WorleyParsons
resources & energy

Industrial Cyber Security

From the Perspective of the Power Sector

Revision 1

July 28th 2010

Authored by:
Wade Polk
Paul Malkewicz
Jaroslav Novak

"The further the spiritual evolution of mankind advances, the more certain it seems to me that the path to genuine religiosity does not lie through the fear of life, and the fear of death, and blind faith, but through striving after rational knowledge."

-Albert Einstein

Abstract

Industrial control systems are flexible constructs that result in increased efficiency and profitability, but this comes at the cost of vulnerability. In past years, industrial cyber security has been mostly ignored due to cost, lack of understanding, and a low incidence rate. More and more these systems rely on commercial, off the shelf software which increases the ease and likelihood of an attack. Today, we face growing threats from individuals, foreign governments and competing companies. The risks have increased by orders of magnitude.

This paper will provide an overview of control components common to the power industry, common vulnerabilities, and the current situation with industry's cyber infrastructure as well as worst case scenarios. This paper provides a short overview of standards and governances followed by recommendations to facilitate achieving compliance with overlapping governances.

Preface

Over the course of the last forty years, modern industrial plants have come to rely more and more on complex networking and computing to automate and monitor processes within the plant. This reliance on automated control has brought with it exponential increases in efficiency, quality of product, safety, as well as many other advantages. Unfortunately, it also brings with it vulnerabilities which can be exploited, either intentionally or unintentionally. This can lead to loss of revenue, damage to equipment, injury, or even fatalities. With this in mind, modern plant control systems must be designed with security as a primary goal.

As with any other type of technology, industrial controls technology is constantly changing and evolving. New vulnerabilities are discovered at a rate which software and hardware developers cannot keep up. Therefore the objective of a good security plan is not to anticipate every possible type of attack, but instead to make systems more difficult to compromise, particularly at the point of entry. A high-quality defense-in-depth strategy will minimize the amount of damage any successful attack is able to do.

The aim of this paper will be to examine the current state of industrial automation defense. It will look at current common vulnerabilities and real cases of intrusion into the control networks of operating plants. It will then examine the various existing standards and requirements for security of a power plant. Using these as a basis, an efficient method to implement a security plan which will comply with each of these overlapping standards while executing an effective security strategy will be proposed.

Although this paper will focus mainly on the power industry, the same methods are valid for nearly any type of large industrial plant. Most of the components are identical in function and design.

1. Introduction to Process Networks and Industrial Cyber Security

1.1. Typical Control Hierarchy

A control system is typically described by levels of control, with the lowest levels corresponding to the most basic levels of control. Understanding this design method is important because often times the Electronic Security Perimeters (ESPs) will mirror the division of these levels; ESPs are discussed in section 4.4.2.1. Because each level of control in a plant has a different level of criticality to the overall operation of the plant, as well as different vulnerabilities to the various types of cyber attacks, varying types and levels of security will apply. Because of this, it is important for the security plan to control how and if one level of control is able to communicate with another level of control.

A typical industrial plant will have several discrete levels in its control system. There exist several standard methods for describing each level. The one used here is the one proposed in ISA standard 88.01 section 4.2.

The lowest level of control is the Control Module Level. This level describes basic input and output (I/O) devices such as sensors (e.g. pressure, flow rate, temperature, turbidity, etc.) and control devices (e.g. valves, motors, solenoids, burner controls, etc.) fundamental to the power generation process in the field. The amount of intelligence is typically very limited at this level, though some new smart devices are changing this trend.

Above the Control Module Level is the Equipment Module Level which performs basic monitoring and control functions with input from and feedback to the Control Module Level equipment. The equipment at this level can detect and respond to emergencies within its area of control, usually by monitoring for conditions outside of the normal ranges of operation. A programmable logic controller (PLC) or distributed control system (DCS) is usually found at this level. Occasionally, a single loop controller (SLC) can be found within this level.

Supervisory control and coordination functions between the various Equipment Module Level hardware is performed by the Unit Level. The Unit Level is usually made up of modules that together perform a specific task within the overall process. Supervisory control and data acquisition (SCADA) systems are often found at this level, though more and more the distinction between a DCS and a SCADA system has become blurred and they are used nearly interchangeably.

The top level which spans the entire process is called the Process Cell Level which is comprised of all the Unit Level hardware. The Process Cell Level is particularly important in the coordination of an emergency, including one potentially caused by a hostile attack, as it would coordinate the emergency action plan of all the levels below it.

The remaining 3 levels, Area Level, Site Level and Enterprise Level, are part of the business network, which is split by organizational requirements. A Demilitarized Zone

separating these levels from the plant control levels is perhaps one of the most important security precautions as usage and security within these levels is more relaxed then it is within the lower levels of control[1].

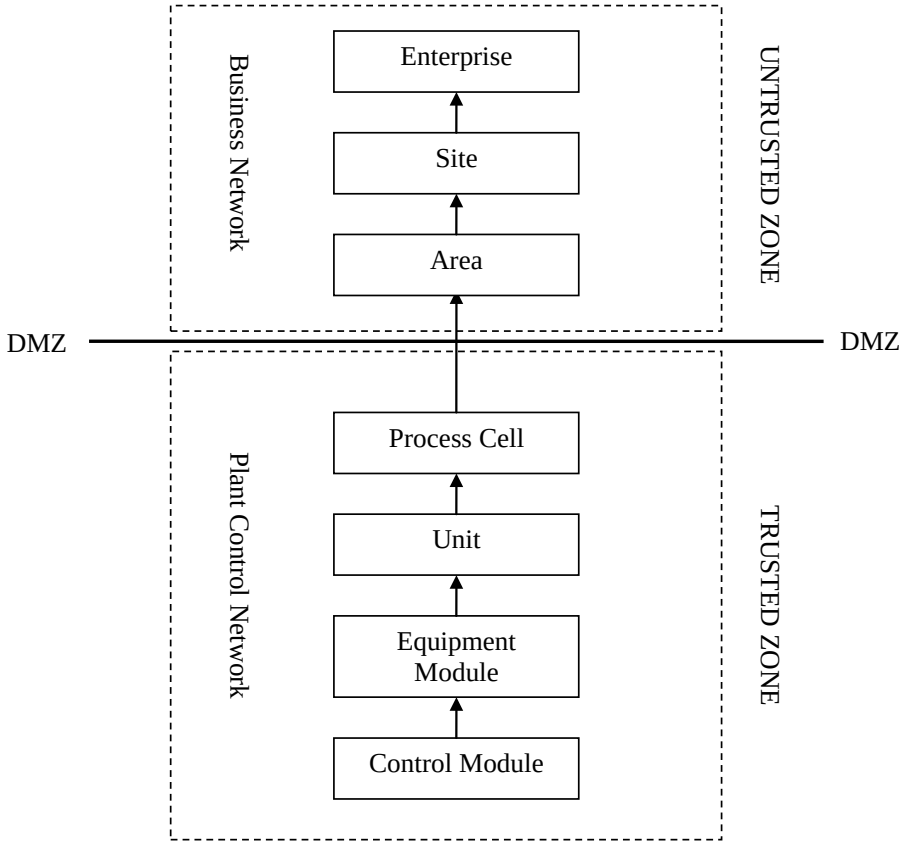


Figure 1: Plant Control Architecture as described by ISA standard 88.01 Note that all levels are not required for every implementation.

