Research Challenges for the Security of Control Systems

Alvaro A. Cárdenas Saurabh Amin Shankar Sastry
University of California, Berkeley

Abstract

In this paper we attempt to answer two questions: (1) Why should we be interested in the security of control systems? And (2) What are the new and fundamentally different requirements and problems for the security of control systems? We also propose a new mathematical framework to analyze attacks against control systems. Within this framework we formulate specific research problems to (1) *detect* attacks, and (2) *survive* attacks.

1 Introduction

Control systems are computer-based systems that *monitor* and *control* physical processes. These systems represent a wide variety of networked information technology (IT) systems connected to the physical world. Depending on the application, these control systems are also called Process Control Systems (PCS), Supervisory Control and Data Aquisition (SCADA) systems (in industrial control or in the control of the critical infrastructures), or Cyber-Physical Systems (CPS) (to refer to embedded sensor and actuator networks).

Control systems are usually composed of a set of networked agents, consisting of: sensors, actuators, control processing units, and communication devices. Most industrial control systems have a hierarchical structure.

Figure 1 shows a common network architecture: In the first layer the physical infrastructure is instrumented with sensors and actuators. These field devices are connected via a field area network to programmable logic controllers (PLCs) or remote terminal units (RTUs), which in turn implement local control actions (regulatory control). A control network carries real-time data between process controllers and operator workstations. The workstations are used in area supervisory control, planning the physical infrastructure setpoints. The higher level is the site manufacturing operations, which is in charge of production control, optimizing the process, and keeping a process history.

Several control applications can be labeled as *safety-critical*: their failure can cause irreparable harm to the physical system being controlled and to the people who depend on it. SCADA systems, in particular, perform vital functions in national critical infrastructures, such as electric power distribution, oil and natural gas distribution, water and wastewater treatment, and transportation systems. They are also at the core of health-care devices, weapons systems, and transportation management. The disruption of these control systems could have a significant impact on public health, safety and lead to large economic losses.

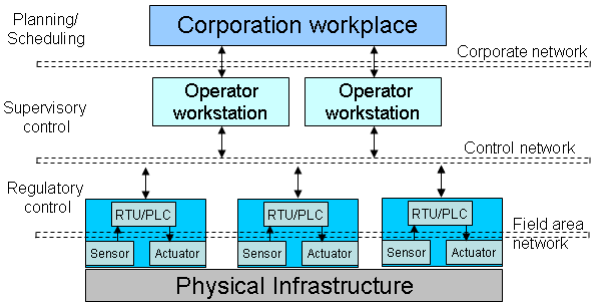

Figure 1. Architecture of control systems.

2 Analysis of the Secure Control Problem

2.1 New Vulnerabilities and New Threats

Control systems have been at the core of critical infrastructures and industrial plants for many decades, and yet, there have been very few confirmed cases of cyberattacks. Control systems, however, are more vulnerable now than before to computer vulnerabilities for many reasons:

Controllers are computers. 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 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 implementation flaws (software bugs).

Networked. Control systems are not only remotely accessible, but increasingly –for 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). Similarly, Internet-connected embedded devices (including CPS) are expected to be the largest contributors to the growth of the Internet in future years [18], and are expected to have

major technical, economic and societal impact. The security challenges of CPS will become more severe as the scale and scope of the Internet grows.

Commodity IT solutions. Although in the past control systems were generally made up of proprietary software and hardware components, today many control systems employ commodity IT systems; such as, off-the-shelf Windows computers, TCP/IP networking etc. Consequently, control systems inherit the vulnerabilities of these components.

Open design. Increasingly, even protocols that are unique to control systems are now more open and more accessible, therefore it is easier for an attacker to obtain the necessary knowledge to attack the system. This point is, however, controversial: security professionals generally argue that open design is preferable because they can find and fix bugs more easily. The debate between open design and closed design is an active one [1].

Increasing size and functionality. Wireless sensor networks and actuators are allowing industrial control systems to instrument and monitor larger number of events and operations. Some infrastructures are also changing to provide new functionalities, such as the Smart Grid program [6]. It is a standard security concern that new functionalities may give rise to new vulnerabilities.

