Chapter 6

TOWARDS A TAXONOMY OF ATTACKS AGAINST ENERGY CONTROL SYSTEMS

Terry Fleury, Himanshu Khurana and Von Welch

Abstract Control systems in the energy sector (e.g., supervisory control and data acquisition (SCADA) systems) involve a hierarchy of sensing, monitoring and control devices connected to centralized control stations or centers. The incorporation of commercial off-the-shelf technologies in energy control systems makes them vulnerable to cyber attacks. A taxonomy of cyber attacks against control systems can assist the energy sector in managing the cyber threat. This paper takes the first step towards a taxonomy by presenting a comprehensive model of attacks, vulnerabilities and damage related to control systems. The model is populated based on a survey of the technical literature from industry, academia and national laboratories.

Keywords: Energy sector, control systems, attack taxonomy

1. Introduction

Energy control systems involve a hierarchy of sensing, monitoring and control devices connected to centralized control stations or centers. Within this hierarchy, control systems remotely monitor and control sensitive processes and physical functions. Supervisory control and data acquisition (SCADA) systems utilized to monitor power, oil and gas transmission systems are common instantiations of energy control systems. Owing to various commercial and external forces such as deregulation, asset owners are extending the connectivity of their control systems by adopting commercial off-the-shelf (COTS) components. Standard operating systems (e.g., Windows and UNIX) and communication technologies (e.g., public and private IP networks, public telephone networks and wireless networks) are being used more frequently in control systems.

Earlier control systems operated in isolated environments with proprietary technologies. Consequently, they faced little to no cyber security risk from

external attackers. However, the adoption of commercial technologies causes process control systems in the energy sector to become increasingly connected and interdependent. This makes energy control systems attractive targets for attack. Along with the cost saving benefits of commercial technologies comes a multitude of vulnerabilities inherit in the technologies. This attracts a range of adversaries with the tools and capabilities to launch attacks from remote locations with significant consequences. Systems are attacked by hackers for glory and attention, by criminals for financial gain, by insiders for retribution, by industrial and government spies for intelligence gathering, and by botnet operators for inclusion in their bot armies. These adversaries may have significant resources at their disposal and use them to launch cyber attacks that exploit vulnerabilities and potentially cause harm.

Cyber attacks can have a significant impact on the operation of control systems. For example, denial-of-service attacks can disrupt the operation of control systems by delaying or blocking the flow of data through communication networks. Attacks that result in corruption of data can lead to propagation of false information to the control centers, which may result in unintended decisions and actions.

A large body of technical literature discusses security issues related to control systems, especially threats, attacks and vulnerabilities. Our survey has examined research efforts that address specific aspects of control systems security [1, 3, 4, 14, 16–18, 28] as well as work focused on broader security issues [5–8, 22, 24, 26, 29]. However, most of these efforts adopt *ad hoc* approaches to discuss and prioritize the various aspects of attacks. What is needed is an attack taxonomy that enables researchers and practitioners to have a comprehensive understanding of attacks against energy control systems. The taxonomy would help answer the following key questions:

- What are the different ways of perpetrating attacks against a control system?
- What kind of damage can these attacks cause?
- What are the challenges involved in defeating these attacks?
- What are the requirements for developing adequate defense mechanisms?

This paper takes the first major step towards the creation of a taxonomy by presenting a comprehensive attack model and populating the model based on an extensive survey of known attacks against control systems. This attack-vulnerability-damage (AVD) model places equal importance on how attacks take place, what vulnerabilities enable these attacks to be performed, and what damage these attacks can cause. The model is geared specifically towards control systems and serves as a basis for developing a comprehensive taxonomy of attacks against energy control systems.

2. Energy Control Systems

Energy control systems include SCADA systems, distributed control systems (DCSs) and programmable logic controllers (PLCs). These systems are critical

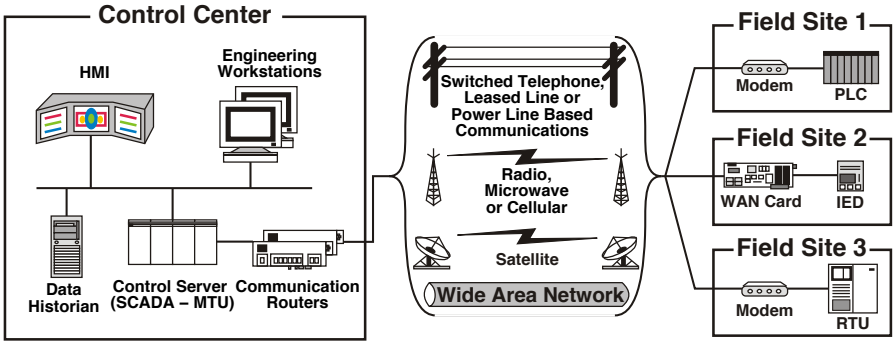

Figure 1. Sample SCADA system [27].