1.2. Common Internal Connections

With a basic understanding of the control hierarchy of an industrial plant, the complexity of communication between hardware at each level is apparent. Communication at the lowest levels consists of field devices providing information in the form of a simple analog or digital signal to a controller. From the device end this is accomplished with either a digital signal, like in the case of a switch, or an analog signal which provides a continuous measurement, such as pressure or temperature. More complex methods of communication also exist at this level and are becoming very common in a plant setting. Protocols like Profibus and Foundation Fieldbus allow additional information to be transmitted on the same medium. This will be discussed in more detail at a later time.

[1] ANSI/ISA. NSI/ISA-88.01-1995, Batch Control, Part 1: Models and Terminology. Research Triangle Park, North Carolina: The Instrumentation, Systems and Automation Society, 1995.

The controller end of the lowest level usually consists of a PLC or DCS. PLCs use ladder or Boolean logic to produce control outputs based on inputs received from the field. DCSs use computers combined with graphics to interpret inputs in a more flexible way than PLCs and can perform several functions in parallel.[2]

Because all connections at this level are internal, security measures should focus on internal threats as well as segmentation. Access to the control system should be limited and monitored. Equipment should be enclosed and physically secured where appropriate. A true defense-in-depth approach should also protect the lower levels from failures that occur at levels higher levels. This is accomplished through the use of firewalls, data diodes, and other devices which control and restrict the flow of information between hardware, as discussed in section 4.4.2.3, Protection of cyber devices

1.3. Common External Connections

At higher levels of the control architecture, connections to external networks typically become more common. Most of these connections are intended, at least in an ideal world, and usually required for plant operation. Unintended connections, like unsecured wireless connections must be avoided at all costs. Wireless communication in an industrial setting should be avoided in general, and only implemented when other options are not practical and only on non-critical systems. Extra precautions should be implemented on wireless devices including data protections like complex encryption and hard authentication; multi-band frequency hopping should be used for transmission security and hardware protections, of course, are required. Consider adjusting radio power and using directional antennas.

Intentional external connections are often connections to plant business networks, grid networks or, on rare and dangerous occasions un-trusted zones like an enterprise networks or even the web. These external connections typically allow information on plant operation and output to be sent outside of the plant control system for production analysis, scheduling, maintenance, load determination and other purposes. Often, external connections go to networks that are used by personnel untrained in recognizing potential security dangers. Because of the intended use of networks such as the business network, and the fact that it is not considered a critical application from a generation standpoint, the level of security is much lower and the incidence of exposure to external networks and the internet is much higher. A combination of these factors makes this network a likely and often easy target for a cyber attack, and navigation to plant networks may be easier than expected. Care must be taken to secure the connection between these two networks to ensure data only flows as intended, in the direction intended. Methods for doing this will be discussed in detail in section 4.4.2.2 Protection of ESP Access Points. Care must also be taken to ensure that data only flows through the intended connection points from one network to the other. A fortuitous connection could easily allow unhindered access to the plants control system. For this reason, connections between the two networks should be limited to as few segments as possible, and those segments should be carefully monitored.

[2] Liptak, Bela G. Instrument Engineers Handbook: Process Control and Optimization. Boca Raton, FL : CRC Press, 2006.

Because the lifespan of an industrial plant can span upwards of forty years or longer, hardware and software must be kept up to date as technology evolves. Additionally, as parts of a plant are upgraded or as new sections are added, it is important that the change management process is followed carefully so that additional connections can be tracked and monitored.

1.4. Protocols

Many communications protocols exist in a modern industrial plant. Currently, there is no general agreement on a standard of communication, and as a result several competing standards perform nearly the same function. It is a matter of preference which communication philosophy is chosen. Many protocols have versions of the protocol appropriate for both the device level of control as well as communication at higher levels of the control architecture; hardware and software considerations are usually included during the design of these versions. Examples of this include Serial MODBUS at the device level and MODBUS TCP at the controller level, PROFIBUS PA at the device level and PROFIBUS DP at the controller level. Foundation Fieldbus, a very common protocol, is an open Fieldbus standard which also comes in two levels, H1 for device level communication and HSE for communication between controllers.

There are several other common protocols worth mentioning here. HART protocol allows analog devices to transmit additional information over the common 4-20 mA analog instrument signal by shifting the frequency of the signal; this allows instrumentation to continue operating while a user communicates with the device. Devicenet is another communication protocol at the device level which allows several devices to be daisy-chained together brought back to the controller on one pair of wires.[3]

Another standard worth mentioning here is the OLE for Process Control (OPC) data access standard. OPC is an open standard governing the communication of data between a device in the field and control equipment. This allowed devices which supported the OPC standard to communicate with any type of control equipment which also supported this standard with no additional interface required.

When choosing a protocol for plant communication, one must keep in mind that all devices and controllers must be compatible with that protocol to minimize cost and confusion. Because this is not always practical, bridges and converters exist to allow more than one protocol to be used within a discrete network. When deciding what level of the control hierarchy to protect and to what degree, protocols are often use as the deciding factor.

[3] Liptak, Bela G. Instrument Engineers Handbook: Process Control and Optimization. Boca Raton, FL : CRC Press, 2006.

2. Hazards and Risks to Operability

2.1. Industrial Cyber Security Incidents

The realities of the current situation with the industrial security infrastructure are bleak. In general, control system design has not kept pace with the rest of the IT industry in terms of security and the result is the state of affairs currently faced by Control System Engineers. Part of the problem is owed to the fact that, although many plants are designed to last 40 years, the life span of many industrial plants can far exceed forty years. At their time of design, cyber attacks were a non-existent threat and safeguards were not built into the design of the control system. Without a well established and documented security plan, including policies for change management, these aging control systems are often modified with new undocumented and insecure ad-hoc connections which can compromise the overall security of the plant. This situation, combined with a dramatic increase in attacks driven by monetary and political motivators leaves all sectors of national infrastructure including water, power, and manufacturing vulnerable to devastating attacks.

To understand the urgency of this situation, one needs to look no further then President Obama's Commission on Cyber Security which is quoted as saying "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[4] This realization of the current state of affairs led to an early 2009 review of the current state of affairs and efforts to shore up the nations vital networks. The review highlighted a 10 item near-term action plan which included appointing a governmental policy official tasked with coordinating national cyber security efforts, a position later dubbed the "cyber czar". Other items on the action plan included making cyber security a national priority with measurable performance metrics to track progress and creating a nation-wide cyber security awareness campaign.[5]

For fairly obvious reasons, publicly available detailed reports of industrial cyber security incidents are not common. In 2009 the United States government confirmed that the US power infrastructure is vulnerable to cyber attacks.[6] Sources report that there had been many intrusions into different plants across the country, sometimes leaving behind software which could be used to take over or disable the system at a later time. Another CIA official reported that there have been multiple cases of cyber attacks on power plants outside the US in some cases followed by extortion demands.[6]

One such case of a targeted intrusion occurred in 2001 at a California utility responsible for electric transmission. The invasion went undetected for nearly 20 days as attackers gained access to a portion of the utility's system that was under development through an

[4] Center for Strategic and International Studies. Securing Cyberspace for the 44th Presidency. Washington: GPO, 2008.
[5,6] The White House. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington: GPO, 2009.
[6] G`orman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." Wall Street Journal April 8 (2009): http://online.wsj.com/article/SB123914805204099085.html.

un-firewalled connection. Additionally, unused ports were left open leaving the network vulnerable. Thankfully, no damage was done to the system and power service was not affected. Reports indicate that the attacker was attempting to penetrate further into the network for access to more critical controls when the intrusion was discovered.[7]

