Chapter 1

TOWARDS A TAXONOMY OF ATTACKS AGAINST ENERGY CONTROL SYSTEMS*

Terry Fleury, Himanshu Khurana, and Von Welch
University of Illinois at Urbana-Champaign

Abstract Control systems for energy such as Supervisory Control And Data Acquisition (SCADA) involve a hierarchy of sensing, monitoring, and control devices connected to centralized control stations/centers. With increasing connectivity to commercial off-the-shelf technologies these systems have become vulnerable to cyber attacks. To assist the energy sector in dealing with these cyber attacks, we propose the development of a taxonomy. In this work we take a first step towards a taxonomy by developing a comprehensive model of attacks, vulnerabilities, and damages in control systems. We populate the model with a survey of available literature from industry, academia, and national laboratories.

Keywords: Attack models, energy control systems, taxonomy

1. Introduction

Energy control systems involve a hierarchy of sensing, monitoring, and control devices connected to centralized control stations/centers. Within this hierarchy, control systems remotely monitor and control sensitive processes and physical functions. The Supervisory Control And Data Acquisition (SCADA) systems utilized to monitor power, oil, and gas transmission systems are common instantiations of such 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) technology.

*in Proceedings of the IFIP International Conference on Critical Infrastructure Protection, March 2008

Standard operating systems such as Windows or UNIX as well as common communication technologies such as the Internet, public-switched telephone networks, private Internet Protocol (IP) based 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 available commercial technologies causes process control systems for the energy sector to become increasingly connected and interdependent. This results in attractive targets for attacks. Along with the cost saving benefits of these 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 on control systems 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 botnet 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 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 control communication networks. Attacks that result in corruption of data can lead to propagation of false information to the control centers which results in unintended decisions and actions.

There is a relatively large body of work in academia, national labs, and industry involving security requirements, threats, attacks, and vulnerabilities in control systems [1, 3–8, 14, 16–18, 22, 24, 26, 28, 29]. However, each work adopted an ad hoc approach in discussing and prioritizing different aspects of attacks against control systems. To address this problem we argue that there is a need to develop a *taxonomy of attacks against energy control systems* that can be adopted by the community. Such a taxonomy will allow researchers and practitioners to have a common understanding of the following questions.

1. What are the different ways of perpetrating an attack against control systems?
2. What kind of damage can these attacks cause?
3. What are the challenges in preventing such attacks?
4. What are the requirements in developing adequate defense mechanisms?

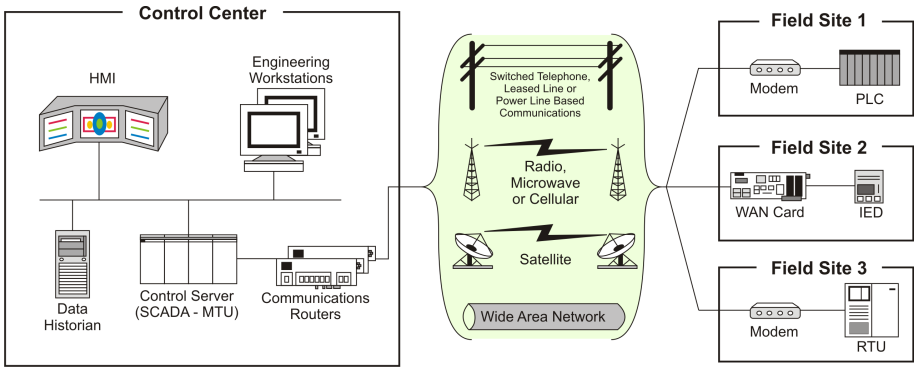

Figure 1. Sample SCADA Layout by Stouffer *et al.* [27]

In this work we take the first major step towards creation of such a taxonomy by developing a comprehensive attack model and populating the model with an extensive survey of known attacks against control systems. The model, called the Attack-Vulnerability-Damage (AVD) model, places equal importance on how attacks take place, what vulnerabilities allow these attacks to be performed, and what damage these attacks can cause. The model is geared specifically towards control systems. We believe it can serve as a basis for developing a taxonomy of attacks against energy control systems.

2. Overview of Energy Control Systems

Energy control systems include several types of systems such as SCADA systems, Distributed Control Systems (DCSs), and Programmable Logic Controllers (PLCs). These systems are critical to the continued generation, distribution, and delivery of energy to consumers in the oil, gas, and electricity 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 throughout SCADA and DCSs, as well as independently in small control systems.