to the generation, distribution and delivery of energy across all sectors. SCADA systems provide centralized monitoring and control of field devices spread over large geographic areas. DCSs provide control of local processes that comprise integrated subsystems. PLCs are computer-based solid-state devices that are used in SCADA systems and DCSs as well as independently in small control systems.

This paper uses a SCADA system as a primary example of a complex control system employed in the energy sector. Figure 1 presents a typical SCADA system [27]. The SCADA system transmits operational data from field sites to control centers, and control information from control centers to field sites. Once field data reaches the control system, software systems provide capabilities to visualize and analyze the data. Based on automated or human-driven analysis, actions are performed as needed (e.g., recording data, processing alarms or sending control information back to the field sites). Data acquisition and supervisory control are undertaken by hardware and software systems connected by a multitude of networking technologies. The hardware includes PLCs, remote terminal units (RTUs), intelligent electronic devices (IEDs), relays, SCADA servers (master terminal units (MTUs)), communication routers, workstations and displays. These hardware systems run software for data input and output processing, data transfer and storage, state estimation, visualization, remote access, equipment control, and alarm processing and reporting. All these hardware and software systems are connected via local-area or wide-area networks depending on their proximity. Standard and proprietary communication protocols are used to transport information between the control center and field sites via telephone lines, cable, fiber, microwave and satellite links.

Due to the increased use of COTS hardware, software and networking components, control systems are beginning to look like traditional IT infrastructures. However, there are key differences between control and traditional IT systems that significantly impact design and management. This paper analyzes how these differences impact threat analysis and the development of an attack taxonomy.

There are three core aspects of energy control systems that lead to unique performance, availability, deployment and management requirements. First, the critical nature of these systems necessitates uninterrupted generation, distribution and delivery of energy. Second, these systems operate under a safety-first paradigm due to hazards to equipment and personnel. Third, the power transmission system has direct physical interactions with the control system. The three core aspects are not necessarily distinct as they have an overlapping nature. Combined together, they impact control system software, hardware and networking in two ways.

- **Performance and Availability:** Applications depend on data in a critical manner. This requires control systems to provide a deterministic response without delays or jitter in data delivery. In turn, the systems that generate and distribute data must be highly reliable and available, and the delivered data must have high integrity. Additionally, any (cyber) security mechanism, such as one that may provide integrity assurances, must be fail-safe. A failure of the security mechanism should not result in a failure of the underlying control system.

- **Deployment and Management:** Control systems must be tested extensively in "real" environments before they can be deployed. This is because they control physical systems over vast geographic areas and the deployed equipment typically has a long life (possibly one or two decades). Furthermore, downtime for system maintenance and upgrades (e.g., patch management) is unacceptable without significant advanced planning. In contrast, traditional IT systems are usually deployed without extensive testing. Their initial deployment phase often serves as a partial test environment. Also, IT systems have expected lifetimes of a few years and operate under the assumption that they may be taken down for maintenance and upgrades with relatively short notice.

3. Methodology

A model for classifying cyber attacks against control systems must satisfy several goals.

- The model should be specific to cyber attacks on control systems. Several researchers have attempted to classify cyber threats to general computer systems (see, e.g., [11, 15]). Since the energy sector incorporates COTS technologies (e.g., TCP/IP), much of this research can be applied to energy control systems. However, as discussed above, control systems have unique features and requirements, and it is important that the model addresses these issues.
- The model should have a relatively high level of abstraction. Some classification schemes for cyber threats to general computer systems describe attacks in a detailed manner. For example, attack trees/graphs [3, 12, 23, 25] break down a single cyber attack into its constituent parts, tracing

the attack from the source (attacker) through various system components to the target. Instead of enumerating every possible attack, the model should permit parts of specific attacks to be sorted into generalized categories.