Large and highly skilled IT global workforce. Larger groups of people can now find and generate attack vectors for computer-based systems.

Cybercrime. Less computer-skilled people also have access to a number attack tools and cybercrime networks. A driving factor for the interest of cybercrime in control systems is extortion.

2.2 Vulnerabilities can be Exploited

In the previous section we presented a high-level description of the reason why current control systems are now more vulnerable than before. In this section we discuss some specific events showing that the threat to control systems is real. While there has been some reported indirect attacks to control systems –mostly the side-effects of worms– in this section we concentrate on intentional attacks.

The most well-known computer security incident in SCADA systems is the attack on Maroochy Shire Council's sewage control system in Queensland, Australia [28]. 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. These problems continued for the next four months: pumps were not running when needed, alarms were not being reported, and there was a loss of communications between the control center and the pumping stations. These problems caused the flooding of the grounds of a nearby hotel, a park, and a river with a million liters of sewage. One of the insights in analyzing this attack, is that cyberattacks may be unusually hard to detect (compared to physical attacks). The response to this attack was very slow and the attacker managed to launch 46 reported attacks until he was caught. At the beginning, the sewage system operators thought there was a leak in the pipes. Then they observed that valves were opening without being commanded to do so, but they did not think it was an attack. It was only after months of logging that they discovered that spoofed controllers were activating the valves, and it took even more time to find the culprit: a disgruntled ex-employee of the contractor company that had installed the control system originally and who was trying to convince the water treatment company to hire him to solve the problem.

There have been other recorded attacks to control systems. For example, in 2000 the Interior Ministry of Russia reported that hackers had seized temporary control of the system regulating gas flows in natural gas pipelines (it is not publicly known if there was physical damage) [25]. The former Soviet Union was victim of another attack to their gas pipeline infrastructure in 1982 when a logic bomb caused an explosion in Siberia [26].

There are also several recent attacks. In 2008 a teenager in Poland used a modified TV remote control to control the switch tracks of trams. There were four derailments and twelve resultant injuries [21]. Also, in 2008, a senior analyst for the CIA mentioned that there was evidence of computer intrusions into some European power utilities followed by extortion demands [11]. Attacking SCADA systems for extortion is not new. Physical attacks –for extortion and terrorism– are a reality in some countries [24]. Cyberattacks are a natural progression to physical attacks: they are cheaper, less risky for the attacker, are not constrained by distance, and are easier to replicate and to coordinate.

Besides attacks to deployed systems, there have been numerous studies and experiments showing the vulnerabilities of control systems. On March 2007, researchers at Idaho National Laboratories investigated the results of a possible cyber attack directed against a power network. The "Aurora Generator Test" demonstrated the ability of a cyber attack to damage a power generator turbine [22]. Similarly, most available penetration testing reports show how easy it is to obtain access to computers controlling our physical infrastructures, [10, 12].

Researchers also demonstrated the vulnerability of embedded CPS. In a recent example, Halperin et al. [13] showed radio attacks to implantable cardioverter defibrillators. These attacks could compromise patient safety and privacy.

Also, new security audits are starting to reveal the vulnerability of major critical infrastructures. In a recent security audit, the Tennessee e Valley Authority (TVA), the nation's largest public power company, was found to be vulnerable to cyber attacks that could sabotage their control systems [9].

There is also an increase in awareness on the vulnerability of SCADA protocols. Security venues such as DEFCON, Blackhat, and RSA have recently included SCADA presentations to discuss possible attack vectors. The presentations

have shown implementation vulnerabilities that allow attackers to execute arbitrary code in specific SCADA protocols. This new awareness prompted US-CERT and CERT/CC to start processing and issuing vulnerabilities on SCADA systems beginning 2006.

2.3 Consequences of an Attack

To our knowledge there has not been a publicly-available objective analysis of the possible consequences to attacks against critical infrastructures. In our view, while some of the reports on SCADA security might appear overly alarmist (safety safeguards in most control systems might prevent major catastrophes), the fact that a user is able to obtain unauthorized privileges in a control system should be taken seriously.