In this work we use the SCADA system as a primary example of complex control systems that are common among a variety of energy sectors such as power, oil, and gas. Figure 1 illustrates a typical layout of a SCADA system [27]. SCADA systems use a wide variety of networking technologies to enable transmission of field data from field sites to the control centers, and of 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, action is taken as needed such as recording the data, processing alarms, or sending control information back to field sites. This data acquisition and supervisory control is undertaken by a combination of hardware and software systems connected by a multitude of networking technologies. Hardware includes PLCs, Remote Terminal Units (RTUs), IEDs, relays, SCADA servers (a.k.a. Master Terminal Units or MTUs), communication routers, workstations, and displays. These hardware systems run a variety of software such as data input and output processing, data transfer protocols, state estimators, visualization tools, data historians, equipment controllers, alarm processing and reporting, and remote access. All of these hardware and software systems are connected via local and wide-area networks depending on their proximity. Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites via communication mediums such as telephone line, cable, fiber, and radio frequency, such as broadcast, microwave, and satellite.

2.1 Unique aspects of energy control systems

With increasing 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. In this work we look at how these differences impact threat analysis and the need for a 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 continued generation, distribution, and delivery of energy. Second, there is a safety-first paradigm of these systems due to risks to equipment and personnel. Third, the power transmission system has a direct physical interaction with the control system. These are not necessarily distinct as they have an overlapping nature. Combined together they impact control system software, hardware, and networking in two ways.

1. Performance and Availability. Applications depend on data in a critical way requiring 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 in nature such that the failures of the security mechanism do not result in failure of the underlying control system.

2. Deployment and Management. Given the aforementioned aspects, control systems need to be extensively tested in "real" environments before they can be deployed. This is because they govern physical systems over vast geographic areas and deployed equipment typically has a long life (i.e. decades). Furthermore, while in operation they cannot suffer "down-time" for system maintenance and upgrades (e.g. for patch management) without significant advanced planning. In contrast, traditional IT systems are deployed with the initial deployment phase acting as a partial test environment, an expected lifetime of a few years, and expectations of being manageable with short notice downtimes for regular updates.

3. Goals, Challenges and Approach

In the development of a model for classifying cyber attacks against control systems, we had several goals.

- The model should be specific to cyber attacks against control systems. A good deal of research has been done on classifying cyber threats for general computer systems, e.g. [11, 15]. As power systems have begun to incorporate COTS technology (e.g. TCP/IP networks), much of this research can be applied to the power industry. However, there are aspects of a control system not found in a general computer system as discussed in the previous section. We would like our model to encompass such cases.
- The model should be "high-level". Some classification schemes for cyber threats for general computer systems seek to describe a particular attack in a detailed manner. For example, attack trees/graphs [4, 12, 23, 25] break down a single cyber attack into its constituent parts, tracing the attack from the source (attacker) through the various networking components to the target. We do not wish to enumerate every possible attack in such manner. Rather we want a system where parts of specific attacks can be sorted into generalized categories.
- The model should be easily expandable. As we populate the model with a relatively small number of papers dealing with incidents of cyber attacks on the power industry, we should not assume that our model is exhaustive. Any model we create should be able to incorporate instances of future cyber attacks and grow and adapt as necessary. The desire for easy expandability also supports the previous goal.

- The model should tolerate incompleteness. A report of a particular cyber attack on a power control system may give only a brief account of the attack. For example, one report may list how the attack was carried out, but omit the consequences of the attack. Another report may describe a vulnerability of a system and how exploiting that vulnerability would lead to damage, but omit how an attacker may carry out an attack. Such omissions are inevitable due to privacy concerns. However, our model should allow for such omissions while incorporating those aspects of the cyber threat that were reported.

With these goals in mind, we conducted an extensive survey of papers and industry reports. We found that nearly all of the papers contained threat descriptions. Several papers (e.g. [2, 20]) described the attack and the associated vulnerability, while other papers (e.g. [3, 10]) described the attack and its effects. One paper [8] discussed vulnerabilities and the impact or damage of an attack. This clustering of descriptions led us to the opinion that a cyber threat for the power industry can be decomposed into three broad categories: attack, vulnerability, and damage. This is the basis of our Attack–Vulnerability–Damage (AVD) model. While studying various classification models we found that [9] and the System–Fault–Risk (SFR) framework [30] matched well with our goals and helped inspire the development of our AVD model.