- The model should be easily expandable. New attacks are continually being developed. The model should accommodate instances of future attacks and grow and adapt as necessary.
- The model should tolerate incompleteness. Incident reports often provide terse accounts of attacks for reasons of sensitivity. For example, a report may mention how an attack was carried out but omit its consequences. Alternatively, a report may describe a system vulnerability and how its exploitation may cause damage, but it may not discuss how attackers might conduct the exploit. The model should allow for such omissions while incorporating all the reported aspects of cyber threats.

With these goals in mind, we conducted an extensive survey of the technical literature. Nearly all the documents that were examined contained threat descriptions. Several papers (e.g., [2, 19]) described attacks and the associated vulnerabilities; others (e.g., [4, 10]) described attacks and their effects. One paper [8] discussed vulnerabilities and attack impact or damage. This clustering of descriptions led us to believe that cyber threats to energy control systems are best decomposed into three categories: attack, vulnerability and damage. These three categories form the basis of our attack-vulnerability-damage (AVD) model. The Howard-Longstaff approach [9] and the system-fault-risk (SFR) framework [30], in particular, matched our modeling goals and inspired the development of the AVD model.

4. Attack-Vulnerability-Damage Model

This section describes the AVD model and populates it with examples of cyber attacks against energy control systems.

The AVD model (Table 1) classifies cyber threats based on three broad categories. The attack category includes "local" origins and "system" targets to identify physical control system components that may be the origin of the attack (e.g., compromised or exposed end device) and/or the target (e.g., unauthorized opening of a relay). The vulnerability category includes configuration and implementation errors in physical devices (e.g., malfunctioning device). The damage category considers the harm caused to computer systems as well as the physical control system (e.g., electric power relay). Given the time-critical nature of energy systems, the damage category also considers the performance effect and the severity of the attack.

Since control systems face threats that strongly overlap those that affect IT systems, several categories and descriptions in the AVD taxonomy are common to those encountered in attack taxonomies developed for IT systems. However, in this paper, we focus on example attacks that are specific to control systems in the energy sector.

Table 1. Attack-vulnerability-damage (AVD) model.

Attack		
Origin	*Action*	*Target*
Local	Probe	Network
Remote	Scan	Process
	Flood	System
	Authenticate	Data
	Bypass	User
	Spoof	
	Eavesdrop	
	Misdirect	
	Read/Copy	
	Terminate	
	Execute	
	Modify	
	Delete	
Vulnerability		
Configuration		
Specification		
Implementation		
Damage		
State Effect	*Performance Effect*	*Severity*
None	None	None
Availability	Timeliness	Low
Integrity	Precision	Medium
Confidentiality	Accuracy	High

4.1 Attacks

An attack has an origin, an action (taken by the attack) and a target (Table 2).

Attack Origin: The attack origin describes the location of the attacker with respect to the target.

- Local: A local attack originates from within the target. Such an attack occurs when the attacker has physical access to equipment [4, 13, 17] or when a malfunction occurs in a nearby piece of equipment [10].
- Remote: A remote attack originates outside the target site. Such an attack may involve a dial-up modem [4, 19], open wireless network [2, 4, 20, 29], private network and bridge [21] or a connection to a trusted third-party system [4].

Table 2. Attack category examples.

Origin	
Local	*Remote*
Physical access to equipment	Dial-up modem
Malfunctioning PLC	Open wireless network
	Worm via private network and bridge
	Trusted third-party connection
Action	
Probe	*Scan*
Map available equipment	Perform simple vulnerability scan
Flood	*Authenticate*
Launch data storm	Guess/crack password
Launch denial-of-service attack	
Bypass	*Spoof*
Use different method to access process	Hijack session
Eavesdrop	*Misdirect*
Monitor wireless traffic	Alarm output not displayed
Read/Copy	*Terminate*
Download business reports	Shut down service
	Shut down SCADA system
Execute	*Modify*
Exploit MS-SQL vulnerability	Alter SCADA system metering data
	Change protection device settings
Delete	
Render data non-retrievable	
Target	
Network	*Process*
Deluge network with data	Disable safety monitoring
Wireless transmissions	Use computer resources to play games
System	*Data*
Digital circuit breaker	Business report
User	
Profile theft	

Attack Action: The attack action describes the activity that the attack performs on the target.

