Cyberthreats, Vulnerabilities and Attacks on SCADA Networks

Rose Tsang

abstract

Recent media and press attention has generated a lot of concern over the security of the U.S. critical infrastructure, and moreover, the ease and ability of cyberattackers to cause catastrophic failure of important utility services such as the electric power grid. However, to date, there have been remarkably few documented intentional cyberattacks on U.S. critical infrastructure networks. This work discusses the current state of today's Supervisory Control and Data Acquisition (SCADA) networks including information on recent attacks and incidents. So far, the most common threat agents have been unintentional threats caused by publicly released worms/viruses, accidents and incidents caused by disgruntled employees, former employees, and others that have worked within the organization. Vulnerabilities in SCADA systems, both historic and new due to the incorporation of new technology, are identified. Given the alarmist messages from government officials, politicians, policy analysts, and journalists, why hasn't a major cyberattack already occurred? This work discusses the significant technical hurdles to performing an attack with the intent to do serious widespread damage. However, this work does not dismiss the consequences of a serious attack. Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. An incident in one infrastructure may directly and indirectly affect other infrastructures through cascading and escalating failures.

1.0 Introduction

Supervisory Control and Data Acquisition (SCADA) systems are computer-based control systems which are used to monitor and control physical processes. They are usually composed of a set of networked devices such as controllers, sensors, actuators, and communication devices. In this report, SCADA systems are examined, although many aspects also apply to Industrial Control Systems (ICSs)[1], in general.

---

[1] The term *Industrial Control System (ICS)* encompasses the broad group of control systems found in industrial sectors and critical infrastructures. The most common types of ICSs are SCADA systems, Distributed Control Systems (DCSs) and Programmable Logic Controllers (PLCs). A PLC is a computer-based solid-state device. They are often used within DCS and SCADA systems. The primary difference between a DCS and a SCADA system is that a DCS is usually confined within a factory floor or plant whereas a SCADA system is geographically distributed.

SCADA systems are highly distributed systems used to control geographically dispersed assets. In these systems, centralized data acquisition and control over the distribution of assets are critical to system operation. SCADA systems are used in distribution systems such as electrical power grids, water distribution and wastewater collection systems, oil and natural gas pipelines, and railway transportation systems. These control systems, which are often highly interconnected and mutually dependent systems, are critical to the operation of the U.S. critical infrastructures. It is interesting to note that approximately 90 percent of the nation's critical infrastructures is privately owned and operated [Marburger].

In the past, the SCADA, and industrial control systems in general, that have been responsible for monitoring and controlling critical infrastructures and manufacturing processes operated in isolated environments. These control systems and devices communicated with each other within an isolated network, and rarely shared information with systems outside their environment. However, over time as more components of control systems have become interconnected with the outside world using Internet-based standards, and as control networks have become integrated into larger corporate networks in order to share valuable data, the probability and impact of a cyberattack has increased.

This report examines the possibility and implications of a cyberattack on a SCADA system. A **cyberattack**[Owens] is defined as the deliberate actions (perhaps over an extended period of time) to alter, disrupt, deceive, degrade and destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. A cyberattack consists of a *vulnerability*, an *access path* to the vulnerability and a *payload* to be executed. A *vulnerability* is an aspect (or defect) of a system that can be used by an adversary to compromise one or more of its attributes. An *access path* is the means by which a target can be reached. An access path to a target may be remote or close. A remote-access cyberattack is launched at some geographical distance from the adversary computer or network. A close-access cyberattack occurs in close proximity to the computer or network; in this type of attack the adversary has physical control over the device or network, just as an insider would. Close access is a possibility anywhere in the supply chain of a system that will be deployed. *Payload* is a term used to describe the action that will be performed once the vulnerability has been exploited. For example, a payload which functions as a virus will have a function of reproducing and retransmitting itself.

The next section describes the basic components of a SCADA system. There have been numerous asserted cyberattacks on critical infrastructures, especially since 9/11. Many of these are known to be urban legends [Lemos]. Section 3 describes actual documented cyberattacks and incidents on SCADA systems or ICSs. Section 4 discusses new vulnerabilities and new threat agents to SCADA systems. The specifics of a cyberattack on SCADA networks are discussed in Section 6. This includes risks, technical aspects to an attack as well as their consequences. Current efforts to secure SCADA networks are discussed in Section 6. Section 7 provides the Conclusion.

2.0 SCADA Systems

SCADA systems consist of hardware, software and communications components. Figure 1 shows the general layout of the basic components of a SCADA system. For simplicity, Figure 1 shows only the basic components of a SCADA system; for fault-tolerance purposes, SCADA systems are usually designed with significant redundancy built into the system. Figure 1 does not represent a secure SCADA system.

A **SCADA control center** performs centralized monitoring and control for field sites over wide area (long-distance) communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, or field devices in **field sites**. Field devices control local operations such as opening and closing valves or breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