4. The Attack–Vulnerability–Damage (AVD) Model

In this section we present our AVD model and populate it with examples of real cyber attacks against energy control systems. Our AVD model is presented in Table 1.

The AVD model is composed of columns, each representing a category by which a specific cyber attack can be classified. To address the unique aspects of energy control systems discussed in Section 2, we designed the AVD model to have three broad categories for each attack: an "attack", a "vulnerability", and the "damage" incurred by an attack. In the attack category we include "local" origins and "system" targets to identify physical control system components that may be the origin of the attack (e.g. compromised/exposed end device) and/or the target (e.g. unauthorized opening of a relay). In the "vulnerability" category we similarly include configuration and implementation errors in the physical devices (e.g. malfunctioning device). For the "damage" category we consider damages caused to the computer systems in the control systems as well as the physical control system itself (e.g. electric power relays). Given

Table 1. Attack–Vulnerability–Damage (AVD) Model

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

the time-critical nature of the power grid, we also provide columns for performance effects and damage severity of the attack.

In the remainder of this section, we describe the model in detail and populate it with examples. Since control systems that face cyber threats have a strong overlap with Internet computer systems and networks, several categories and descriptions are common to those found in taxonomies for attacks on Internet systems. However, we focus on our goal of addressing control system security by adopting the above-mentioned approach for the model and using attack examples that are specific to the energy sector.

4.1 Attack

An attack is broken down into an "origin" of the attack, an "action" taken by the attack, and a "target" of the attack (Table 2).

Attack Origin: This describes the location of the attacker with respect to the target.

- Local: A local attack originates local to the target. Examples include an attacker with physical access to equipment [3, 13, 16] and a malfunction in a nearby piece of equipment [10].

- Remote: A remote attack originates somewhere outside the target site. This kind of attack usually occurs due to an unsecured connection such as an open wireless network or a trusted third-party physical connection. Examples include attacks through a dial-up modem [3, 20], an open wireless network [2, 3, 19, 29], a private network and bridge [21], and a connection to a trusted outside party [3].

Attack Action: This describes the activity the attack is performing on the target.

- Probe: A probe seeks to determine the characteristics of a particular system. An example is probing equipment to determine attributes such as the make and model of a device or the software services (and their versions) running on it [8, 18].
- Scan: A scan attempts to access targets sequentially for the purpose of determining specific characteristics. An example is a scan to determine open networking ports [2].
- Flood: A flood repeatedly accesses a target, overloading the target's capacity to handle traffic, possibly disabling the target. Examples include a data storm [10] and a denial of service attack [18].
- Authenticate: An attack on the authentication system attempts to perform unauthorized, illicit authentication as a valid user or process in order to access the target. An example is password cracking [18].
- Bypass: Use an alternative method to access the target, bypassing standard access protocols.
- Spoof: Spoofing attempts to assume the appearance of a different entity in the system thereby accessing the target. An example is session hijacking [18].
- Eavesdrop: Listen to a data stream and extract information. This typically assumes that the underlying data stream is not adversely affected. An example is monitoring (unencrypted) wireless traffic [29].
- Misdirect: Intercept proper communication channels and output bogus information. Here, the recipient is unaware that the output is not genuine. An example is cross-site scripting where the input is redirected to a malicious site which 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 would be read by a human, whereas a "copy" attack would duplicate the original data source for later processing by a human or another process. An example is downloading private business reports [2].
- Terminate: Stop a running process. This could be as specific as shutting down a service such as a monitoring or display system [13, 19], or as broad as shutting down an entire SCADA system [16].

- Execute: Run a possibly malicious process on the target. This is behavior typical of a computer virus, for example the Slammer Worm exploiting a MS-SQL vulnerability [19].
- Modify: Change the contents of the target. This include modifying SCADA system data or the protection settings of a device [16].
- Delete: Remove data from the target, or perhaps simply make the data impossible to retrieve.

Attack Target: This describes the resource that is being attacked.