Targeted attacks on plant control systems are not the only threat faced by these networks. Because parts of many common plant control systems rely on off the shelf operating platforms, they are also vulnerable to mass malware programs as well. This was the case in 2003 when the Slammer worm brought down part of the safety monitoring system at the then offline Davis-Besse nuclear plant in Ohio. The increased traffic from the worm caused denial of services to parts of the plant safety and monitoring networks which became inaccessible to other parts of the network. The worm entered the plant's control network through an unsecured contractor connection to the contractor's business network which bypassed normal firewalls.[8] The Repository of Industrial Security Incidents (RISI) released a report in March of 2010 indicating that nearly 50% of all reported cyber security incidents were caused by viruses, worms and Trojans.[9]

In addition to defending against intentional malicious attacks, the security design of a control system must also be prepared to deal with unintentional disgruntled employees and security incidents caused by untrained users and faulty software. Although unintentional, this type of incident can be just as dangerous, if not more so then an intentional attack because it will often originate from inside the control network from a trusted source. This was the case when in 1999 a petroleum pipeline in Washington exploded and led to the deaths of three people. The cause of this incident, which many recognized to be the first cyber incident which led directly to a fatality, was ruled to have been caused by a combination of factors. One of the primary causes however, was a failure in the control system which prohibited the operator from relieving pressure on the pipe to prevent the explosion. An additional finding during the investigation of the incident was that adherence to NIST standard 800-53, one of the standards referenced later in this document, could have prevented the incident from ever occurring.[10]

2.2. Possible Outcomes of an Attack

The effects of a successful attack on an industrial control system can vary greatly depending on what the system is controlling. A general control philosophy for protecting critical or potentially dangerous processes is to put a system of interlocks into place. An interlock is either a piece of hardware, or logic built into software to prevent equipment from

[7] Mojain, Dan. "Hackers Victimize Cal-ISO." Los Angeles Times. 9 Jan. 2001: http://articles.latimes.com/2001/jun/09/news/mn-8294.
[8] Nuclear Regulatory Commission, United States. "NRC Issues Information Notice On Potential Of Nuclear Power Plant Network To Worm Infection." Office of Public Affairs. 2 Sep. 2003: http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html.
[9] "RISI. 2009 Report on Control System Cyber Security Incidence Released. 30 Mar. 2010. Repository of Industrial Security Incidents (RISI). http://www.securityincidents.org/members/news.asp?ID=13.
[10] Singel, Ryan. "Industrial Control Systems Killed Once and Will Again, Experts Warn.." Wired. 9 Apr. 2008: http://www.wired.com/threatlevel/2008/04/industrial-cont/.

operating in a way that it could damage itself or create a dangerous situation. An example of an interlock is the device in a seatbelt that prevents the belt from extending when the break is applied with a certain force. In many cases, the worst case outcome of an attack is whatever occurs when one of these interlocks is broken. In the best case scenario, after an attack has been detected it will be cleaned up, investigated, and the vulnerability will be closed.

In some scenarios an incident could lead to expensive and potentially dangerous equipment failures. Because of the presence of large quantities of energy rich fuels and complex equipment and controls, many potentially dangerous scenarios exist. Often these scenarios are documented within the logic of a control system and can be discovered simply by deciphering the conditions that the logic tries to prevent. An example is the algorithms that control the mixture of Oxygen and fuel in a boiler. These controls are designed to manage the firing rate of a boiler, however if they were tampered with, it is possible that the mixture could become fuel rich. If there was an influx of oxygen at that point, a large explosion could result. In a well designed system, hardwired interlocks should prevent this from happening; however these could be functioning incorrectly or be disabled entirely.

Another possible scenario involving a boiler would be to disable the Forced Draft (FD) fan, a fan which blows air into a boiler, while leaving the Induced Draft (ID) fan, a fan that sucks air out of a boiler, running at full. Boilers are designed for normal operation at around neutral pressure. The fans balance the pressure keeping the boiler at this neutral operating pressure. However, if the balance is disturbed, the pressure produced by the fans is enough to collapse the walls of a large boiler causing an implosion.

Other portions of the plant contain similar weaknesses. A steam turbine, for example uses pressurized superheated steam to rotate the blades of a turbine to produce mechanical energy. A valve and spray nozzle up stream of the turbine sprays water into the steam to control the temperature. If this valve was allowed to open fully and spray enough water to saturate the steam, droplets of water would blast the blades of the turbine. This could warp or crack a turbine blade, a costly repair which could cause months of down time.

Damage to plant equipment and injury or loss of life in areas near the incident are not the only possible outcome of tampering with a control system. Many modern plants use a process called Selective Catalytic Reduction (SCR) to decrease pollutants in plant emissions by injecting them with Ammonia. Because the process requires a large amount of ammonia, many plants store massive quantities of anhydrous ammonia on site. If a weakness was found in the controls that allowed an attack to vent this gas to the atmosphere it could pose a serious public health risk to a large area around the plant.

In 2007 a leaked government video showing a government demonstration known as the “Aurora Generator Test” which displayed the affects of an exploited vulnerability in a

control system leading to the violent destruction of a turbine generator.[11] The video, which is light on details of the vulnerability, is a graphic demonstration of the type of damage that can be done when the control network has been compromised by an entity with malicious intent.

The feasibility of attacks on these major pieces of equipment is very much dependant on the design of the control system. Often critical equipment will have redundant interlocks, one set independent of the control network to prevent damage in the case of a control system failure. Examples of this include pressure safety valves, set to open automatically and relieve excess pressure when conditions reach a certain point. This device operates without a signal from the control system. Careful planning and redundancy required on some of the most dangerous equipment, like a nuclear reactor make the very worst scenarios unlikely or nearly impossible.

Aside from being immediately dangerous to plant personnel, high risk equipment failures like these can take months or years to repair and cost millions of dollars to rebuild. In addition to the direct cost to repair the equipment, the power outages caused by this can also have a devastating economic impact to the entire region. The 2003 power outage in the Northeastern United States, which was ruled not to be the result of a cyber attack, caused a loss of power for more than 50 million people, is estimated to have cost nearly $6 billion and lead to at least eleven fatalities.[12] A similar result is a feasible result of a well planned malicious attack plan.

Another concern is that of a cyber attack being used on US infrastructure as part of a larger military offensive. Attacks like the ones mentioned above could be used to disable vital parts of US Infrastructure leaving the US vulnerable in a time of war.

[11] Bridis, Ted. "Government video shows mock hacker attack." MSNBC. 26 Sep. 2007: http://www.msnbc.msn.com/id/21000386/%3E..
[12] Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American. 13 Aug. 2008: http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

3. Governances and Standards

3.1. NERC

Cyber security in an industrial power plant, excluding nuclear, is largely governed by a set of Critical Infrastructure Protection (CIP) standards created by the North American Electric Reliability Corporation (NERC). A facility can be fined up to **$1,000,000 per day per violation**[13] for failing to meet the requirements of these standards. There are eight NERC standards which highlight the primary methods and goals of a cyber security framework; CIP-001 contains reporting requirements.