The SCADA control center collects and logs information gathered by the field sites, displays information to the HMI (human machine interface) which may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The SCADA **control server** hosts the supervisory control software that communicates with the lower level control devices. The **Human-Machine Interface** (**HMI)** allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also displays process status and historical information to authorized users. The location, platform, and interface of the HMI may vary a great deal. For instance, an HMI could be located on a dedicated workstation in the control center, a laptop on a wireless LAN, or a browser on a system connected to the SCADA control center through the Internet. The **database/logging facility** stores process information. This information can be used to support different types of analyses, from statistical process control to enterprise level planning. The **communications router** transfers messages between different networks.
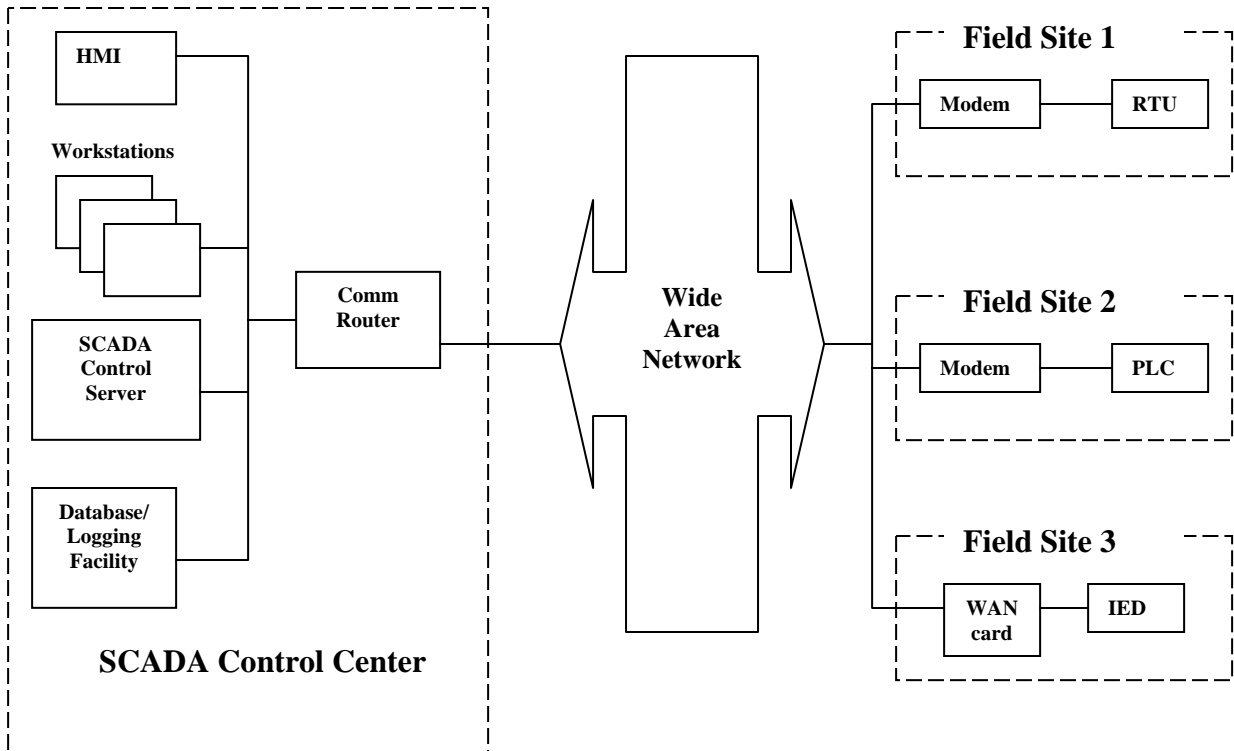
Figure 1: General Layout of a SCADA system

Each field site performs local control of actuators and monitors their associated sensors. A **Remote Telemetry Unit (RTU)** is a special purpose data acquisition and control unit designed to support the operations of SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces in order to support situations where wire-based communications are not possible. A **Programmable Logic Controller (PLC)** is a small industrial computer originally designed to perform logic functions executed by electrical hardware such as relays, switches, and mechanical timer/counters. Today's PLCs have become sophisticated controllers with the capability of controlling complex processes. They are used substantially in SCADA systems and DCSs. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs. An **Intelligent Electronic Devices (IED)** is a smart sensor/actuator which contains the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA systems allows for automatic control at the local level. Field sites are often equipped with a remote access capability which allow field operators to perform remote diagnostics and repairs (usually) over a separate dial up modem or WAN connection.

Communications architectures between the SCADA control center and various field sites vary among different implementations. The various architectures may by point-to-point, series, series-star, and multi-drop. Standard and proprietary communication protocols running over serial communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, and fiber, as well as radio frequency techniques such as broadcast, microwave and satellite.

3.0 Known Cyber Attacks and Incidents
There are three broad categories of documented attacks on SCADA systems, other industrial control systems or critical infrastructures.

- Intentional targeted attacks such as gaining unauthorized access to computers within the network infrastructure, performing a Denial of Service (DoS) attack, or spoofing[2].

- Unintentional consequences or collateral damage from worms, viruses or control system failures

- Unintentional consequences caused by internal personnel or mechanisms. This may include the testing of inappropriate software on operational systems or unauthorized system configuration changes.

The first category of attacks, the intentional targeted attacks, have the most potential for damage, however are the least frequently occurring. An intentional targeted attack requires detailed knowledge of the system and supporting infrastructure and are almost always caused by an insider with personal grievances[3].

3.1 Intentional CyberAttacks
So far there have been remarkably few documented intentional cyberattacks on critical infrastructure networks. This section describes those few known cases.

January 2000: Maroochy Shire Sewage Spill [Slay]. The most well-known attack upon a SCADA system was the attack on the Maroochy Shire Council's sewage control system in Queensland, Australia. On January 2000, almost immediately after the control system for the sewage plant was installed by a contractor company, the plant experienced a series of problems. Pumps failed to start or stop when specified. Alarms failed to be reported. There were intermittent loss of communications between the control center and the pumping stations. At the beginning, the sewage system operators thought there was a leak in the pipes. Then they observed that valves were opening without being

---

[2] A spoofing attack occurs when one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Internet Protocol (IP) spoofing is one of the most common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine.

[3] See www.cert.org/archive/pdf/**insider**cross051105.pdf

commanded to do so. Still they did not consider it was an attack. It was only after months of logging that they discovered that spoofed controllers were activating the valves. It took several more months to find the culprit: a disgruntled ex-employee of the contractor company that had installed the control system originally. The ex-employee was trying to convince the water treatment company to hire him to solve the problems he was creating.

The effect of the attacks was the flooding of the grounds of a nearby hotel, park, and river with approximately 264,000 gallons of raw sewage. In analyzing this attack, one of the insights was that cyberattacks may be unusually hard to detect (compared to physical attacks). The response to this attack was very slow; the attacker managed to launch 46 documented attacks before he was caught.

March 1997: Worcester Air Traffic Communications Attack [CNN]. In March 1997, a teenager in Worcester, Massachusetts broke into the Bell Atlantic computer system and disabled part of the public switched telephone network using a dial-up modem connected to the system. This attack disabled phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. The tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland.

2000 and 1982: Gas Pipelines in Russia (and the former Soviet Union). In 2000, the Interior Ministry of Russia reported that hackers seized temporary control of the system regulating gas flows in natural gas pipelines, although it is not publicly known if there was physical damage [Quinn-Judge]. The former Soviet Union was victim of an attack to their gas pipeline infrastructure in 1982 when a logic bomb caused an explosion in Siberia [Reed].