- Network: A network consists of the computers, switches, hubs, etc. connected either via wires or wirelessly. When the network is the target of the attack, the intent is to make communications among the computers and switches difficult or impossible. Examples of such attacks include [10, 29].
- Process: A process is a program running on a computational device. A process consists of the actual program as well as any data being accessed by the process. Examples of attacks that target a process include the disabling of safety monitoring [19] and the use of computer resources to play games [16].
- System: A system consists of one or more connected components that can perform substantial computations. A system typically refers to a computer but could also describe a device such as a digital circuit breaker [20].
- Data: Data consists of information suitable for processing by humans or machines. Data can refer to a single resource such as a file stored on a hard drive, or the transmission of such data across a communications network. An example of an attack which targets data is unauthorized data access from a server [2].
- User: A user is someone with authorized access to a system. When a user is the target of an attack, the attacker typically attempts to illicitly gain information from the user for later use. An example is monitoring communications in order to discover the user's password [18].

4.2 Vulnerability

A vulnerability describes *why* a particular attack can be successful (Table 3). The vulnerability does not specify the actual target that is vulnerable, but rather the weakness in the system that can be exploited.

- Configuration: When a resource is improperly configured, a hacker can gain improper access. Examples include poor account management where certain unused accounts [8, 26, 28] and/or services

Table 2. Examples of "Attack" Category

Origin	
Local	*Remote*
Physical access to equipment	Dial-up modem
Malfunctioning programmable logic controller	Open wireless network
	Worm via private network and bridge
	Trusted third-party connection
Action	
Probe	*Scan*
Map available equipment	Simple vulnerability scan
Flood	*Authenticate*
Data storm	Password guessing/cracking
Denial of service attack	
Bypass	*Spoof*
Use alternative method to access process	Session hijacking
Eavesdrop	*Misdirect*
Monitor wireless traffic	Alarm output not displayed
Read/Copy	*Terminate*
Download business reports	Shutdown of service
	Shutdown of SCADA system
Execute	*Modify*
MS-SQL vulnerability	Alter metering data of SCADA system
	Change protection device settings
Delete	
Render data irretrievable	
Target	
Network	*Process*
Deluge of data	Disable safety monitoring
Wireless transmissions	Use computer resources to play games
System	*Data*
Digital circuit breaker	Business report
User	
Profile theft	

Table 3. Examples of "Vulnerability" Category

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	

Table 4. Examples of "Damage" Category

State Effect	
Availability	*Integrity*
Trip circuit breaker	Corrupt data received
Recirculation pump failure	
Confidentiality	
Business reports downloaded	
Performance Effect	
Timeliness	*Accuracy*
Slowdown of plant network	Missing alarm data
Precision	
Unable to view plant data	
Severity	
None	*Low*
Exploit was attempted without impact	Attacker gains additional information
Medium	*High*
Attacker degrades performance	Attacker acts as a legitimate user
Attacker alters state of system	Attacker gains admin rights
Loss of public confidence in services	Attacker spoofs displays via man-in-the-middle
	Attacker disables process
	Damage to equipment

[8] have (possibly high-level) access to the system; components with known flaws that are not correctly patched [8, 21, 26]; weak or non-existent authentication (including unchanged passwords) [5, 28]; and misconfigured perimeter protection and/or access control policy [2, 8, 20, 26].

- Design/Specification: When a process or component has design flaws, these flaws can be utilized in unintended ways to gain access to the system. Examples are usage of insecure communication protocols between processes or between a user and a process [5, 8, 26, 29] and flawed coding practices [8, 28].
- Implementation: Even when the design of a hardware or software system is correct, the implementation of the system may still be incorrect. This can lead to security holes [8, 19, 28] or to a lack of robustness that causes malfunctioning [10, 26].

4.3 Damage

Finally, there is the "damage" caused by a cyber attack. The damage is broken down into three columns: "state effects", "performance effects", and "severity" (Table 4). State effects and performance effects describe the actual damage done to the system components, while severity attempts to quantify the effects of the attack.

State Effect: A state effect describes the state change that occurs on the target as a result of the attack.

- Availability: The availability of an asset is determined by the responsiveness of the asset in its ability to service requests. A successful attack will disable an asset or increase its response time. Examples include the tripping of a circuit breaker [20] and the failure of a recirculation pump [10].
- Integrity: Integrity describes the correctness of an asset when meeting service requests. An example is the corruption of data.
- Confidentiality: An unauthorized use or access of an asset is also considered a confidentiality state effect. An example is an unauthorized access to business reports [2].