- CIP-002 Critical Asset Identification – Identifying which assets should be protected and the varying levels of risk associated with each asset.
- CIP-003 Security Management Controls – Defines system users and sets up responsibilities and access controls based on need.
- CIP-004 Personnel & Training – Further defines access controls and responsibilities of users and sets minimum training standards for awareness of security policies.
- CIP-005 Electronic Security Perimeters – Creates the idea of security perimeters around critical cyber assets. This standard also controls how items inside the perimeter are accessed.
- CIP-006 Physical Security of Critical Cyber Assets – Defines guidelines for a physical security plan for critical cyber assets and physical security perimeters.
- CIP-007 Systems Security Management – Defines processes for protecting assets within an electronic security perimeter.
- CIP-008 Incident Reporting and Response Planning – Sets up requirements for an emergency response plan and defines requirements for the reporting of incidents.
- CIP-009 Recovery Plans for Critical Cyber Assets – Sets requirements for recovery plans, backups, and planed incident drills.

3.2. NIST

In addition to NERC requirements, the Federal Information Security Management Act (FIMSA) created a set of standards managed by the National Institute of Standards and Technology (NIST) which apply to federal agencies serving a nearly identical purpose to the NERC CIPs, though somewhat more in-depth and **without financial penalties**. While adherence to these standards is not directly required for non-governmental organizations, and much of the content overlaps the NERC standards, the NIST guidelines are worth consideration.

- FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems – Similar in content to CIP-002, used to category critical assets and levels of risk for each asset, typically intended for informational assets.

[13] Ziegler, Kelly. "Blackout's 5th Anniversary Marks Progress, New Challenges Ahead ." North American Electric Reliability Corporation (NERC). 14 Aug. 2008: http://www.nerc.com/news_pr.php?npr=142.

- FIPS Publication 200 Minimum Security Requirements for Federal Information Technology Systems – Defines processes for protecting assets within an electronic security perimeter.
- Special Publication 800-30 Risk Management Guide for Information Technology Systems – Framework for identifying and managing risks.
- Special Publication 800-37 Guide for Security Authorization of Federal Information Systems: A Security Lifecycle Approach – Guideline to apply risk management framework to a computer network.
- Special Publication 800-40 Creating a Patch and Vulnerability Management System – Guidelines for security reviews and remediation.
- Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations – Further defines processes for protecting assets within an electronic security perimeter. Provides detailed descriptions about the processes and methods described in FIPS 200.
- Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems – Criteria to evaluate security in a control system.
- Special Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories – Further detail on defining critical assets and levels of risk. Contains more detail then FIPS 199.
- Special Publication 800-82 Guide to Industrial Control System Security – Guidelines for securing an industrial control system from cyber threats.
- And many others ranging from cell phone use to printer security requirements, but the above should be of the most use.

3.3. NRC

Finally, nuclear plants are exempt from compliance with NERC standards. Instead nuclear plants are mandated by NRC Title 10 Code of Federal Regulations Section 73.54 which require a plant's "computer and communications systems be adequately protected against cyber attacks". Because of the vagueness of this requirement the NRC released regulatory guide 5.71, Cyber Security Programs for Nuclear Facilities. This guide is based heavily on the principals in NIST publications 800-53 and 800-82.

4. Exceeding Compliance with Overlapping Standards

4.1. Purpose

Compliance is often a very difficult thing to achieve in general; to compound this, cyber security compliance for industry is relatively new, and most people who know anything about their particular site, no little about cyber security. Conversely, those who know the details of cyber security (usually IT/CS professionals), often know little or nothing about industrial processes. This presents a significant challenge. It is not as simple as contracting a group of IT professionals and security experts to come in and secure a network, it is much more complicated because IT professionals aren't usually trained for industrial environments. To compound the situation further, some sites are required to deal with multiple overlapping and possibly conflicting standards on the same subjects. For all the above reasons, it is far better to set a goal of exceeding compliance rather than meeting compliance; this is the only real approach to guarantee compliance.

4.2. Scope

This section will attempt to provide the reader with a comprehensive security plan and techniques that can be used and tailored to a site, to help exceed compliance with multiple overlapping governances. It is written with the understanding that exceeding compliance by automation and meticulous design will save on overhead in the near and long terms in comparison to simply meeting compliance with manual labor intensive methods.

4.3. Management Policies, Procedures & List

All compliance activities will require documentation and records as well as evidence or proof. It is important to understand the distinction between documentation and records and evidence and how each plays its role in compliance and security. To give a few examples, documentation and records may refer to drawings, configuration data, backup drive images, etc. while evidence may refer to things like sign-off sheets for drawings, original configuration scanner raw output, and backup image validation and verification. To put it another way, documentation and records are required for operational, maintenance and design purposes while evidence is required for internal and external audits. This section will provide a recommended set of compliance procedures and details of what needs to be included in each. Details of what documentation and record requirements are recommended as well as methods to maintain an audit trail will also be given.

4.3.1. Master Lists

There are three master lists usually required for compliance and always recommend by good policy. These lists should be hierarchical in nature, the highest level providing information about sites, the next about systems and the last providing basic data about devices. These lists will be used later for classification activities.

4.3.1.1. Sites and Systems

If the organization consists of multiple satellite entities such as a major power producer with multiple plants, the first master list should identify basic information about each site. If the organization consists of only a single site, the first master list should provide basic data about each system since a sites list would be fairly pointless and of no use. Fields contained in these lists should include the following at a minimum, additional fields can be added by the organization, but it is not recommended that any of the fields be removed:

Sites List

- Site Name
- Location
- Address
- Type - e.g. coal, nuclear, etc
- Peak load output
- Responsible Organizations and contact information
- Classification – discussed later

The sites list should include control centers, backup control centers, auxiliary control centers, large transmission substations, facilities critical to system restoration, automatic load shedding, special protection systems and finally generating facilities.

Systems List

- Site
- System Name
- Description
- Responsible Party
- Classification – discussed later

The systems lists should be comprehensive for a given site and will generally be site specific. Systems lists are usually defined during plant construction and are not difficult to obtain. For the purposes of cyber security compliance, the systems list may require some modification. For examples of the two lists described above Refer to section 7 Appendix A: Examples. Additional lists such as I/O lists and bill-of-materials (BOM) will also be useful.

4.3.1.2. Cyber Devices

A decision will need to be made regarding what level of device to include on this list. A related decision will need to be made regarding how each site defines a cyber device. For example, one would not want the list to include end devices like instrument transmitters. Of course, all end devices must be captured on documentation somewhere such as connection diagrams and I/O lists, but these devices are not easily protected from cyber attack and it is assumed that far worse holes exist; the time may come when instrument manufacturers include added security measures.

The following is a recommendation for defining the term Cyber Device: A programmable electronic device whose primary programming interface is **not** implemented using a local non electronic method such as a keypad. The latter exclusion is intended to eliminate from compliance requirements, those devices which an attacker could not easily access, program and control from a remote location. Non-remotely accessible devices should be installed in locations of higher order devices to provide added physical protection by inclusion, whenever possible. Fields contained in this list should include the following at a minimum, additional fields can be added by the organization, but it's not recommended that any of the fields be removed:

- Characteristic Identifier/Tag
- Unit
- Type – e.g. PLC, DCS, PC, etc.
- Manufacturer
- Model
- Operating system
- Number of Ethernet ports
- IP address and host name
- Equipment description
- Approximate location
- Physical security – Yes/No
- Physical security type – Camera, lock, etc.
- Protocols
- Protocol type – routable or non-routable
- Site
- System
- Classification – discussed later

The device list should include PLC, DCS, Serial or Network Recorders, Computers and Servers, KVM switches, media converters, external drives, controllers, thin clients, network switches, routers, hubs, any device with an Ethernet connection and any other device the site feels should be included.