3.2 Unintentional CyberAttacks and Incidents
Unintentional cyberattacks and cyber incidents fall into two categories. Those caused by "public" worms or viruses unleashed on the public Internet, as well as those caused by the inadvertent behavior of someone (usually) working on-site.

Incidents involving collateral damage from publicly released worms and viruses include the following

August 2005: Automobile plants and the Zotob Worm [Roberts]. Zotob is a worm that spreads by exploiting the Microsoft Windows Plug and Play Buffer Overflow Vulnerability[4]. In August 2005, Zotob crashed thirteen of DaimlerChrysler's U.S. automobile manufacturing plants forcing them to remain offline for almost an hour. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were also forced down. Zotob affected computers by slowing them down and causing them to continually crash and reboot. Infected Windows 2000 computers were potentially left exposed to more malicious attacks, while infected Windows XP computers can only continue to

---

[4] See http://www.microsoft.com/technet/security/Bulletin/MS05-039.mspx

spread the worms. While the Zotob worm itself did not have a destructive payload, it left an open backdoor control channel that could allow attackers to commandeer the infected machine. The worm also added several lines of code into a machine to prevent it from accessing certain antivirus websites. Zotob and its variations also caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.

August 2003: CSX Train Signaling System[5] and the Sobig Virus. The Sobig computer virus arrives in an e-mail with an attachment that when opened infects the computer and sends itself on to other victims using e-mail addresses from the victim's address book. Thus the virus rapidly spreads itself to other machines and makes it difficult to trace back to the source.   The virus also infects the computer by opening a back door that lets a hacker gain access without detection. Spammers can then use the back door to upload applications that send spam anonymously. Sobig was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were also delayed between four and six hours.

January 2003: Davis-Besse Ohio Nuclear Power Plant[6] and the Slammer Worm. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as the Slammer worm[7] infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again.

The Slammer worm entered the Davis-Besse plant through the unsecured network of an unnamed Davis-Besse contractor. The worm was then transmitted through a T1 line bridging that network and Davis-Besse's corporate network. Investigators later found that the T1 line was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall.   From the corporate network, the worm spread to the plant network, where it found residence in at least one unpatched Windows server. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.

---

[5] Additional information on the CSX Train Signaling System incident can found at: http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807

[6] Additional information on the Davis-Besse incident can found at: http://www.securityfocus.com/news/6767

[7] The Slammer worm (also called the Sapphire worm) had an extremely high infection rate.   As it began spreading through the Internet, it doubled in size every 8.5 seconds. Within 10 minutes, it infected more than 90% of vulnerable hosts.   Slammer exploited a buffer overflow vulnerability in computers running Microsoft's SQL Server or MSDE 2000. It is interesting to note that there were no known electric system outages or disruptions of service. For details see http://www.caida.org/publications/papers/2003/sapphire/sapphire.html.

The following incidents were caused by accidents.

March 2008: Hatch Nuclear Power Plant shutdown[8]. The Hatch Nuclear Power Plant in Georgia went through an emergency shutdown as a result of a software update that was made on the plant's business network. The business network was in two-way communication with the plant's SCADA network and the update synchronized information on both systems. Reset after a reboot, the SCADA safety systems detected a lack of data and signaled that the water level in the cooling systems for the nuclear fuel rods had dropped, which caused an automatic shutdown. Engineers were aware of the two-way communication link, but they did not know that the update would synchronize data between the two networks. There was no danger to the public, but the power company lost millions of dollars in revenue and had to incur the substantial expense of getting the plant back. As a result of this problem, the engineers chose to sever all physical connections between the SCADA and business networks.

August 2003: Northeast Power Blackout[9].   On August 14, 2003, large portions of the Midwest, Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm EDT, and power was not restored for fourdays in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of total costs in the United States range between $4 billion and $10 billion dollars.

 The Department of Energy's Office of Energy concluded[10] that the failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate *situational awareness* of critical operational changes to the electrical grid. In addition, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345kV transmission lines in Northern Ohio tripped due to contact with trees. Much earlier, the trees should have been identified as a potential vulnerability and **trimmed**. The initial failure resulted in a cascading series of overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. A total of 61,800 MW load was lost as 508 generating units at 265 power plants tripped.

June 1999: Bellingham, Washington Gasoline Pipeline Failure [NTSB].
In June 1999, 237,000 gallons of gasoline leaked from a 16" pipeline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1 1/2 hours after

---

[8] See http://www.reuters.com/article/pressRelease/idUS158811+30-Jul-2008+PRN20080730

[9] Additional information on the Northeast Power Blackout incident can found at:
http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf

[10] See http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf

the rupture, the gasoline ignited and burned approximately 1 1/2 miles along the creek causing 3 deaths and 8 documented injuries. A single-family residence and the city of Bellingham's water treatment plant were severely damaged. The total property damages were estimated at $45 million. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation.   The National Transportation Safety Board (NTSB) report issued October 2002 cited one of the five key causes of the accident was the Olympic Pipe Line Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline, which led to the system becoming non-responsive at a critical time during pipeline operations.

3.3 Aggregate Data

BCIT (British Columbia Institute of Technology), funded by a petroleum company, is one of a few groups which tracks industrial cyber security incidents[11]. Their database, the Industrial Security Incident Database (ISID), tracks information regarding security related attacks on process control and industrial networked systems. The information stored per incident includes: the nature of the attack, attack vector and equipment used. Prior to 2001, the majority of attacks reported in the database were from insiders of the company. After 2001, the majority of the incidents reported were due to external sources. This swing has been attributed to the increase in use of more common operating systems and applications, larger interconnected networks and automated "worm" attacks.

Between 1994 and June 2006, 97 incidents have been investigated and logged in the database, with 15 incidents still pending investigation. Of these, 13 were flagged as hoax or unlikely and removed from the study data.   Figure 2 shows the trend between 1994 and 2006.

