use any of the available sniffing tools such as Ethereal, Snort or TCPdump to intercept private network traffic.
- IUS 12: A man-in-the-middle attack on an unencrypted telnet session can be used to "hijack" a session in progress, granting the attacker all of the access and privileges inherited from the legitimate user.

LAN Access

- IUS 13: A malicious individual uses a ping sweep to identify the publicly accessible IP addresses of network controllers (e.g. IEDs and RTUs). Determining the public IP address(es) of corporate servers and then attempting to ping the other addresses within the same class may illuminate potential future target addresses.
- IUS 14: Once an intruder has access to one part of the network, it may be possible to gain access

to another subnet. For example, by hacking into the corporate IT network, SCADA and supervisory control systems may be at risk. Likewise, compromising the control infrastructure may provide access to the corporate network.

Sabotage and Fraud

- IUS 15: Once unauthorized access has been acquired via one of the above scenarios, protective equipment settings may be altered to operate beyond their safety limit instead of tripping off line. Alternatively, equipment could be set to prematurely trip off-line, reducing the service level of the power grid and shortening the life span of the equipment.
- IUS 16: An end user gains access to remote metering equipment and modifies energy usage records.

Denial of Service Attacks

- IUS 17: A rudimentary denial of service attack can be initiated by "flooding" an analog modem with requests to connect, forcing it to time out between retries.
- IUS 18: Wireless networks are susceptible to denial of service attacks through traditional radio frequency jamming.
- IUS 19: By taking advantage of known software flaws or other vulnerabilities, it may be possible to force a substation controller to crash or shutdown prematurely.
- IUS 20: A classic distributed denial of service attack can be initiated against a network operator's public IP addresses from foreign or domestic sources.

4. Survivability Analysis

The final phase of the SSA process, the survivability analysis, draws upon the above normal and intrusion usage scenarios to develop a list of *softspot* components and a survivability map. This section presents the cornerstone of the survivability map: an analysis of resistance, recognition, and recovery capabilities.

Softspot Components

Softspot components are components that are both essential and capable of being compromised [3,4]. Some of the softspot components that can be identified from the above IUSs include: analog modems, user authentication and auditing systems, network communications over unsecured channels, legitimate users (through social engineering and insider abuse) and networks where penetration into one system allows an intruder to compromise other subnets.

The power grid communications infrastructure should incorporate technologies, policies and controls that are capable of resisting unauthorized access, recognizing unauthorized access and behavior when it does occur and recovering from an intrusion after it has ended. Much of the equipment identified in the normal and intrusion usage scenarios have extremely limited resistance capabilities and, usually, rudimentary user authentication (e.g. modems, RTUs, etc.).

Similarly, recognition capabilities in many pieces of equipment are virtually non-existent, in some cases due to poor implementation, in others due to the characteristics of the equipment. Where it is practical, automated recognition strategies are recommended. For equipment where automated recognition is not practical, it is recommended that supervisory personnel be notified of incidents that could constitute an intrusion. Automated recognition procedures must balance security and reliability to maintain system integrity while minimizing the erroneous identification of benign conditions as intrusions (i.e. "false positives").

Recovery capabilities, both current and recommended, are examined for the equipment exploited in the intrusion usage scenarios. While many components are limited with respect to their recovery capabilities, some of the components could employ much more effective recovery strategies than are currently in use.

The Survivability Map

The end result of the SSA is the survivability map, presented in Table 1. The survivability map combines into a single table the current and recommended resistance, recognition and recovery strategies for the component that is compromised in each class of intrusion usage scenario. The table indicates, for each class of intrusion scenarios under consideration, current strategies as well as recommendations suggesting mitigation strategies.

The table illuminates the need for significant changes to many of the common power grid communications infrastructure components and provides a roadmap from which to create a more secure, reliable and survivable infrastructure.