4.3.2. Master Drawing

One series of network drawings must be developed and maintained using highly confidential methods. It must include every connection using routable and digital protocol to every cyber device; however the site chooses to define the term cyber device. Refer to Section 7. Appendix A: Examples. Connections usually included are Ethernet, serial, fiber, USB, proprietary protocols, wireless, printer and others. Devices usually include PLCs, a DCS, process recorders, computers, servers, media converters, external storage, controllers, thin clients, Keyboard Video Mouse (KVM) switches, Ethernet switches, routers, hubs and any device which has an Ethernet connection. Of course, symbology, line types, borders, etc must be defined prior to embarking on this development.

4.3.3. Procedure 1: Policies

This procedure should be considered the master document, identifying associated procedures and requirements that are common to all cyber security procedures. This master document should include:

- An overview of scope, approach and commitment to cyber security
- Cyber security team including roles, responsibilities and contact data
- Accountability of employees statement
- References: governing standards, guidance
- Issuance and update policies for procedures
- Processes for initiating, documenting and closing exceptions to policies: *documented exceptions should always require compensating measures to mitigate any added risk*
- Exception review policies: exceptions, conditions for exceptions and the exceptions process
- Identification, Classification and Categorization policies and processes
- Personnel security training requirements, processes and policies
- Introductions/overview of associated procedures
- Periodic reviews of all policies

Applying contiguous security management controls across an organization proves to be more cost effective in the near and long terms than attempting to apply two or more sets of controls to sub entities.

4.3.4. Procedure 2: Information Protection

It is essential that only individuals with a need to know are allowed to view sensitive information, regardless of the media type. This procedure should provide the process to ensure this happens.

4.3.4.1. Information management controls- How to deal with large quantities of information, most of which may be considered sensitive information.

- Policies, process and reporting requirements for information loss or theft
- Data retention requirements: *everything should be kept, electronically, indefinitely and well organized*
- Policies for determining the sensitive nature of information and subsequent controls through assessments
- Individuals responsible for access authorization.

4.3.4.2. Information access controls - How to access sensitive information and maintain an accurate record of information owners and what they own.

- User management policies: *Information access control list and policies for adding, removing and modifying users/user rights*
- Authorization process for access rights
- Personnel risk assessments/background checks

4.3.4.3. Sensitive/Top Secret Information - Whatever policies an organization has in place regarding classifying information, sensitive/top secret information should include the following at a minimum.

- Operational procedures and lists
- Network topology and similar, floor plans of computing centers, equipment layouts
- Disaster recovery/incident response plans
- Security configuration information

Information must be protected from start to finish, from initial plant design to plant shutdown and abandonment. Once information about the network is leaked, the only effective mitigation is to redesign the network or perhaps augment certain security controls.

4.3.5. Procedure 3: Physical Security Plan

This procedure should define the physical access controls, monitoring and user management policies of the organization; it defines requirements for the first and last lines of defense against local cyber attacks and local brute force physical destruction of systems.

4.3.5.1. Physical Security Perimeters (PSPs) - segmenting and layering physical security and identification of physical access points.

- PSP design requirements: *a layered approach is highly recommended by making use of primary, secondary and tertiary ESPs.*

- Requirements for protection of physical access points to PSPs: *two factor authentication at each PSP access point, whether primary, secondary or tertiary, is recommended.*

4.3.5.2. Physical Security Controls – protection of PSP access points and devices used for the monitoring and control of physical access points.

- Policies and tools to monitor, log and alert attempts at unauthorized physical access and breaches at all access points to PSPs and critical areas at all times
- Incident Response Plan for physical security breaches and reporting requirements
- Physical enclosures (6 walled devices) with physical access warnings (e.g. "Authorized Personnel Only")
- Acceptable physical security controls: *Keys/Locks, RFID readers, iris, fingerprint or other biometric systems, cameras, etc*

4.3.5.3. Physical Access Controls – user management and auditing

- User management policies: *Physical access control list and policies for adding, removing and modifying users/user rights*
- Levels of physical access including restricted, escorted, unescorted, visitor or unrestricted and conditions for membership: *use a scaled value to define what the user is allowed to do once granted access. A need to know approach should be taken*
- Policies and tools to monitor and log authorized physical access: *a historical audit trail should be kept indefinitely.*
- Pass, ID, keys and locks management and response to loss or tampering

This procedure will inherently be tied closely to Procedure 5, Change Control and Configuration Management. Anytime there is a change to the physical security of cyber assets, requirements in both procedures will need to be met.

4.3.6. Procedure 4: Electronic Security Plan

This procedure should define the electronic access controls, monitoring and user management policies of the organization; it defines requirements for the first and last lines of defense against remote and local cyber attacks.

4.3.6.1. Electronic Security Perimeters (ESPs) – segmenting and layering electronic security and identification of electronic access points.

- ESP design requirements: *a layered approach is highly recommended by making use of primary, secondary and tertiary ESPs. A Demilitarized Zone should be used to isolate the Primary ESP from untrusted networks*

- Requirements for protection of electronic access points to ESPs: *two factor authentication at each ESP access point, whether primary, secondary or tertiary, is recommended*

4.3.6.2. Electronic Security Controls – protection of ESP access points and individual cyber devices.

- Policies and tools to monitor, log and alert attempts at unauthorized electronic access and actual breaches at all access points to ESPs as well as devices at all times
- Incident Response Plan for electronic security breaches and reporting requirements
- Network security controls: encryption and authentication policies, password/username policies, protection of interfaces between internal and external networks, firewalls, network and device design requirements, network backup and recovery infrastructure, security assessments
- Device security controls: security settings, hardening plan, software verification and code reviews, firewall use and policies, digital media policies
- Backup and recovery: define process for backup generation, validation and recovery and requirements for media and backup systems

4.3.6.3. Electronic Access Controls – user management and auditing

- User management policies: *Electronic access control list and policies for adding, removing and modifying users/user rights*
- Levels of electronic access (user rights) including admin or other user groups and conditions for membership
- Policies and tools to monitor and log authorized electronic access*: a historical audit trail should be kept indefinitely*
- Personnel, domain, login and fair use banner policies

This procedure will inherently be tied closely to Procedure 5, Change Control and Configuration Management. Anytime there is a change to the electronic security of cyber assets, requirements in both procedures will need to be met.

4.3.7. Procedure 5: Change Control and Configuration Management

It is extremely important that semi-automated management systems be in place prior to any attempt to keep track of configuration data. Previous attempts at manual survey and walk downs have not proven to be cost effective compared to automated systems. Even with use of automated scripts to capture data and databases to store data, the costs associated with these reoccurring activities far exceeds those to install new automated analogs. This procedure should include the following main points.