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

- Timeliness: This is a measure of time from input of data to output of data. When there is a sustained increase in this measure, a timeliness performance effect has occurred. An example is the slowdown of a plant network [19].
- Precision: This is a measure of the amount of output generated from the input of data. When the output is not 100% of the expected output, a precision performance effect has occurred. For example, when a process crashes before completing execution, output is less than 100% of the expected. When a wire tap is copying a data stream, double the amount of expected output is generated. An example is a shortcoming of data causing an "unable to view plant" condition [3].
- Accuracy: This is a measure of the correctness of the output generated by the input of data. When data has been altered during transmission, an accuracy performance effect has occurred.

Severity: With this column, we seek to quantify the damage by ascribing a level of impact.

- None: While the attack may have been successful, it had no noticeable impact on the target [8].
- Low: At low severity, the attacker typically gains information which may not be directly exploitable [2, 4, 8, 29]. An example would be discovering user names but not the associated passwords.
- Medium: At medium severity, the attacker can degrade system performance [8, 13, 21] and/or alter the state of the system [4, 19]. This is typically where one would start seeing state and/or performance effects. This may result in a loss of public confidence in system services [26].

Table 5. Example Attacks in the AVD Model

Attack Name	**Origin**	**Action**	**Target**	**Vulnerability**	**State Effect**	**Performance Effect**	**Severity**
Data Storm [10]	Local	Flood	Network	Specification	Availability	Precision	Medium
Slammer Worm (Remote) [19]	Remote	Copy	Process	Implementation	Integrity	Accuracy	Low
Slammer Worm (Local) [19]	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

- High: At the highest level of severity, the attacker can effectively act as a legitimate user [8], operator [3, 8], or administrator [4, 8] to disable processes [10, 20] or damage equipment [26].

4.4 Putting It All Together

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

5. Conclusions and Future Work

Control systems for energy such as SCADA have become vulnerable to cyber attacks. In order for the energy sector to deal effectively with these cyber attacks we argue that there is a need to develop a taxonomy. In this work we take a first step by developing a comprehensive model of attacks, vulnerabilities, and damages in control systems. We also populate the model with an extensive survey of available literature from industry, academia, and national laboratories.

In order to develop a taxonomy, the model needs to be expanded carefully by considering additional categories and sub-categories as well as analyzing additional attack data. Additional categories for consideration include (1) attack sophistication, i.e. the level of expertise required for the attack; (2) fiscal impact i.e. financial loss caused by the attack; and (3) protocol and operation system specifics, i.e. details of the attack in terms of specific protocols and operating systems exploited by the attack.

Acknowledgments

We would like to thank the entire Trustworthy Cyber Infrastructure for Power Grid project team for various discussions on cyber security and the anonymous reviewers for their comments and suggestions. This material is based upon work supported by the National Science Foundation under Grant No. CNS-0524695.

References

[1] Kenneth P. Birman, Jie Chen, Kenneth M. Hopkinson, Robert J. Thomas, James S. Thorp, Robert Van Rennesse, and Werner Vogels, Overcoming communications challenges in software for monitoring and controlling power systems, *Proceedings of the IEEE*, 9(5), 2005.

[2] Alan S. Brown. SCADA vs. the hackers, *Mechanical Engineering*, 124(12), December 2002.

[3] Eric Byres and Justin Lowe, The myths and facts behind cyber security risks for industrial control systems, In *VDE Congress*, pages 213–218, Frankfurt, Germany, November 2004, VDE - The Association for Electrical, Electronic & Information Technologies.

[4] Eric J. Byres, Matthew Franz, and Darrin Miller, The use of attack trees in assessing vulnerabilities in SCADA systems, In *IEEE International Infrastructure Survivability Workshop (IISW)*, December 2004.

[5] Rolf E. Carlson, Sandia SCADA program: High-security SCADA LDRD final report, Technical Report SAND2002-0729, Sandia National Laboratories, Albuquerque, NM, USA, April 2002.

[6] Jack Eisenhauer, Paget Donnelly, Mark Ellis, and Michael O'Brien, Roadmap to secure control systems in the energy sector, Technical report, Energetics Incorporated, Columbia, Maryland, USA, January 2006, Sponsored by The Office of Electricity Delivery and Energy Reliability, U. S. Department of Energy and The Science and Technology Directorate, U. S. Department of Homeland Security.

[7] Joseph Falco, James Gilsinn, and Keith Stouffer, IT security for industrial control systems: Requirements specification and performance testing, In *2004 NDIA Homeland Security Conference & Exposition*, Arlington, VA, USA, May 2004, National Defense Industrial Association.