Table 1. Survivability Map

Intrusion Scenario Class	Resistance Strategy	Recognition Strategy	Recovery Strategy
Analog Modems:	**Current:** Rudimentary password protection, logon retry delays and dial back modems.	**Current**: Terminate session after *n* unsuccessful logon attempts. Log file analysis may be possible after the fact in some cases.	**Current**: Typically nonexistent as recovery of analog modems is usually automatic.
	Recommended: Improve password protection including multi-level access, support for robust passwords, use of modem key-lock systems and deployment of dial back modems that are more resistant to spoofing. Any identifying information such as make and model should be obscured from the logon screen.	**Recommended**: Automated reporting of multiple unsuccessful logon attempts.	**Recommended**: Add redundant means of connecting to the equipment attached to the modem.
Passwords, Backdoors and Social Engineering:	**Current**: Policies may exist to prohibit employees and contractors from bringing external programs (e.g. floppy discs, email attachments and downloaded games) into the organization.	**Current**: Individual pieces of equipment may resist multiple unsuccessful logon attempts. Virus detection suites may be in use.	**Current**: Recovery of authentication devices is a function of its design.
	Recommended: Improve training with an emphasis on increasing awareness of social engineering techniques and the dangers of unknown software. Restrict software installation rights to administrators. Improve password policies and establish unique user IDs and passwords for each employee. Revoke employee and contractor logon privileges at termination.	**Recommended**: Improve log file analysis and automate notification of unauthorized logon attempts (e.g. former employees).	**Recommended**: No changes.
Wireless Network Access:	**Current**: Rudimentary security may be implemented (e.g. WEP).	**Current**: None.	**Current**: None.
	Recommended: Encrypt all wireless network traffic, utilize MAC address registration and deploy wireless access points only when absolutely necessary.	**Recommended**: Aggressively analyze log files and implement real time notification of potential intrusions with possible wireless equipment deactivation.	**Recommended**: Restart wireless equipment when intrusion appears to have passed (e.g. when unregistered MAC addresses are no longer present). Add redundant means of connecting to the equipment attached to the wireless network.

Table 1. Survivability Map

Intrusion Scenario Class	Resistance Strategy	Recognition Strategy	Recovery Strategy
Physical Access and Sniffing:	**Current:** Physical barriers, warning signs and lights protect physical assets. Virtual assets may or may not be obscured on the public network. Telnet and similar remote logon sessions may or may not be encrypted.	**Current:** Physical inspection of equipment and log file analysis.	**Current:** Physically reset equipment when applicable.
	Recommended: Maintain and improve physical security including additional authentication devices and tamper-resistant equipment. Virtual assets should be obscured behind well-maintained firewalls and all remote sessions such as telnet should be encrypted (e.g. SSH or bump-in-the-wire cryptographic devices).	**Recommended:** Automate reporting of access to facilities, increase log file analysis and deploy intrusion detection systems.	**Recommended**: Automated recovery strategies may be possible but should be considered with caution; physical equipment known to have been compromised should be thoroughly inspected before being reconnected.
LAN Access:	**Current:** Firewalls may be in use separating subnets.	**Current:** Log file analysis.	**Current**: Corporate IT recovery strategy.
	Recommended: Implement switching and firewall technology to isolate corporate sub-networks by function. Log file analysis and dynamic firewalls can be implemented to automatically block traffic from IP addresses or networks perceived as threats.	**Recommended:** Continue log file analysis, deploy intrusion detection systems and automate notification of potential intrusions.	**Recommended**: Amend the corporate IT recovery strategy to include forensic analysis of intrusions.
Sabotage and Fraud:	**Current:** Physical security.	**Current:** Physical inspection and aggregation of billing information to verify integrity.	**Current**: Manual reset or calibration.
	Recommended: Use tamper-resistant equipment, encrypt metering data and employ strong authentication techniques.	**Recommended:** Periodically poll protective equipment and compare results with historical settings and recent work orders.	**Recommended:** Automated calibration and resets may be implemented.
Denial of Service Attacks:	**Current:** None.	**Current:** Secondary effects of DOS attacks may trigger alerts as the quality of service degrades.	**Current:** None.
	Recommended: Security though obscurity may deter casual attackers; use separate subnets for different functional networks and minimize the number of publicly accessible IP addresses.	**Recommended:** Automated reporting of network QOS and operating conditions.	**Recommended:** Implement multiple, in-dependent network paths to critical systems with automated switchover. For simple DOS attacks, automate firewall/router settings to block the source IP address(es).