4.3.7.1. Asset management - changes in network design and how devices are tracked and managed on a network

- All changes to the network must be tracked on lists, drawings, databases and anywhere else "current" data exists
- Defines roles and responsibilities for authorization of changes
- Defines policies for new devices or disposal/relocation of hardware

4.3.7.2. Configuration management – changes to device software or hardware design

- All configuration and logic changes to cyber devices must be tracked indefinitely via Operations & Maintenance (O&M) activities: *most of the power sector currently tracks at least the most critical or hard to replace logic on cyber devices, others effectively track all logic.*
- Policies regarding where and how configuration data is tracked, protected and stored: *systematically and electronically manage data to improve security in a cost effective way.*
- Define what configuration data is required and recommended: *all configuration data is useful under certain scenarios. Always know all open ports, installed programs and services, security setting configurations, hardware configurations and other pertinent data.*
- Defines process for hardware upgrades, software changes and version upgrades of operating systems, logic/graphics changes, firmware updates, vendor releases, implementation of security patches and cumulative service packs
- Patch management, testing and rollout: *operating systems, network devices and control system components*
- Define what devices require configuration management: *Typically not necessary for devices like process transmitters, though calibration instructions should be on file and available for immediate recalibration. At a minimum, distributed the DCS, PLCs, human machine interfaces, PCs/servers, switches, routers, hubs and all devices with an Ethernet, serial, modem or USB port should be included.*

4.3.7.3. Change Process – change requests, implementation and testing

- Changes may result from vulnerability identification, patch releases, a need for added/reduced functionality, or many other scenarios.
- A plan should be in place for implementing and testing changes prior to any change occurring. Changes should be tested in-lab prior to implementation in-field and after implementation in-field.
- Process for initiating reviewing, approving, authorizing, implementing and testing changes: *Plan reviews should be approved by authorized personnel to ensure there are no adverse consequences to security. Sufficient backups should be maintained in case a rollback is required.*

Configurations need to be periodically (at least daily) validated to ensure they have not been changed inadvertently or without authorization. This would be completely impractical using manual time intensive methods, automation must be used.

4.3.8. Design Guides

Design guides should not list hard requirements, rather guidelines for effective implementation of security systems based on lessons learned throughout the industry and general best practices. They should be written when a particular need is identified.

4.4. Recommendations for a True Defense-in-depth Approach

Section 4.3 deals entirely with documentation, records and the audit trail. This section is intended to provide an in-depth and comprehensive rundown of the recommended methods, techniques and tools for complying with the policies outlined in the previous section. The methods outlined in this section were developed over the course of a year with particular attention paid to ensuring compliance with the standards previously discussed. When appropriate, new processes should be rolled into existing processes such as the sites Corrective Action Program (CAP) which usually gives requirements for identifying, reporting, evaluating and correcting problems with the plant in general.

4.4.1. Identification, Classification and Categorization

Existing documentation such as connection diagrams and network diagrams could be incomplete and/or inaccurate depending on how well the organization developed and maintained documentation in the past. Any existing documentation must be field verified prior to use in a new compliance effort. It is assumed the organization has already developed a network diagram and sites, systems and a device list.

Sites should be classified by importance to operations and risk of long term widespread impact to other facilities (i.e. severity of an attack). Systems should be classified by importance to plant operation and worst case scenario down time or time to restart (i.e. severity of attack) and likeliness of attack. Devices should be classified based on importance to operation and control (i.e. severity of attack), likeliness of attack and ease of attack.

Classification of all items on the sites list should be completed prior to classification of items on the system or device list. Items on the systems list will inherit some requirements from the sites list and devices will inherit some requirements from the systems list. The results of this classification process should be used to determine what sites, systems and devices should be addressed first and which sites, systems and devices should be protected the most. This will help determine yearly funding needs. The process should be kept as simple and intuitive as possible yet remain effective.

As of 2010, most governing authorities do not specifically call out the methods and classification titles of sites, systems or devices. It is therefore left up to the organizations to develop a scheme. The following provides a recommended scheme for classifying items on the sites, systems and devices lists. This should be tailored to the organization, but it is not recommended that the organization curtail any of the requirements. Classifications are numbered based on level of importance in ascending order with 1 implying the most essential and important classification, this will assist in quickly interpreting and disseminating the knowledge concerning the severity of an immediate attack regardless whether the attack is against a site, system or device.

4.4.1.1. Sites

Examples of sites may include generating stations, control centers, backup control centers, large transmission substations, facilities critical to system restoration, automatic load shedding, and special protection systems.[14]

Scheme:
Q0 - severity of attack: Does an asset if destroyed, degraded, compromised or otherwise rendered unavailable, impact the reliability of the Bulk Electric System? Can adverse consequences of a cyber attack at the target site spread far beyond the target site?

Level of Importance	Q0	Classification	Implications
2	No	Non-Critical Site	Well protected site, eventually.
1	Yes	Critical Site	Highly protected site and addressed first.

Usually, factors to consider when answering Q0 should include peak load generation, availability (how long process restoration will take in a worst case cyber attack scenario) and integrity (how resistant the site is to compromise and permanent damage to systems). Precise methodology to determine the critical nature of a site has not been given by most governing authorities, probably because the authorities simply have not identified the most effective methods yet due to the relative newness of this field. See Appendix A: Examples.

4.4.1.2. Systems

Systems vary greatly from site to site; each site usually has a pre-developed systems list. Examples of common systems at a coal plant are Boiler, Turbine Control,

[14] North American Electric Reliability Corporation, NERC. CIP-002-3: Critical Infrastructure Protection. Washington, DC : NERC, 2009.

Burner Management, and many more. Examples of common systems at nuclear plants include Reactor Control, Fuel Loading, Turbine Control, and many more.

Scheme:
Q1 - likeliness of attack: Does the system include cyber devices?
Q2 - severity of attack: Does the system directly support the reliable operation of the site or can system compromise negatively affect generation capacity or reliability?

Level of Importance	Q1	Q2	Classification	Implications
4	No	No	Non-Critical Non-Cyber System	Least critical systems which are usually outside scope of compliance, but which should still be at least minimally protected in some manner.
3	No	Yes	Critical Non-Cyber System	System will still require physical security controls and management if feasible.
2	Yes	No	Non-Critical Cyber System	System will still require electronic security controls and management. Physical security controls are still highly recommended and are often required under certain scenarios anyway.
1	Yes	Yes	Critical Cyber System	By far the most critical systems, Requiring application of all the nuances of an organizations security policies and processes.

Answering Q1 is relatively straightforward and only depends on how an organization defines a cyber device or cyber asset (as discussed in section 4.3.1.2). Answering Q2 will usually involve approximating the effect of total system loss to the plant and other systems; it will be a somewhat subjective process and should be answered by knowledgeable plant personnel and verified. Precise methodology to determine the critical nature of a system has not been given by most governing authorities, however, most authorities recognize or recommend some form of device grouping; remember, new processes and requirements should be merged with existing processes to as much extent as possible. See Appendix A: Examples.

4.4.1.3. Cyber Devices

Examples of cyber devices typically include a DCS, PLCs, SLCs, modern switchgear and relays, recorders, analyzers, and other Ethernet devices. Digital meters, indicators, process transmitters, and other such devices whose software functions are only validated by calibration, devices whose primary programming interface is a local manual keypad or devices without digital communications connections should not be included **generally**. Cyber devices need to be assigned to a system and documented on the device list prior to classification.

Scheme:
Q3 - severity of an attack: Does the device directly support the reliable operation of a critical cyber system (level 4 system) or would the device disrupt operations of a critical site (level 1 site) or critical cyber system if compromised (level 4 system)?
Q4 - likeliness of attack: Is the device used for physical or electronic access control or monitoring of a PSP or an ESP or does the device perform system or plant control via human machine interfaces (level 2 & 3 systems)?
Q5 - ease of attack: Does the device use routable protocol to communicate outside an ESP, does the device use routable protocol inside a control center, or is the device dial-up accessible (level 3 & 4 systems)?