- Probe: A probe seeks to determine the characteristics of a particular system. For example, a probe may attempt to identify the make and model of a device or the software services (and versions) running on the device [8, 16].
- Scan: A scan attempts to access targets sequentially for the purpose of determining specific characteristics. An example is a network scan that identifies open ports [2].
- Flood: A flood repeatedly accesses a target, overloading it with traffic, possibly disabling it. Examples include data storms [10] and denial-of-service attacks [16].
- Authenticate: This involves unauthorized or illicit authentication as a valid user or process in order to access the target. An example is password cracking [16].
- Bypass: This involves the use of an alternative method to access the target (e.g., bypassing standard access protocols).
- Spoof: A spoofing attempt assumes the identity of a different user in order to access the target. An example is session hijacking [16].
- Eavesdrop: This involves the passive monitoring of a data stream to obtain information (e.g., sniffing unencrypted wireless traffic [29]).
- Misdirect: This involves intercepting communication channels and outputting bogus information. The recipients are unaware that the output is not genuine. An example is cross-site scripting where the input is redirected to a malicious site that outputs seemingly correct information.
- Read/Copy: This usually refers to a static data source, but could also refer to a dynamic data stream. In a "read" attack, the data is read by a human. A "copy" attack duplicates the original data source for later processing by a human or process. An example is downloading private business reports [2].
- Terminate: This involves stopping a running process. It could be as specific as shutting down a service (e.g., a monitoring or display system [13, 20]) or as broad as shutting down an entire SCADA system [17].
- Execute: This involves running a malicious process on the target. This behavior is typical of a virus or worm (e.g., Slammer worm that exploits an MS-SQL vulnerability [20]).
- Modify: This involves changing the contents of the target. Examples include modifying SCADA system data or device protection settings [17].
- Delete: This involves erasing data from the target or simply making the data non-retrievable.

Attack Target: The attack target describes the resource that is attacked.

- Network: A network comprises computers and networking equipment connected via wires or wirelessly. An attack on a network target typically involves disrupting communications between computers and network devices [10, 29].

Table 3. Vulnerability category examples.

Vulnerability	
Configuration	*Implementation*
Account management	Poor authentication
Unused services	Scripting/interface programming
Unpatched components	Malfunctioning devices
Perimeter protection	Poor logging/monitoring
Design/Specification	
Cleartext communications	
Poor coding practices	
Network addressing	
Web servers and clients	
Enumeration	

- Process: A process is a program running on a computing system. It consists of program code and data. Example attacks are disabling safety monitoring software [20] and using computer resources for entertainment (e.g., to play games) [17].
- System: A system comprises one or more connected components that perform computations. A system typically refers to a computer but could also describe a device such as a digital circuit breaker [19].
- Data: Data consists of information that is suitable for processing by humans and machines. Data can refer to a single resource such as a file stored on a hard drive or packets that are transmitted over a communications network. An example attack is the unauthorized access of data from a server [2].
- User: A user has authorization to access certain system resources. Attacks targeting users typically attempt to illicitly gain information for later use. An example is monitoring network traffic to discover user passwords [16].

4.2 Vulnerabilities

A vulnerability describes why a particular attack may be successful (Table 3). The vulnerability does not specify the actual target, but the weakness that can be exploited.

- Configuration: An improperly configured resource may enable an attacker to gain unauthorized access to a target. Examples include poor account management where certain unused accounts [8, 26, 28] and/or services [8] have high-level privileges; components with known flaws that are not

Table 4. Damage category examples.

State Effect	
Availability	*Integrity*
Circuit breaker tripped	Corrupt data received
Recirculation pump failure	
Confidentiality	
Business reports downloaded	
Performance Effect	
Timeliness	*Accuracy*
Plant network slowdown	Missing alarm data
Precision	
Plant data cannot be viewed	
Severity	
None	*Low*
Attacker does not impact target	Attacker gains additional information
Medium	*High*
Attacker degrades performance	Attacker acts as a legitimate user
Attacker alters system state	Attacker gains admin rights
Loss of public confidence in services	Attacker disables process
	Attacker causes equipment damage
	Attacker spoofs displays via man-in-the-middle attack

properly patched [8, 21, 26]; weak or non-existent authentication (including unchanged passwords) [5, 28]; and misconfigured perimeter protection and/or access control policies [2, 8, 19, 26].

- Design/Specification: Design flaws in a process or component can be utilized in unintended ways to gain access to a target. Examples are insecure communication protocols used by processes and users [5, 8, 26, 29] and flawed code [8, 28].
- Implementation: Even when the design of a hardware or software system is correct, the implementation may be incorrect. This can lead to security holes [8, 20, 28] or malfunctions [10, 26].