Incidents are obtained from either organizations voluntarily submitting a form to ISID investigators, or from ISID staff gathering reports from public sources such as the Internet, discussions at SCADA/industrial cybersecurity conferences, and relevant industrial publications. When an event is either submitted by an ISID member or noted in a public forum, it is reviewed and verified by the ISID researchers.

---

[11] For more information on the BCIT industrial security database see
http://www.andritzautomation.com/documents/industrialcybersecurity.pdf
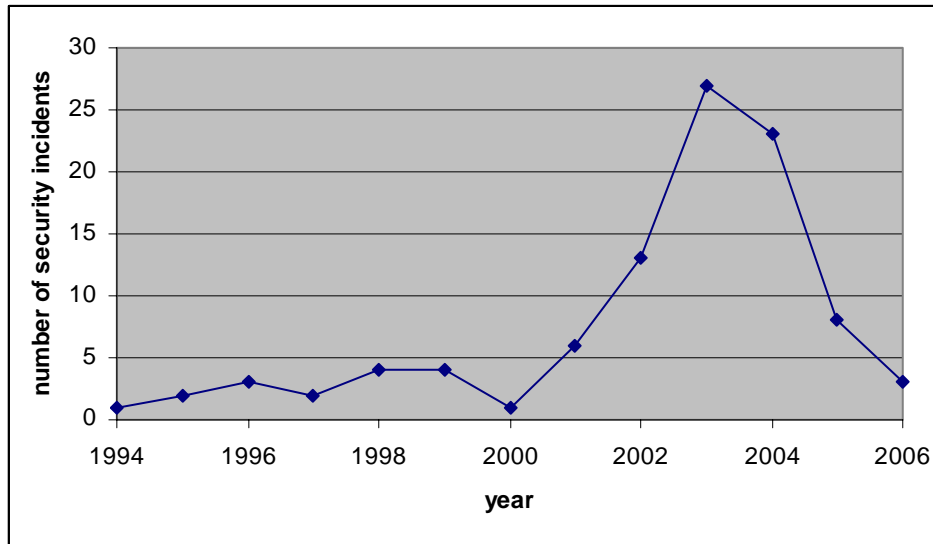
Figure 2: Industrial Security Incidents by Year

From examining the data and individual incidents, the most likely threat agents appear to be unintentional threats caused by publicly released worms/viruses and accidents and disgruntled employees, former employees, and others that have worked within the organization.

[Byers] notes that for external incidents between 2002 and 2006, 78% were the result of common viruses, Trojan horses, or worms. The three worms (Slammer, Blaster, and Sasser) accounted for over 50% of the incidents. It is interesting to note that the majority of these attacks occurred months or years *after* the virus/worm was publicized in the media and patches were available and proven for control systems. This is indicative of a lapse in security policy rather than technology.

4.0 New Vulnerabilities and Threats

A vulnerability is an aspect (or defect) of a system that can be used by an adversary to compromise one or more of its attributes. A defect may be introduced accidentally or intentionally. Accidental defects are often introduced through a design or implementation flaw. This defect, or bug, may be exploited by an attacker who either accidentally discovers it, or "hears" about it from other sources. Today, after they are discovered, many vulnerabilities are widely publicized and thus may be exploited by anyone with sufficient technical skills until a patch can be disseminated and installed.

4.1 New Vulnerabilities

For many decades control systems have been at the core of critical infrastructures and industrial plants, yet, there have been very few confirmed cases of cyberattacks.

However, many [Eisenhauer,Tenable] believe that control systems such as SCADA facilities are more vulnerable now than ever before. The following list reasons why the current generation of SCADA systems are considered vulnerable.

External connectivity. Control systems are now not only remotely accessible for troubleshooting purposes, but increasingly, for practicability and efficiency reasons, they are being connected to corporate networks and the Internet. Even control systems designed to be closed may, in practice, not be perfectly isolated: connectivity through uncontrolled connections can occur in many ways (e.g., via mobile devices, dialup connections). Internet-connected embedded devices are expected to be the largest contributors to the growth of the Internet in future years [Marburger].

Commodity software and hardware solutions. In the past, control systems were primarily made up of proprietary software and hardware components. However, with the decreasing prices of commodity software and hardware, as well as the increasing requirements for connectivity outside of the control system network itself, many control systems employ commodity systems, such as Microsoft Windows computers, TCP/IP networking etc. As a result, control systems inherit the vulnerabilities of these commodity components.

Computer-controlled controllers. Most of the original physical controls (traditionally conformed of a logic of electromechanical relays) have been replaced by microprocessors and embedded operating systems. These controllers may provide many new functionalities, such as flexible configuration via a web server, and digital communication capabilities that allow remote access and control. The increased complexity of the software base may also increase design and implementation flaws, and, hence, increased number of vulnerabilties open for exploitation.

Rapidly growing global workforce. Larger groups of people can now find and generate attack vectors for computer-based systems.

Open design. The move to open standards such as Ethernet, TCP/IP, and web technologies has resulted in commonly released worms/viruses also affecting the computer systems of critical infrastructure and manufacturing industries. Hence it may be easier for an adversary to obtain the necessary knowledge, via the source code, to attack a system. It is important to note that this point is controversial; many computer scientists argue that open design is the most secure solution [Andersen].

Increasing size and functionality. The wide-spread use of 802.11 WLANs has created countless opportunities for intrusion and information theft. Wireless sensor networks and actuators allow industrial control systems to instrument and monitor large numbers of events and operations. Some infrastructures are also changing to provide new functionalities, such as the Smart Grid program[12] [6]. These new functionalities may give rise to new vulnerabilities.

---

[12] See: Department of Energy, Smart Grid, http://www.oe.energy.gov/smartgrid.htm.

4.2 Types of Adversaries

This section breaks up the different types of potential adversaries in the following categories: (i) lone individual (coder/hacker), or small group of individuals, (ii) insider(s) with malicious intent, (iii) criminal groups, (iv) terrorist groups, and (v) nation-states.

The lone individual (coder/hacker), or small group of individuals. The threat behind any cyberattack is a human who has access to a computer and the internet. A **highly skilled coder** is a sophisticated programmer who has the ability to find unique vulnerabilities in existing software and to create working exploit codes. They would have the equivalent of an undergraduate degree in computer science with an emphasis on the systems area. They would have a deep understanding of the TCP/IP[13] network protocol as well as network and security protocols in general, and understand operating systems concept. They would need several years of hands-on experience in an IT environment so they could perform host platform vulnerability assessments and understand hardening standards and methodologies.