The Maroochy Shire incident showed some of the effects that attacks can have. We believe that an important direction for future research is on identifying the risks and consequences of a successful attack.

2.4 Efforts for securing control systems

Up to now, most of the effort for protecting control systems (and in particular SCADA) has focused on *reliability* (the protection of the system against random faults). There is, however, an urgent growing concern for protecting control systems against malicious cyberattacks [2, 7, 8, 31, 32].

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 [23]. 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.

NIST has also published a guideline for security best practices for general IT in Special Publication 800-53. Federal agencies must meet NIST SP800-53. To address the security of control systems, NIST has also published a Guide to Industrial Control System (ICS) Security [29]. Although these recommendations are not enforceable, they can provide guidance for analyzing the security of most utility companies.

ISA (a society of industrial automation and control systems) is developing ISA-SP 99: a security standard to be used in manufacturing and general industrial controls.

The Department of Energy has also led security efforts by establishing the national SCADA test bed program [16] and by developing a 10-year outline for securing control systems in the energy sector [7]. The report –released in January 2006– 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.

The use of wireless sensor networks in SCADA systems is becoming pervasive, and thus we also need to study their security. 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 [14,17]. 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.

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 (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.

2.5 Differences

While it is clear that the security of control systems has become an active area in recent years, we believe that, so far, no one has been able to articulate what is new and fundamentally different in this field from a research point of view compared to traditional IT security.

In this paper we would like to start this discussion by summarizing some previously identified differences and by proposing some new problems.

The property of control systems that is most commonly brought up as a distinction with IT security is that software **patching and frequent updates, are not well suited for control systems**. For example, upgrading a system may require months of advance in planning of how to take the system offline; it is, therefore, economically difficult to justify suspending the operation of an industrial computer on a regular basis to install new security patches. Some security patches may even violate the certification of control systems.

In a recent anecdote, on March 7 of 2008, a nuclear power plant was accidentally shutdown because a computer used to monitor chemical and diagnostic data from the plant's business network rebooted after a software update. When the computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods [20].

Another property of control systems that is commonly mentioned is the real-time requirements of control systems. Control systems are autonomous decision making agents which need to make decisions in real time. While availability is a well studied problem in information security, **real-time**

availability provides a stricter operational environment than most traditional IT systems.

Large industrial control systems also have a large amount of **legacy systems**. Several research efforts have tried to provide lightweight cryptographic mechanisms to ensure data integrity and confidentiality [30,33]. The recent IEEE P1711 standard is designed for providing security in legacy serial links [15]. Having some small level of security is better than having no security at all; however, *we believe that most of the efforts done for legacy systems should be considered as short-term solutions*. For properly securing critical control systems the underlying technology must satisfy some minimum performance requirements to allow the implementation of well tested security mechanisms and standards.

Not all operational differences are more severe in control systems than in traditional IT systems. By comparison to enterprise systems, control systems exhibit comparatively **simpler network dynamics**: Servers change rarely, there is a fixed topology, a stable user population, regular communication patterns, and a limited number of protocols. Therefore, implementing network intrusion detection systems may be easier than in traditional enterprise systems [4].

2.5.1 New Security Problem in Control Systems

While all these differences are important, we believe that the major distinction of control systems with respect to other IT systems is the interaction of the control system with the physical world.

In general, information security has developed mature technologies and design principles (authentication, access control, message integrity, separation of privilege, etc.) that can help us prevent and react to attacks against control systems. However, research in computer security has focused traditionally on the protection of information. Researchers have not considered how attacks affect the *estimation* and *control* algorithms –and ultimately, how attacks affect the physical world.

We argue that while the current tools of information security can give *necessary* mechanisms for the security of control systems, these mechanisms alone are not *sufficient* for the defense-in-depth of control systems.

We believe that by understanding the interactions of the control system with the physical world, we should be able to

1. Better understand the consequences of an attack: so far there is no research on how an adversary would select an strategy once it has obtained unauthorized access to some control network devices.