4.3 Damage

The damage caused by an attack has three attributes: state effect, performance effect and severity (Table 4). State effects and performance effects

describe the damage done to the system components. The severity attribute attempts to quantify the overall impact of the attack.

State Effect: A state effect describes the state change that occurs to the target because of the attack.

- Availability: The availability of an asset refers to its ability to service requests. A successful attack disables an asset or increases its response time. Example state effects include tripping a circuit breaker [19] and disrupting a recirculation pump [10].
- Integrity: Integrity refers to the correctness of an asset when meeting service requests. An example state effect is data corruption.
- Confidentiality: Confidentiality refers to authorized access to, or use of, an asset. An example state effect is the unauthorized access of business reports [2].

Performance Effect: A performance effect describes the performance degradation that occurs on the target because of the attack.

- Timeliness: This is a measure of time from data input to output. A timeliness performance effect has occurred when there is a sustained increase in this measure. An example is plant network slowdown [20].
- Precision: This is a measure of the amount of output generated by data input. A precision performance effect has occurred when the output is not 100% of the expected output. This may occur, for example, when a process is terminated before it completes its execution or when insufficient data output produces an "Unable to View Plant" error message [4].
- Accuracy: This is a measure of the correctness of the output generated by data input. For example, an accuracy performance effect has occurred when control messages or measurements are altered during transmission.

Severity: Severity seeks to quantify the level of impact of an attack.

- None: The attack may have been successful, but it has no noticeable impact on the target [8].
- Low: The attack typically gains information that may not be directly exploitable [2, 3, 8, 29]. An example is the discovery of user names but not the associated passwords.
- Medium: The attack degrades system performance [8, 13, 21] and/or alters the state of the system [3, 20]. State and/or performance effects may start to be seen. This may result in a loss of public confidence in system services [26].
- High: The attack enables the perpetrator to gain the privileges of a legitimate user [8], operator [4, 8] or administrator [3, 8] to disable processes [10, 19] or damage equipment [26].

Table 5. Example attacks in the AVD model.

Attack	**Origin**	**Vulnerability**	**State Effect**
	Action		**Performance Effect**
	Target		**Severity**
Data Storm [10]	Local Flood Network	Specification	Availability Precision Medium
Slammer Worm (Remote) [20]	Remote Copy Process	Implementation	Integrity Accuracy Low
Slammer Worm (Local) [20]	Local Execute System	Specification	Integrity Accuracy High
Software Bug XA/21 [21]	Local Terminate Process	Implementation	Integrity Timeliness Medium
Dial-In Password [5]	Remote Authenticate User	Configuration	Any Any High
Component Data Spoofing [5]	Local Modify Data	Specification	Integrity Accuracy High

4.4 Example Attacks

Table 5 lists several complete attacks by name and shows how they fit into the AVD model.

5. Conclusions

Energy control systems are vulnerable to cyber attacks. In order for the energy sector to deal effectively with these attacks, it is necessary to develop a taxonomy of attacks against control systems. The comprehensive model of attacks, vulnerabilities and damage presented in this paper is a first step to developing such a taxonomy.

Our future work on developing the taxonomy will expand the model by considering additional categories and sub-categories as well as analyzing a broader range of attack data. Categories for consideration include (i) attack sophistication, i.e., level of expertise required for an attack; (ii) fiscal impact, i.e., the financial loss incurred due to the attack; and (iii) protocol and operation sys-

tem specifics, i.e., details of the attack in terms of the protocols and operating systems that are exploited.

Acknowledgements

This research was supported by the National Science Foundation under Grant No. CNS-0524695. The authors also wish to acknowledge the technical assistance provided by participants in the Trustworthy Cyber Infrastructure for the Power Grid Project.

References

[1] K. Birman, J. Chen, E. Hopkinson, R. Thomas, J. Thorp, R. van Rennesse and W. Vogels, Overcoming communications challenges in software for monitoring and controlling power systems, *Proceedings of the IEEE*, vol. 93(5), pp. 1028–1041, 2005.

[2] A. Brown, SCADA vs. the hackers, *Mechanical Engineering*, vol. 124(12), pp. 37–40, 2002.

[3] E. Byres, M. Franz and D. Miller, The use of attack trees in assessing vulnerabilities in SCADA systems, *Proceedings of the International Infrastructure Survivability Workshop*, 2004.

[4] E. Byres and J. Lowe, The myths and facts behind cyber security risks for industrial control systems, *Proceedings of the VDE Congress*, pp. 213–218, 2004.