The **low skill coder**, often called the "script kiddie", is the most common type of hacker. Their name (script kiddie) comes from the fact that members of this group generally rely on previously coded scripts and prepackaged hacking tools downloaded from the Internet to do their hacking. Script kiddies are often challenged by the notion of gaining unauthorized access and are sometimes open to using untested pieces of code without knowing their consequences. If a low skill coder penetrates a corporate network, and have malicious intent, they could wreak havoc until they are detected. A low skill coder would be subject to quick detection because of their inability to cover their tracks.

There are **mid skill coders** who have capabilities in between the low skill coder and the highly skilled coder but we usually focus on the highly skilled coder because of their capabilities to actually impact systems, and the low skill coders because they make up the overwhelming majority of the "hackers" in the world.

It is important to note that most highly skilled coders/hackers are *not* malicious. In fact, some are actively involved in developing technologies that can be used to improve overall computer and network security. Coders can work independently or through a network of hacking teams that run exploits from a variety of locations, making it difficult to trace the activities back to their source. These teams can be developed in Internet Relay Chat (IRC) channels, in conferences such as DefCon[14], or in small groups of computer savvy friends. Often coders create the programs and other members of the team run them against target networks. This creates a reputation for the group rather than a single individual.

---

[13] TCP/IP: Transmission Control Protcol/Internet Protocol is the basic communication language or network protocol of the Internet. It consists of a set of rules that define how information is routed and sent through a network.

[14] DefCon is the largest underground hacking conference. See http://www.defcon.org

The Insider(s). The disgruntled insider is a principal source of computer crime and sabotage[15]. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems. Insiders may be employees, contractors, or business partners.

Criminal Groups. The primary motivation of a criminal group launching, or seeking to launch, a cyberattack on a SCADA facility would be extortion.[16] [Greenberg, 2008] reveals that a CIA official publicly announced that hackers have penetrated power systems in several regions outside the United States, and in at least one case caused a power outage affecting multiple cities.

Terrorist Group. Most terrorist groups seek higher-impact targets than bringing down a critical infrastructure, even one in the USA. However, a group with a long enough time horizon and enough financial backing may develop capabilities on par with nation-states.

Nation-States. A nation state, or highly motivated terrorist group, most likely could develop the capabilities to bring down a SCADA facility, or even a network of facilities. Besides being able to recruit highly-skilled coders, hire control system engineers and bribe insiders, they also have the capabilities to do the following.
- Obtain the source code for proprietary software and thus identify vulnerabilities unknown to the general public.
- Persuade vendors or their employees to intentionally insert "backdoors" or other zero-day vulnerabilities into their software code or hardware devices. A zero-day vulnerability is a vulnerability which the adversary has known about for some time but the defender has known about for zero days.
- Obtain (usually buy) the system of interest in order to understand its operational strengths and weaknesses as well as its vulnerabilities.

5.0 SCADA CyberAttacks

The complexity of modern SCADA systems leaves many vulnerabilities as well as vectors for attack. Attacks can come from many places, including indirectly through the corporate network, virtual private networks (VPN), wireless networks, and dial-up modems. Possible attack vectors on an SCADA system include:

- **Backdoors and holes in network perimeter**.

- **Vulnerabilities in common protocols**.

- **Database attacks**.

- **Communications hijacking and 'man-in-the-middle' attacks.**

---

[15] See www.cert.org/archive/pdf/**insider**cross051105.pdf
[16] See http://www.infosecurity-us.com/view/1194/cia-claims-hackers-attack-global-power-grid/

5.1 Risks in SCADA systems

The following is a list of some risks which are inherent to SCADA systems.

- **Difficulty in using standard intrusion detection techniques**. The "network vulnerability scanner" has become a standard tool for quickly and actively discovering hosts on a network, which services they are running, and which vulnerabilities may be present. Unfortunately, the techniques of port scanning, service fingerprinting, and rapidly probing hosts to determine the present vulnerabilities sometimes results in locking devices, disrupting processes and causing erroneous displays in control centers. Since SCADA networks must run 24/7 these disruptions are unacceptable. Thus many SCADA control networks are more unlikely to perform extensive intrusion detection.

- **Loose (or rogue) connections**. SCADA systems have stringent reliability and availability requirements. When there is a need to troubleshoot and repair, the technical resources may not be physically located at the control room or facility. Traditionally SCADA systems use modems to enable vendors, system integrators, or control engineers maintaining the system to dial in and diagnose, repair, configure, and perform maintenance on the network or component. While this allows easy access for authorized personnel, if the dial-up modems are not properly secured, they can also provide backdoor entries for unauthorized use. Dial-up often uses remote control software that gives the remote user powerful (administrative or root) access to the target system.

  Besides modems, other connections which provide adversaries with access to a SCADA system include: wireless, third-party connections, Virtual Private Networks (VPNs), mobile devices such as laptops, PDAs and Flash drives, and the Internet. There are many ways these connections can be exploited. For instance, if a laptop is used in both a SCADA system and in a less secure home environment, malware obtained in one setting may be unwittingly transferred to the other. Typical motivations for connecting a SCADA system to an Internet, even temporarily, include the desire to download system patches or antivirus updates from vendor web sites, or the desire to conduct typical office activities (such as email) from the plant floor.

- **Protocols with lack of support for authentication**. SCADA systems use specialized protocols, such as MODBUS/TCP, EtherNet/IP, and DNP317, to communicate between most control devices. Unfortunately, these protocols were designed without security built in and do not typically require any authentication to remotely execute commands on a control device.

5.2 Technical Aspects of Launching a CyberAttack on a SCADA System

All but the most naïve adversary would seek to conceal their identity, (i.e., the machine which would launch the attack), before initiating any steps to an attack or even a preliminary set-up or probe for an attack. The method for concealing the identity of the adversary's machine is to set up an intermediary machine(s) which would directly probe or attack the target network. This would entail doing one of the following: (i) set up an anonymous proxy, which is a tool that makes any activity performed difficult to trace, (ii) set up a "botnet[17]" of intermediary machines, or (iii) enlist the services of a bot-network operator from the underground market, i.e., "rent" a bot-net.