2. Design novel attack-detection algorithms: by understanding how the physical process should behave based on our control commands and sensor measurements, we can identify if an attacker is tampering with the control or sensor data.

3. Design new attack-resilient algorithms and architectures: if we detect an attack we may be able to change the control commands to increase the resiliency of the system.

3 Linear Systems

The behavior of physical systems can generally be described by a mathematical dynamical system. Linear dynamical systems is one of the most common models for physical systems; they are described by the system of equations:

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k \\ y_k &= Cx_k \end{aligned} \tag{1}$$

where $x_k = (x_{1k}, \ldots, x_{nk}) \in \mathbb{R}^n$ is the state of the system at time k. $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ models the physical dependence of state i on state j, $B = (b_{ij}) \in \mathbb{R}^{n \times}$ is the input matrix for state i from control input j. Furthermore, the controller signal is $u_k = (u_{1k}, \ldots, u_{1m}) \in \mathbb{R}^m$.

In general, it is very difficult to have an accurate model of the process being controlled; therefore, it is common to consider an additional term w_k, which is called the *process noise*, and accounts for modeling errors, uncertainties or perturbations to the system. It is common to assume that $w_k \in \mathbb{R}^n$ is a Gaussian random sequence with covariance Q_0 and mean 0.

The second equation in Eq.(1) assumes the system is monitored by a *sensor network* with p sensors, where $y_k = (y_{1k}, \ldots, y_{pk}) \in \mathbb{R}^p$, and $y_{lk} \in \mathbb{R}$ is the measurement collected by sensor l at time k. Furthermore $C \in \mathbb{R}^{p \times n}$. The reason to include the observation equation is because sometimes we do not have direct measurements of the state of the system x_k.

4 System Requirements and Attack Models

The estimation and control algorithms used in control systems are designed to satisfy certain **operational goals**, such as, closed-loop stability, safety, liveness, or the optimization of a performance function. Intuitively, our **security goal** is to protect these *operational goals* from a malicious party attacking our cyber infrastructure.

In water tank example, we may want to maintain the water levels x in some bounded set (e.g., for all i $x_{min} \leq x_i(t) \leq x_{max}$), even if the system is under attack.

Motivated by our previous work [3], we consider *DoS* and *deception attacks*. In *deception attacks* (a compromise of integrity), the adversary sends false information $\tilde{y} \neq y$ or $\tilde{u} \neq u$ from (one or more) sensors or controllers. The false information can include: an incorrect measurement, the incorrect time when the measurement was observed, or the incorrect sender id. The adversary can launch these attacks by obtaining the *secret key* or by compromising some sensors or controllers.

In *DoS attacks* the adversary prevents the controller from receiving sensor measurements or the actuators from receiving control commands. To launch a DoS the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, flood the network with data etc.

We now present a general framework to model these attacks by using additive changes to Eq.(1):

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k + w_k + \Gamma r_k \\ y_k &= Cx_k + \Psi z_k \end{aligned} \tag{2}$$

For these examples we assume the attack starts at time $k = t_0$. To model this assumption we use the unit step function $1_{\{k \geq t_0\}}$, a function that is *zero* before t_0 and *one* after t_0.

Modeling a DoS attack on a subset $\mathcal{U}$ of control signals.

$$\begin{aligned} \Gamma &= B \\ \forall i \in \mathcal{U}\ r_{i,k} &= -u_{i,k} 1_{\{k \geq t_0\}} \\ \forall j \notin \mathcal{U}\ r_{j,k} &= 0 \end{aligned}$$

Modeling a DoS attack on a subset $\mathcal{Y}$ of sensor nodes

$$\begin{aligned} \Psi &= C \\ \forall i \in \mathcal{Y}\ z_{i,k} &= -x_{i,k} 1_{\{k \geq t_0\}} \\ \forall j \notin \mathcal{Y}\ z_{j,k} &= 0 \end{aligned}$$

Modeling a deception attack on a subset $\mathcal{U}$ of control signals.

$$\begin{aligned} \Gamma &= B \\ \forall i \in \mathcal{U}\ r_{i,k} &= (-u_{i,k} + \alpha_{i,k}) 1_{\{k \geq t_0\}} \\ \forall j \notin \mathcal{U}\ r_{j,k} &= 0 \end{aligned}$$

where α_k is the arbitrary control signal sent by the attacker.