Level of Importance	Q3	Q4	Q5	Risk	Classification	Implications
4	No	No	No	Low	Non-Critical Cyber Devices	Least critical devices
3	No	No	Yes	Medium	Level 3 Critical Cyber Device	*
3	No	Yes	No	Medium	Level 3 Critical Cyber Device	*
2	No	Yes	Yes	High	Level 2 Critical Cyber Device	*
3	Yes	No	No	Medium	Level 3 Critical Cyber Device	*
2	Yes	No	Yes	High	Level 2 Critical Cyber Device	*
2	Yes	Yes	No	High	Level 2 Critical Cyber Device	*
1	Yes	Yes	Yes	Highest	Level 1 Critical Cyber Devices	Most critical Devices

* Levels of criticality can be used as a guide during network design, to ensure the highest levels of criticality are inherently addressed first and protected and audited the most.

Q3, Q4 and Q5 are not difficult to answer so long as the evaluator is familiar with the systems involved. Q3, Q4 and Q5 inherit some logic from the systems and sites classifications which ties the three classifications together. Precise methodology to determine the critical nature of a device has not been given by most governing authorities, however, most authorities require or recommend some form of risk based and/or tiered approach. In regards to a tiered approach it is often cheaper to apply one class of security control across all devices regardless of the classification than to apply multiple requirements to various classes of devices. See Appendix A: Examples.

4.4.1.4. Information Categorization

Confidentiality, integrity and availability are key goals for information. All information should be classified based on low, medium and high levels of potential impact to any of these information security goals. The following table provides a recommended risk-based approach to information categorization, which is highly based on FIPS 199.

	Risk		
	Low	Medium	High
Confidentiality: Ensures information is accessible only to those authorized to have access	Unintended or malicious release of information is predicted to have a **limited** adverse effect.	Unintended or malicious release of information is predicted to have a **serious** adverse effect	Unintended or malicious release of information is predicted to have a **severe or catastrophic** adverse effect
Integrity: Ensures data is not improperly modified or handled	Unintended or malicious modification of information is predicted to have a **limited** adverse effect	Unintended or malicious modification of information is predicted to have a **serious** adverse effect	Unintended or malicious modification of information is predicted to have a **severe or catastrophic** adverse effect
Availability: Ensures that data is accessible at a required times	Interruption of access to information is predicted to have a **limited** adverse effect	Interruption of access to information is predicted to have a **serious** adverse effect	Interruption of access to information is predicted to have a **severe or catastrophic** adverse effect

SC *information type* = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, impact)}, where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE; information type is administrative, public, investigative, process control data, etc. [15]

4.4.1.5. Classification Summary & Utilization

The following table is based on previously developed classifications and provides guidance regarding which devices, sites and systems need to be addressed in which order, as indicated by the alphabetical order of the letter designations. This is just one example of how classifications can be made of use.

Cyber Device Level	Critical Sites				Non-Critical Sites			
	System Level							
	1	2	3	4	1	2	3	4
1	a	b	c	d	q	r	s	t
2	e	f	g	h	u	-	-	-
3	i	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-

The benefit of designing a comprehensive and open ended classification system is that classification assignments can be automated and tracked by database systems and assigned based on user input to specific questions. New regulations, which are always anticipated, should not significantly alter current operations. The idea is simple, truly protect cyber systems effectively and responsibly and the nuances of compliance standards become somewhat irrelevant. For example, any new regulations requiring identification and classification activities need only assign new titles to an existing methodology; any new requirement set forth can simply be added to an already effective security plan.

4.4.2. Electronic Security Controls and Measures

This section is dedicated to strongly securing access points to electronic security perimeters and discrete cyber devices.

[15] Computer Security Division, National Institute of Standards and Technology (NIST). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: Federal Information Processing Standards (FIPS), 2004.

4.4.2.1. Electronic Security Perimeters (ESPs)

ESPs will be used to segment the network and will be critical in planting security controls. All ESPs need to be inherently trusted zones. All access points, whether Ethernet, fiber, proprietary or any other physical or wireless connection to an ESP, must be identified and protected appropriately. It is extremely important, for an effective defense-in-depth approach that ESPs are defined in a layered or hierarchical approach. Generally, primary, secondary and tertiary ESPs will suffice.

The primary ESP should comprehensively encompass the entire site, all ESPs, and thus, all trusted zones. All physical and wireless connections must be identified and documented. These connections to a primary ESP will be external connections, and are by far the most important to protect, obviously; they are, usually, the only access points available to a remote attacker. Access points to a primary ESP deserve somewhat excessive protection mechanisms, stronger authentication and strong encryption mechanisms.

Connection points between discrete secondary ESPs of a given site will be internal access points for various network segments. A secondary ESP should never have any site external connections. All external connections to a secondary ESP should pass directly through the primary ESP before communicating to the outside world. Connection points between discrete secondary ESPs deserve robust and effective controls, as discussed later.

Often, sites do not protect tertiary ESPs or even define them, this is a mistake. Tertiary ESPs are the last line of defense for cyber devices. They deserve the same level of controls and protection as secondary ESPs, though somewhat more specialized and tailored to each discrete ESP individually. All highest risk critical cyber devices should be included in a Tertiary ESP. This layered approach is an effective defense in depth approach that facilitates isolation of one ESP from another during compromise.

4.4.2.2. Protection of ESP Access Points

Defense-in-depth is a layered security strategy and tactic used to strengthen security controls at all levels. Defense-in-depth originated as a military strategy with a goal of delaying, rather than preventing the advance of an attacker by yielding space to buy sufficient time to respond effectively. An effective defense-in-depth strategy results in either an attack attempt of infeasible duration or an attack duration that buys enough time to detect and respond to an attack. Various methods and tools are discussed in the following section. Always vary the use of tools and vendors across levels to make the network more resistant to compromise.

A. Limiting access to the Primary ESP via the DMZ

The DMZ limits and controls all communication between trusted zones, which make up the area internal to the primary ESP, and un-trusted zones. Any individual device that connects to an un-trusted zone needs be included in the DMZ to maintain a true DMZ. Any device included in the DMZ would inherently be a *level 1 Critical Cyber Asset* by the previously developed classification and thereby all connections to the DMZ will have the highest levels of security. The DMZ is a bit special, and even this is too low of a classification; special considerations are required for this zone. Firewalls from two different manufacturers must bridge the trusted zone and un-trusted zone access points. This prevents a vulnerability in one firewall from allowing access to the entire system. In an ideal setup, there is only one connection between the DMZ and the untrusted zone and one connection between the DMZ and the trusted zone. If only unidirectional communication is required or the organization can operate with unidirectional communication, install a data diode; they serve their purpose well. Virtual Private Networks (VPNs) may prove to be an effective security control within the DMZ.

Internet access should not be permitted directly through the DMZ, an ESP or a trusted zone. Internet access from the primary ESP may be obtained through the DMZ then through the business network, but even this is not good practice and should be avoided. All communication protocols associated with the Internet Protocol Suite (e.g. TCP/IP) should be routed through a stateful firewall.

B. Limiting access between Secondary ESPs

Secondary ESPs should only communicate with other secondary ESPs or access points to the primary ESP. Electronic access to any secondary ESP through any access point should only be permitted through a well managed and stateful firewall. Log all access events. Monitor, detect, and alarm all attempts and actual unauthorized access events continuously and electronically. Consider recording user activity in some manner. Provide session lock for inactive users and an effective method to terminate sessions. Protect redundant connections as well as primary connections. All level 1, 2 and 3 devices should be housed in a secondary or tertiary ESP.