Two major deterrents to adversaries include system hardening[18] and intrusion detection systems[19]. However it is important to note that consistent system hardening is dependent upon a disciplined security staff who will monitor the uses of every computer/device and disable all components which are not necessary for its correct execution. Intrusion detection systems also require dedicated administration and correct configuration from the security staff.

Access Path. There are many ways a system can be penetrated. We describe two ways.

- **Laying Bait**. The easiest and quickest way to obtain unauthorized access into a secured network is to get someone on the inside to perform an action that would result in creating a backdoor. [DarkReading] reported how as part of performing a vulnerability assessment for a credit union, they scattered 20 USB drives (containing "adversary" software) in the employee parking lot. Within a few hours, 15 of the 20 drives had been plugged into machines on the internal network, and thus were running the "adversary" software. The "adversary" now had easy entry into the internal network. There are many other ways to do this, e.g. sending forged email to many employees which tricks them to download something they think they want. Once they click on the link, they have just installed a Trojan horse or backdoor onto their harddrive!

- **Remote Access.** Many vendors of SCADA devices provide systems with dial-up modems that provide remote access so technical field support staff can access the devices remotely. Remote access also provides support staff with administrative-

---

[17] A botnet is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (such as spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - a computer "robot" or "bot" that serves the wishes of the originator. Most computers compromised in this way are home-based.

[18] In the process of *system hardening*, unnecessary services and applications are removed from machines and networks. Unnecessary, open ports are also shut down. This decreases the number of vulnerabilities a system may be exposed to.

[19] Intrusion detection systems (IDS) monitor events on a network, such as traffic patterns, or a system, such as log entries or file accesses, so that they can identify an intruder breaking into or attempting to break into a system. An IDS should be able to recognize unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files.

level access to a system. Adversaries with war dialers, or programs that dial consecutive phone numbers looking for modems, and password cracking software may gain access to systems through these remote access capabilities. Passwords used for remote access are often common to all implementations of a particular vendor's systems and may have not been changed by the end user. These types of connections can leave a system highly vulnerable because people entering systems through vendor-installed modems are often granted high levels of system access.

Payload. As mentioned in the Introduction, payload is a term used to describe the action that will be performed once a vulnerability has been exploited.

1. Denial of Service. Since the adversary has already penetrated the SCADA network, DoS implies DoS on an individual machine/device, a group of devices or an entire subnetwork, inside a SCADA network. DoS attacks are considered the easiest type of attack to launch.
2. Addition of software infected with malware which will disrupt the performance of the network and/or the machines on the network
3. Changes to the software or modifications to the configuration settings (some reverse engineering may be needed).
4. Spoofing system operators and/or devices on the control network. This is the most difficult payload to execute but would provide an adversary with the most capabilities. Depending upon the level of spoofing it may require a LOT of reverse engineering which is a very time consuming and challenging process.
5. Changes to instructions, commands (same difficulty as above).

Protocol manipulation, vulnerability exploitation and the man-in-the-middle attacks are among the most popular ways to manipulate insecure protocols, such as those found in control systems.

- **Vulnerability exploitation.** Once an adversary has access to the control network there are many publicly known vulnerabilities in versions of some typical SCADA protocols. [Tenable] has identified several methods, e.g., performing a port scan, accessing a web server on a device with a URL different than what the device was expecting, all of which will result in the device reaching a failure mode. The failure mode may cause the device to immediately crash or may take several queries to result in a crash. Still other failure modes may result in slow performance or cutting off access to other services. Most of these publicly known vulnerabilities have had patches issued by their manufacturers, or have issued new versions which have removed these vulnerabilities. However, as mentioned before, it takes consistent monitoring by system administrators to keep current of all system software updates and patches on all of the devices in the network.
- **Spoofing (Replay attack)**. In this form of attack, captured data from the control/HMI is modified to instantiate activity when received by the device controller. Captured data reflecting normal operations in the Control Center is played back to the operator as required. This would cause the operator's HMI to

appear to be normal and an attack will go unobserved. During this replay attack, the adversary could continue to send commands to the controller and/or field devices in order to cause an undesirable event while the operator remains unaware of the true state of the system

- **Communications hijacking (or man-in-the-middle).** In this attack, false messages are sent to the operator, and could take the form of a false negative or a false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required. The adversary could send commands to the operator's console indicating a system change, and when the operator follows normal procedures and attempts to correct the problem, the operator's action could cause an undesirable event. There are numerable variations of the modification and replay of control data which could impact the operations of the system.

Note that the last two attacks are also **integrity attacks**. A control systems operator must rely on the integrity of the information in order to take appropriate actions based on the readings or status of the system.

Sophisticated target attacks may be possible through traffic analysis of control systems. Performing traffic analyses would allow an attacker to reverse engineer the protocols. This information, along with operational data, may then be used for a targeted attack. Other sophisticated targeted attacks are possible by studying the control system applications to discover and exploit vulnerabilities to gain control of the system. These attacks require the adversary to gather a lot of data traversing the control network. This data must be transmitted outside the SCADA facility and onto the adversary's system where it is analyzed. This is a very time consuming process and requires the adversary to have an in-depth understanding of the protocols used, the control system architecture and the high-level application. In this case, the adversary must have the skills of a highly skilled coder.

5.3 Cyberattack Consequences
Is it possible to remotely cause physical damage to equipment in a SCADA facility?
Most SCADA devices have a variety of physical and electronic safety precautions. For example, anything that moves, most likely, has control logic in it that limits the top speed. Similarly, ovens, power generators, power relay stations all have physical safety limitations built into them. Despite these built-in precautions, an insider would know where the safety mechanisms are located as well as having the knowledge to affect some sort of damage inside the operating parameters.

On March 2007, engineers at Idaho National Laboratories staged a cyberattack which caused a power generator to "self-destruct". This incident, known as the "Aurora Generator Test" demonstrated the ability of a cyberattack to damage a power generator turbine [Meserve]. This attack was videotaped and sent to CNN where it received a lot of national attention. However, no detailed information has been released discussing how

an actual remote adversary could have found a vulnerability and/or access path to reach the generator, in the first place.