Modeling a deception attack on a subset $\mathcal{Y}$ of sensor nodes

$$\begin{aligned} \Psi &= C \\ \forall i \in \mathcal{Y}\ z_{i,k} &= (-x_{i,k} + \beta_{i,k}) 1_{\{k \geq t_0\}} \\ \forall j \notin \mathcal{Y}\ z_{j,k} &= 0 \end{aligned}$$

where β_k is the arbitrary control signal sent by the attacker.

5 Example 1:Control under DoS Attacks

Adversary Model A (p,q)-Adversary can select p channels (between the sensor and the controller or between the controller and the actuator) and perform a DoS attack for q units of time on all of these channels.

Security Specification While in several control problems we want to design algorithms to optimize certain performance criteria, we believe that when a system is under attack the main objective should be to maintain the *safety* of the physical process. In most cases the safety of the system can be defined as a bounded set such that $x_{min\_i} \leq x_i(t) \leq x_{max\_i}$. Let $\mathcal{P}$ be this safety set.

We want to analyze the behavior of the system from time $k = 0$ to $k = N$. In particular, we want to study the following problem: Does there exist a suitable control sequence u_k such that the performance process $x_0, \ldots, x_N$ lies in a certain safety set with a sufficiently high probability under DoS attacks?

Definition of Security Given a safety parameter set $\mathcal{P}$ and a given ϵ, we say that **the dynamical system** (A, B, C) **is** (p, q, ϵ) **secure** if for every (p,q)-Adversary there is a control sequence $u_k(I_k)$ such that

$$\forall k \in \{0, \ldots, N\} \quad \Pr[x_k \in \mathcal{P}] \geq 1 - \epsilon \tag{3}$$

and where I_k is the information available to the controller at time k.

The feasibility problem Given history I_k we would like to answer two questions: (1) is the system secure? and if it is, (2) how do we find a realization of u_k that maintains the system in the safe set?

6 Example 2: Detection of Attacks

We argue that detecting attacks to control systems can be formulated as anomaly-based intrusion detection systems [5]. The difference in control systems is that instead of creating models of network traffic or software behavior, we use instead the model of the physical system (Eq.(1). Our argument is that if we know how the output of the physical system $Y_1, Y_2, \ldots$ should react to our control commands $U_1, U_2, \ldots$, then any attack to the sensor measurements or control system will exhibit an abnormal view of the physical process (Eq.(2). Given a sequence of observations $Y_1, Y_2, \ldots$ the anomaly detector should also be able to estimate the expected control signals to detect if a controller has been compromised.

The most natural way to detect these attacks is to use sequential detection theory. Unlike previous work [19, 27], we cannot use a fixed model for the attack hypothesis (this is known in statistics as a *simple hypothesis testing problem*) because for deception attacks, we do not know the attack sequences α_k or β_k that an adversary will select. Therefore we need to formulate a *composite hypothesis testing problem*.

We plan to investigate the effectiveness of this approach for detecting a wide range of attacks, and also to analyze the tradeoffs between the accuracy of detection, the number of false alarms, and the damage to the physical system of attacks that can go undetected in our system.

7 Conclusions

We have presented the current status of the field of secure control. We identified some unique properties that these systems have in comparison to traditional IT systems and pro-

posed some new research challenges based on the physical models of the process being controlled. Our research challenges are mostly unsolved and we believe that future research in these areas can provide an additional level of security to control systems.

While we have not presented a model of a real system in this short paper, it is important to emphasize the need for realistic models of physical systems. We are currently experimenting our research directions with three systems: a water canal system, a water distribution network, and a chemical reactor plant. Only by experimenting and simulating realistic infrastructures will our theoretical methods be validated.

8 Acknowledgments

This work was supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244) Cisco, British Telecom, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies.

References

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

[2] BYRES, E., AND LOWE, J. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies* (October 2004).