[8] Raymond K. Fink, David F. Spencer, and Rita A. Wells, Lessons learned from cyber security assessments of SCADA and energy management systems, Technical Report INL/CON-06-11665, U. S. Department of Energy, Office of Electricity Delivery and Energy Reliability, September 2006.

[9] John D. Howard and Thomas A. Longstaff, A common language for computer security incidents, Sandia National Laboratories, Technical Report, SAND98-8667, Livermore, CA, 1998, October 1998.

[10] Robert Lemos, "Data storm" blamed for nuclear-plant shutdown, SecurityFocus, May 2007.

[11] Ulf Lindqvist and Erland Jonsson, How to systematically classify computer security intrusions, In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pages 154–163, Washington, DC, USA, 1997, IEEE Computer Society.

[12] Richard Lippmann, Kyle Ingols, Chris Scott, Keith Piwowarski, Kendra Kratkiewicz, Mike Artz, and Robert Cunningham, Validating and restoring defense in depth using attack graphs, In *Military Communications Conference (MILCOM)*, pages 1–10, October 2006.

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

[14] Miles A. McQueen, Wayne F. Boyer, Mark A. Flynn, and George A. Beitel, Quantitative cyber risk reduction estimation methodology for a small SCADA control system, In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, page 226, Washington, DC, USA, 2006, IEEE Computer Society.

[15] Jelena Mirkovic and Peter Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, *SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.

[16] Paul Oman, Edmund Schweitzer, and Jeff Roberts, Protecting the grid from cyber attack, part I: Recognizing our vulnerabilities, *Utility Automation & Engineering T&D Magazine*, 6(7), November 2001.

[17] Paul Oman, Edmund Schweitzer, and Jeff Roberts, Protecting the grid from cyber attack, part II: Safeguarding IEDs, substations and SCADA systems, *Utility Automation & Engineering T&D Magazine*, 7(1):25–32, January 2002.

[18] Paul W. Oman, Allen D. Risley, Jeff Roberts, and Edmund O. Schweitzer, III, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, In *55th Annual Conference for Protective Relay Engineers*, College Station, TX, USA, April 2002, Texas A&M University.

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

[20] Kevin Poulsen, Sparks over power grid cybersecurity, SecurityFocus, April 2003.

[21] Kevin Poulsen, Software bug contributed to blackout, SecurityFocus, February 2004.

[22] Robert Schainker, John Douglas, and Thomas Kropp, Electric utility responses to grid security issues, *Power and Energy Magazine, IEEE*, 4(2):30–37, March/April 2006.

[23] Bruce Schneier, Attack trees, *Dr. Dobb's Journal*, December 1999.

[24] Frederick T. Sheldon, Thomas E. Potok, Andy Loebl, Axel W. Krings, and Paul W. Oman, Managing secure survivable critical infrastructures to avoid vulnerabilities, In *IEEE International Symposium on High-Assurance Systems Engineering (HASE)*, pages 293–296, IEEE Computer Society, 2004.

[25] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M. Wing, Automated generation and analysis of attack graphs, In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 273–284, Washington, DC, USA, 2002, IEEE Computer Society.

[26] Jason Stamp, John Dillinger, William Young, and Jennifer DePoy, Common vulnerabilities in critical infrastructure control systems, Technical Report SAND2003-1772C, Sandia National Laboratories, Albuquerque, NM, USA, May 2003, 2nd Edition, Revised 11 November 2003.

[27] Keith Stouffer, Joe Falco, and Karen Scarfone, Guide to Industrial Control Systems Security, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-82, Second Public Draft, September 2007.

[28] Carol Taylor, Paul W. Oman, and Axel W. Krings. Assessing power substation network security and survivability: A work in progress report, In *Proceedings of the International Conference on Security and Management (SAM)*, pages 281–287, Las Vegas, Nevada, USA, June 2003, Paper 208SA.

[29] David Watts, Security & vulnerability in electric power systems, In *35th North American Power Symposium*, pages 559–566, Rolla, Missouri, USA, October 2003, University of Missouri-Rolla.

[30] Nong Ye, Clark Newman, and Toni Farley, A System-Fault-Risk framework for cyber attack classification, *Information, Knowledge, Systems Management*, 5(2):135–151, 2006.