5. Conclusions

This paper presented a Survivable Systems Analysis of the North American power grid. Rather than addressing vulnerabilities in an ad hoc fashion considering individual attacks on any specific part of the overall power communication infrastructure, we employed the SSA to help identify essential services, assets and components. Narrowing the scope to these essentials rather than considering the entire system allows survivability to be more effectively evaluated. A variety of intrusion scenarios were presented and partitioned into intrusion groups or classes; whereas the list of intrusion scenarios is by no means assumed complete, it covers a wide range of scenarios helping systems engineers and security personnel to evaluate specific vulnerabilities of their power systems. Finally, a survivability map was created and presented, partitioning survivability into resistance, recognition and recovery. For each class, the current practices and mitigation suggestions were summarized.

It is the authors' hope that this research will help first to address the vulnerabilities of the power grid to cyber attacks on its communication infrastructure and, second, to give engineers a more structured method to achieve system survivability. Whereas the power grid consists of many diverse subsystems, each with very unique components, many of the underlying control infrastructures are very similar and the general approach presented here can be applied to any system in general.

References

[1] *The Report of the President's Commission on Critical Infrastructure Protection*, Critical Infrastructure Assurance Office, Washington, D.C. Oct. 1997. Available at: http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf

[2] R. Carlson, "Industrial Applications of Information Security to Protect the Electric Power Infrastructure," Sandia SCADA Program, Albuquerque, NM. SAND2002-0729, April 1994. Available at: http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/2002/020729.pdf

[3] R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead, "A Case Study in Survivable Network System Analysis," Carnegie Mellon University – Software Engineering Institute, Sept. 1998. Technical Report no. CMU/SEI-98-TR-014 ESC-TR-98-014. Available at: http://www.cert.org/archive/pdf/00tr013.pdf

[4] N. R. Mead, R. J. Ellison, R. C. Linger, T. Longstaff, J. McHugh, "Survivable Network Analysis Method," Carnegie Mellon University – Software Engineering Institute, Sept. 2000. Technical Report no. CMU/SEI-2000-TR-013 ESC-2000-TR-013. Available at: http://www.cert.org/archive/pdf/00tr013.pdf

[5] P. W. Oman, A. D. Risley, J. Roberts, and E. O. Schweitzer, "Attack and Defend Tools for Remotely Accessible Control and Protection Equipment in Electric Power Systems," Schweitzer Engineering Laboratories, Pullman, WA. 2002. Available at: http://www.selinc.com/techpprs/6132.pdf

[6] D. Dolezilek, "SEL Communications and Integration White Paper," Schweitzer Engineering Laboratories, Pullman, WA. 2001. Available at: http://www.selinc.com/techpprs/6085.pdf

[7] T. Godard, R. Kelley, and B. Fesmire, "Metering Automation," *Utility Automation*, vol. 7(5), pp. 35-42, Sep.-Oct. 2002.

[8] D. Woodward, "The Hows and Whys of Ethernet Networks in Substations," Schweitzer Engineering Laboratories, Pullman, WA. 2001. Available at: http://www.selinc.com/techpprs/6115.pdf

[9] T. A. Longstaff, C. Chittister, R. Pethia, and Y. Y. Haimes, "Are We Forgetting the Risks of Information Technology?," *Computer*, vol. 0018-9162, pp. 43-51, Dec. 2000.

[10] D. Conte de Leon, J. Alves-Foss, A. Krings, and P. Oman, "Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack," *ACM Workshop on Scientific Aspects of Cyber Terrorism*, (SACT), Washington DC, 10 pages, November 2002. Available at: http://www.cs.uidaho.edu/~krings/SACT-2002-D.pdf