[3] CARDENAS, A. A., AMIN, S., AND SASTRY, S. Secure control: Towards survivable cyber-physical systems. In *Proceedings of the First International Workshop on Cyber-Physical Systems.* (June 2008).

[4] CHEUNG, S., DUTERTRE, B., FONG, M., LINDQVIST, U., SKINNER, K., AND VALDES, A. Using model-based intrusion detection for SCADA networks. In *Proceedings of the SCADA Security Scientific Symposium* (Miami Beach, FL, USA, 2007 2007).

[5] DENNING, D. An intrusion-detection model. *Software Engineering, IEEE Transactions on SE-13*, 2 (Feb. 1987), 222–232.

[6] DOE. *Smart Grid.* Department of Energy, http://www.oe.energy.gov/smartgrid.htm, Accessed July 14 2008.

[7] 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.

[8] GAO. Critical infrastructure protection. Multiple efforts to secure control systems are under way, but challenges remain. Tech. Rep. GAO-07-1036, Report to Congressional Requesters, September 2007.

[9] GAO. Information security. TVA needs to address weaknesses in control systems and networks. Tech. Rep. GAO-08-526, Report to Congressional Requesters, May 2008.

[10] GREENBERG, A. *America's Hackable Backbone*. Forbes, http://www.forbes.com/logistics/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html, August 2007.

[11] GREENBERG, A. Hackers cut cities' power. In *Forbes* (Jaunuary 2008).

[12] GREENE, T. *Experts hack power grid in no time*. Networkworld, http://www.networkworld.com/news/2008/040908-rsa-hack-power-grid.html, May 9 2008.

[13] HALPERIN, D., HEYDT-BENJAMIN, T. S., RANSFORD, B., CLARK, S. S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., AND MAISEL, W. H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy* (2008).

[14] HART. http://www.hartcomm2.org/frontpage/wirelesshart.html. *WirelessHart whitepaper* (2007).

[15] HURD, S., SMITH, R., AND LEISCHNER, G. Tutorial: Security in electric utility control systems. In *61st Annual Conference for Protective Relay Engineers* (April 2008), pp. 304–309.

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

[17] ISA. http://isa.org/isasp100. *Wireless Systems for Automation* (2007).

[18] JOHN H. MARBURGER, I., 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.

[19] JUNG, J., PAXSON, V., BERGER, A., AND BALAKRISHNAN, H. Fast portscan detection using sequential hypothesis testing. *Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on* (May 2004), 211–225.

[20] KREBS, B. *Cyber Incident Blamed for Nuclear Power Plant Shutdown*. Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html, June 2008.

[21] LEYDEN, J. Polish teen derails tram after hacking train network. *The Register* (11th Jan 2008).

[22] MESERVE, J. *Sources: 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.

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

[24] NEWS, B. *Colombia Rebels Blast Power Pylons*. BBC, http://news.bbc.co.uk/2/hi/americas/607782.stm, January 2000.

[25] QUINN-JUDGE, P. Cracks in the system. *TIME Magazine* (9th Jan 2002).

[26] REED, T. *At the Abyss: An Insider's History of the Cold War*. Presidio Press, March 2004.

[27] SCHECHTER, S., JUNG, J., AND BERGER, A. Fast detection of scanning worm infections. In *Recent Advances in Intrusion Detection* (October 2004), pp. 59–81.

[28] 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.

[29] 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.

[30] TSANG, P. P., AND SMITH, S. W. YASIR: A low-latency high-integrity security retrofit for lecacy SCADA systems. In *23rd International Information Security Conference (IFIC SEC)* (2008).

[31] TURK, R. J. Cyber incidents involving control systems. Tech. Rep. INL/EXT-05-00671, Idao National Laboratory, October 2005.

[32] US-CERT. *Control Systems Security Program*. US Department of Homeland Security, http://www.us-cert.gov/control_systems/index.html, 2008.

[33] WRIGHT, A. K., KINAST, J. A., AND MCCARTY, J. Low-latency cryptographic protection for SCADA communications. In *Applied Cryptography and Network Security (ACNS)* (2004), pp. 263–277.