Another example of a theoretical remote attack which could cause physical damage is the rerouting of electricity in the power grid.   Assume an adversary has used a war dialer to get access to several modems connected to the programmable breakers of the electric power transmission control system. The adversary then cracks the passwords that control access to the breakers, and changes the control settings to cause local power outages and damage equipment. The adversary lowers the settings of the electric flow on some circuit breakers which causes those lines to go out of service and then diverts the power to neighboring lines. At the same time, the adversary raises the settings on neighboring lines, preventing the circuit breakers from tripping, and thus overloading the lines. This may cause significant damage to transformers and other critical equipment, resulting in lengthy repair outages.

Why hasn't there already been a significant attack on the critical infrastructure?
Given the amount of attention the media and press has allocated to potential attacks on critical infrastructure networks, it is natural to ask the above question. A serious attack to debilitate the national critical infrastructure would require the following elements.

- **Highly trained personnel**. Many highly skilled coders, control system engineers and insiders with detailed knowledge of the control system, and supporting infrastructure. One of the few known cyberattacks, the Maroochy sewage spill (described in Section 3), was performed by an insider who had just setup the control system which he later attacked.   Detailed knowledge of the internals of the control system is crucial.
- **A reasonably long time horizon**. It takes a significant amount of time and patience to perform a sophisticated remote attack.   It is likely that just to reverse engineer a single SCADA control center network might take several highly skilled coders at least 6 months. Every SCADA control center is configured differently, with different devices, running different software/protocols; performing an attack on multiple SCADA facilities would require a new attack plan for each facility.
- **A tolerance for failure**. It is impossible to test whether an attack will succeed or not (as one may be able to do with traditional weapons). The risk is that once an attack is launched, if it fails, the adversaries will most likely defend themselves by hardening their systems in order to make future attacks more unlikely. Failure would mean a new much more complicated and sophisticated attack must be planned for the future.

Probabalistic Consequences. The consequences of a cyberattack vary greatly from a simple Denial-of-Service attack on a single control device in a SCADA network to a wide-scale cascading failure of multiple interconnected SCADA networks. As the previous subsection described there are many intermediate-level type attacks too. One interesting aspect of cyberattacks is that their outcome may be *probabilistic*. Real-life control systems often fail in non-deterministic ways. Recall the August 2003 Northeast

Power Blackout (as described in Section 3). The initial failure led to to an uncontrolled cascading failure of the grid which resulted in bringing down 508 generating units at 265 power plants. Extrapolating then, it may be possible for an attack which simply reroutes a few electrical circuits on the power grid to also cause a series of cascading failures which damage more than what was originally intended.

6.0 Current Efforts to Secure SCADA Networks

Up to now, most of the effort for protecting control systems (and in particular SCADA) has focused on reliability, i.e., the protection of the system against random faults. There is, however, an urgent growing concern for protecting control systems against malicious cyberattacks [Alvaro,Eisenhauer,Owens,Quinn-Judge,Tenable,Huang].

There are several industrial and government-led efforts to improve the security of control systems. Several sectors – including chemical, oil and gas, and water– are currently developing programs for securing their infrastructure.

- The electric sector is leading the way with the North American Electric Reliability Corporation (NERC) cybersecurity standards for control systems[20]. NERC is authorized to enforce compliance to these standards, and it is expected that all electric utilities are fully compliant with these standards by 2010.

- The American Gas Association (AGA) has developed a series of documents[21] which recommends practices designed to protect SCADA communications against cyber incidents. The recommended practices focus on ensuring the confidentiality of SCADA communications.

- The American Petroleum Institute (API) represents more than 400 members involved in all aspects of the oil and natural gas industry. The API standard[22] provides guidelines to the operators of oil and natural gas pipeline systems for managing SCADA system integrity and security. The guideline is specifically designed to provide operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual organizations.

- The Chemical Sector Cyber Security Program[23] (CSCSP) is a strategic program of the Chemical Information Technology Center (ChemITC) of the American Chemistry Council. The CSCSP program focuses on risk management and reduction to minimize

---

[20] NERC-CIP, Critical Infrastructure Protection. North American Electric Reliability Corporation, http://www.nerc.com/cip.html, 2008.

[21] American Gas Association, Standard 12, "Cryptographic Protection of SCADA Communications", http://www.awwarf.org/research/TopicsAndProjects/Resources/SpecialReports/2969/

[22] American Petroleum Institute, Standard 1164, "Pipeline SCADA Security", http://api-ec.api.org/.

[23] Chemical Sector Cyber Security Program, http://www.chemicalcybersecurity.com/

the potential impact of cyber attacks on chemical-related business and manufacturing systems.

Government-led efforts and standards-based bodies include the following.

- The Department of Energy has also led security efforts by establishing the national SCADA test bed program [INL] and by developing a 10-year outline for securing control systems in the energy sector [Eisenhauer]. The report identifies four main goals: (1) measure current security, (2) develop and integrate protective measures, (3) detect intrusion and implement response strategies; and (4) sustain security improvements.
- ISA, a society of industrial automation and control systems, is developing the ISA99 Industrial Automation and Control Systems Security Standards[24], a security standard to be used in manufacturing and general industrial controls.
- Under the Department of Energy, Sandia National Laboratories has established the Center for Control System Security [25]. This center is composed of several test bed facilities, which allow real-world critical infrastructure problems to be modeled, designed, simulated, verified, and validated. These labs are integrated into a research effort focusing on solving current control system security problems and developing next generation control systems.
- The use of wireless sensor networks in SCADA systems is becoming more commonplace. A number of companies have teamed up to bring sensor networks in the field of process control systems, and currently, there are two working groups to standardize their communications [Hart, ISA]. Their wireless communication proposal has options to configure hop-by-hop and end-to-end confidentiality and integrity mechanisms. Similarly they provide the necessary protocols for access control and key management.
- Department of Homeland Security Control Systems Security Program (CSSP)[26]. To reduce control systems vulnerabilities, the DHS National Cyber Security Division (NCSD) established the Control Systems Security Program (CSSP) and the US-CERT Control Systems Security Center (CSSC). The CSSP coordinates efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors by reducing cyber security vulnerabilities and risk. The US-CERT CSSC coordinates control system incident management, provides timely situational awareness information, and manages control system vulnerability and threat reduction activities.