[5] R. Carlson, Sandia SCADA Program: High-Security SCADA LDRD Final Report, Technical Report SAND2002-0729, Sandia National Laboratories, Albuquerque, New Mexico, 2002.

[6] J. Eisenhauer, P. Donnelly, M. Ellis and M. O'Brien, Roadmap to Secure Control Systems in the Energy Sector, Technical Report, Energetics Inc., Columbia, Maryland, 2006.

[7] J. Falco, J. Gilsinn and K. Stouffer, IT security for industrial control systems: Requirements specification and performance testing, presented at the *National Defense Industrial Association Homeland Security Conference and Exposition*, 2004.

[8] R. Fink, D. Spencer and R. Wells, Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems, Technical Report INL/CON-06-11665, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[9] J. Howard and T. Longstaff, A Common Language for Computer Security Incidents, Technical Report SAND98-8667, Sandia National Laboratories, Livermore, California, 1998.

[10] R. Lemos, "Data storm" blamed for nuclear plant shutdown, *SecurityFocus*, May 18, 2007.

[11] U. Lindqvist and E. Jonsson, How to systematically classify computer security intrusions, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 154–163, 1997.

[12] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz and R. Cunningham, Validating and restoring defense in depth using attack graphs, *Proceedings of the Military Communications Conference*, pp. 1–10, 2006.

[13] R. McMillan, Admin faces prison for trying to axe California power grid, *PC World*, December 15, 2007.

[14] M. McQueen, W. Boyer, M. Flynn and G. Beitel, Quantitative cyber risk reduction estimation methodology for a small SCADA control system, *Proceedings of the Thirty-Ninth Annual Hawaii International Conference on System Sciences*, p. 226, 2006.

[15] J. Mirkovic and P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, *ACM SIGCOMM Computer Communication Review*, vol. 34(2), pp. 39–53, 2004.

[16] P. Oman, A. Risley, J. Roberts and E. Schweitzer, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, presented at the *Fifty-Fifth Annual Conference for Protective Relay Engineers*, 2002.

[17] P. Oman, E. Schweitzer and J. Roberts, Protecting the grid from cyber attack, Part I: Recognizing our vulnerabilities, *Utility Automation & Engineering T&D*, vol. 6(7), pp. 16–22, 2001.

[18] P. Oman, E. Schweitzer and J. Roberts, Protecting the grid from cyber attack, Part II: Safeguarding IEDs, substations and SCADA systems, *Utility Automation & Engineering T&D*, vol. 7(1), pp. 25–32, 2002.

[19] K. Poulsen, Sparks over power grid cybersecurity, *SecurityFocus*, April 10, 2003.

[20] K. Poulsen, Slammer worm crashed Ohio nuke plant network, *SecurityFocus*, August 19, 2003.

[21] K. Poulsen, Software bug contributed to blackout, *SecurityFocus*, February 11, 2004.

[22] R. Schainker, J. Douglas and T. Kropp, Electric utility responses to grid security issues, *IEEE Power and Energy*, vol. 4(2), pp. 30–37, 2006.

[23] B. Schneier, Attack trees, *Dr. Dobb's Journal*, vol. 24(12), pp. 21–29, 1999.

[24] F. Sheldon, T. Potok, A. Loebl, A. Krings and P. Oman, Managing secure survivable critical infrastructures to avoid vulnerabilities, *Proceedings of the Eighth IEEE International Symposium on High Assurance Systems Engineering*, pp. 293–296, 2004.

[25] O. Sheyner, J. Haines, S. Jha, R. Lippmann and J. Wing, Automated generation and analysis of attack graphs, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 273–284, 2002.

[26] J. Stamp, J. Dillinger, W. Young and J. DePoy, Common Vulnerabilities in Critical Infrastructure Control Systems, Technical Report SAND2003-1772C, Sandia National Laboratories, Albuquerque, New Mexico, 2003.

[27] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems Security, Second Public Draft, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2007.

[28] C. Taylor, P. Oman and A. Krings, Assessing power substation network security and survivability: A work in progress report, *Proceedings of the International Conference on Security and Management*, pp. 281–287, 2003.

[29] D. Watts, Security and vulnerability in electric power systems, *Proceedings of the Thirty-Fifth North American Power Symposium*, pp. 559–566, 2003.

[30] N. Ye, C. Newman and T. Farley, A system-fault-risk framework for cyber attack classification, *Information-Knowledge-Systems Management*, vol. 5(2), pp. 135–151, 2005.