All these efforts have essentially three goals: (1) create awareness of security issues with control systems, (2) help control systems operators and IT security officers design a security policy, and (3) recommend basic security mechanisms for prevention

---

[24] ISA99: ANSI/ISA-TR99.00.01 - Application and Practices, and ANSI/ISA-TR99.00.02 - Integrating Electronic Security into the Industrial Automation and Control Systems Environment.
[25] http://www.sandia.gov/scada/
[26] http://www.uscert.gov/control_systems/

(authentication, access controls, etc), detection, and response to security breaches. These recommendations and standards have not considered technical details of the new research problems that arise when control systems are under attack.

7.0 Conclusion

The U.S. critical infrastructure is often referred to as a "system of systems" because of the interdependencies that exist between its various industrial sectors as well as interconnections between business partners [Peerenboom,Rinaldi]. Critical infrastructures are highly interconnected and mutually dependent in complex ways, both physically and through a host of information and communications technologies. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

Recent media and press attention has generated a lot of concern over the security of the critical infrastructure, and moreover, the ease and ability of cyberattackers to cause catastrophic failure of important utility services. Given all the documented breaches of security on public and private networks, it is very possible for such intrusions and attacks to also occur on critical control systems, such as SCADA networks, which compose a large part of the critical infrastructure. SCADA systems must be hardened against such attacks, and there are many efforts, as discussed in Section 6, which are currently taking place. However, regarding the likelihood of an intentional attack, by an individual or small group of individuals, it is unlikely such an attack would result in a wide-scale failure of the critical infrastructure.

One reason why may be the sheer complexity of the systems. Though some SCADA computers have weak external security, controlling them takes significant computer engineering and control systems engineering expertise. Taking control of these systems from the outside required a great deal of specialized knowledge and must also overcome non-computerized fail-safe measures. Also because the failure of a control system could result in significant impact or consequence, over-engineering and redundant features are inherent to many of today's SCADA systems.

This is not to dismiss the gravity of the situation. Recall the August 2003 Northeast Power Blackout (as described in Section 3). The initial (unintentional) failure led to an uncontrolled cascading failure of the grid which crashed 508 generating units at 265 power plants. Recall also the Maroochy sewage spill. The adversary was an insider who had just been part of the engineering team who performed the installation of the sewage system. This adversary had physical access as well as intimate knowledge of the facilities. Extrapolating then, it may be possible for a sophisticated cyberattack with insider-level knowledge of the facility to also cause a serious system failure.

.

Bibliography

Alvaro A. Cárdenas, Saurabh Amin, Shankar Sastry, "Research Challenges for the Security of Control Systems", 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium. San Jose, CA, USA. July 2008.

Andersen, R. "Security in open versus closed systems– the dance of Boltzmann, Coase and Moore". In *Open Source Software Economics* (2002).

Byers, E., Leversage, D., Kube, M., "Security Icidents and Trends in SCADA and Process Industries", The Industrial Ethernet Book, Issue 45.

CNN Interactive, "Teen Hacker Faces Federal Charges", March 18, 1988, http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

Dark Reading, "Social Engineering, the USB Way: Those thumb drives can turn external threats into internal ones in two easy steps", DarkReading.com, June 7, 2006.

Eisenhauer, J., Donnelly, P., Ellis, M., and O'Brien, M., Roadmap to Secure Control Systems in the Energy Sector, Energetics Incorporated, Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, January 2006.

Greenberg, Andy, "America's Hackable Backbone", Forbes, August 22, 2007.

Greenberg, Andy, "Hackers' Cut Cities Power", Forbes, January 18, 2008.

Hart, http://www.hartcomm2.org/frontpage/wirelesshart.html, WirelessHart whitepaper (2007).

ISA, http://isa.org/isasp100, Wireless Systems for Automation (2007).

INL, National SCADA Test Bed Program. Idaho National Laboratory, http://www.inl.gov/scada.

Lemos, R., "What are the real risks of cyberterrorism?" ZDNet News, August 26, 2002.

Marburger, J., and Kvamme, E. F. "Leadership under challenge: Information technology R&D in a competitive world. An assessment of the federal networking and information technology R&D program". Tech. rep., President's Council of Advisors on Science and Technology, August 2007.

Meserve, J., "Staged Cyber Attack Reveals Vulnerability in Power Grid". CNN, http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, September 26 2007.

NTSB (National Transportation Safety Board), Pipeline Accident Report: Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999

Owens, W., Dam, K., Lin, H., *(editors),* "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Research Council of the National Academies, 2009.

Quinn-Judge, P., Cracks in the system. TIME Magazine (9th Jan 2002).

Peerenboom, James, "Infrastructure Interdependencies: Overview of Concepts and Terminology", Argonne National Laboratory, http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/proceedings/&toc=comp/proceedings/hicss/2007/2755/00/2755toc.xml&DOI=10.1109/HICSS.2007.78.

Reed, T. At the Abyss: An Insider's History of the Cold War. Presidio Press, March 2004.

Rinaldi, et al., "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, 2001, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf.

Roberts, P. "Zotob, PnP Worms Slam 13 DaimlerChrysler Plants", eweek.com, August 18, 2005,   http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants/

Slay, J., and Miller, M. Lessons learned from the maroochy water breach. In Critical Infrastructure Protection (November 2007), vol. 253/2007, Springer Boston, pp. 73–82.

Stouffer, K., Falco, J., and Kent, K., Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security. Sp800-82, NIST, September 2006.

Tenable Network Security, "Protecting Critical Infrastructure: SCADA Network Security Monitoring", whitepaper, August 1, 2008.

Yu-Lun Huang, Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Hsin-Yi Tsai, Shankar Sastry, "Understanding the Physical and Economic Consequences of Attacks Against Control Systems", International Journal of Critical Infrastructure Protection. Volume 2, Issue 2, Pages 69-134. October 2009.