C. Limiting access between Devices and/or Tertiary ESPs

Tertiary ESPs should only be defined for highest risk cyber devices and must be tailor to each system.

D. Domain Controllers, Active Directory and Group Policy Objects (GPOs)

In-depth discussion of domain controllers, active directory and GPOs are outside the scope of this paper, however, they are highly recommended. These controls provide ease and cost savings to security and user management and deeper insights into an operating system's security configurations, if they are used properly. NIST Special

Publication 800-81, "Secure Domain Name System (DNS) Deployment Guide" is a recommended guide for installing domains at enterprise facilities. As of July 2010, an equivalent guide does not exist for generating facilities, but this is a good starting point.

4.4.2.3. Protection of cyber devices

When determining how to protect cyber devices, classifications can play a key role, but only if they are design and implemented correctly; over fragmenting policies across too many levels of criticality or over applying too few policies across often too few devices are common mistakes. The classifications outlined in section 4.4.1 are intended for large industrial facilities. When security controls are applied, apply them in a layered approach but try to maintain some continuity at each layer, unless excessively strong protection mechanisms are required, such as in the DMZ, where the **appearance** of disorder may be advantageous.

A. Applying protections to devices

The protections applied to various components in an industrial control system will vary greatly depending on many factors, but the following guidance should be helpful. The protections will generally vary by level of risk/criticality, but note that it is often more cost effective to apply one set of controls to all classes of devices rather than attempting to apply different sets of controls across the same class of devices; a balance needs to occur. The below recommendations for applying controls to devices is meant to act as a list of minimum requirements. Each hardening subject matter applied below is discussed in detail in section 4.4.2.3B.

<u>PCs/Servers</u>

Age, Operating System (OS) and function of PCs/Servers throughout a plant tends to vary greatly. This needs to be a consideration while applying controls. Whenever possible, standardize on one operating system for a given plant.

- Surface area reduction via baseline hardening - level 1, 2 and 3 devices
- Surface area reduction via device specific hardening – level 1 and 2 devices and certain level 3 devices
- Configuration and security settings – level 1, 2 and 3 devices
- Protection software – level 1 and 2 as well as level 3 devices where yes was answered to Q5 (ease of attack).
- Communications and Data hardening –level 1, 2 and 3 devices
- Maintenance and hardware hardening – all device levels
- Physical security hardening – levels 1, 2 and 3 devices

Network switches

This refers mainly to managed switches here. Unmanaged switches, hubs and routers have limited security capabilities and should be avoided.

- Surface area reduction via baseline hardening - level 1, 2 and 3 devices
- Surface area reduction via device specific hardening – level 1 and 2 and some level 3 devices
- Configuration and security settings – level 1, 2 and certain 3 devices
- Protection software – level 1 and 2
- Communications and Data hardening –level 1, 2 and 3 devices
- Maintenance and hardware hardening – all device levels
- Physical security hardening – levels 1, 2 and 3 devices

Printers

Modern printers tend to come with operating systems, storage and Ethernet capabilities. They can be just as vulnerable as PCs, security controls may be limited.

- Surface area reduction via baseline hardening - whenever feasible
- Surface area reduction via device specific hardening – whenever feasible
- Configuration and security settings – all device levels
- Protection software – Not directly applicable
- Communications and Data hardening –level 1, 2 and 3 devices
- Maintenance and hardware hardening – whenever feasible
- Physical security hardening – whenever feasible on level 1 and 2 devices

PLCs

Many modern and all obsolete PLCs were not designed with security in mind. As a result, inherent controls are currently limited and a dedicated add-on security device such as the Tofino Security Appliance is usually required. Whether or not a similar appliance is the housing device, the following controls should be applied.

- Surface area reduction via baseline hardening – level 1, 2 and 3 devices
- Surface area reduction via device specific hardening – level 1 and 2 devices
- Configuration and security settings – all device levels
- Protection software – Usually not directly applicable, but implement when feasible.
- Communications and Data hardening –level 1 & 2 devices
- Maintenance and hardware hardening – all device levels
- Physical security hardening – all device levels

DCSs

Until recently, DCSs have not accounted for much in the way of security. Modern DCS manufacturers claim to have built in "compliance" toolsets, which probably will be of some use when protecting these devices. Applying security controls to a DCS may be difficult depending on the age of the device, and third party hardware may be required.

- Surface area reduction via baseline hardening – level 1, 2 and 3 devices
- Surface area reduction via device specific hardening – level 1, 2 and 3 devices
- Protection software – level 1 and 2 devices when feasible (third party devices will be required on older systems)
- Communications and Data hardening –level 1, 2 and 3 devices
- Maintenance and hardware hardening – all device levels
- Physical security hardening – all device levels

Recorders, Relays and similar Ethernet devices

Security, both physical and electronic, is limited for this class of devices, though controls are still often mandated by governances. If it is infeasible to implement the following controls, try using third party tools or, if possible, disabling the Ethernet capabilities of these devices until a solution is marketed.

- Surface area reduction via baseline hardening – port closing only when feasible across levels 1, 2 and 3.
- Surface area reduction via device specific hardening – port closing only when feasible across level 1, 2 and 3 devices.
- Protection software – level 1 and 2 devices when feasible using third party hardware
- Communications and Data hardening –level 1, 2 and 3 devices
- Maintenance and hardware hardening – all device levels when feasible
- Physical security hardening – all device levels when feasible

Devices used for access control and/or monitoring of ESPs & PSPs

Deserve strong protection mechanisms; if an attack can gain control over a device of this class, the attacker can usually gain control over all communications running through the device. A device of this class will never be a level 4 device due to the content of Q4 (likeliness of attack).

- Surface area reduction via baseline hardening – all device levels
- Surface area reduction via device specific hardening – all device levels
- Protection software – all device levels

- Communications and Data hardening – all device levels
- Maintenance and hardware hardening – all device levels
- Physical security hardening – all device levels

At this point it should be obvious that it is often more cost effective to apply one set of controls to all classes of devices rather than attempting to apply different sets of controls across the same class of devices. This may not always be feasible though, because different systems may have been installed at different times and by different people throughout the 50 year life of the plant. A database that automatically assigns necessary controls based on criticality (which is based on user inputs to a discrete set of questions) is highly recommended for applying differing security controls across all devices and across individual classes of devices.

B. Hardening

The goal of hardening efforts on cyber machines is to ensure that only those ports, programs, and services required for normal and emergency operations are enabled, to ensure the security policies are met and to add or strengthen security mechanisms (e.g. virus protection) to result in a more secure system than initial examination revealed. This section is written from the standpoint of hardening mainly computers, but a number of the requirements herein may be applied to other devices as appropriate.

A full hardening process should only be required on a single cyber device once, so long as no major changes have occurred. If a major change has occurred, such as changing the purpose of the device, a full hardening process is required. Security policies should be sufficient to maintain an unchanged device's hardened status.

It is extremely critical that hardening be done using a systematic and software assisted technique. Generally, the first major step of any technique used should involve the development, implementation and testing of baseline hardening policies via objects in an active directory, security or administrative templates, or third party tools such an enterprise configuration manager. The second major step of any technique used should be to harden each specific cyber device against developed and tested device specific hardening policies.

Extreme care must be taken during hardening efforts. Significant adverse effects can occur when a device is incorrectly hardened. Loss of functionally requiring a full system restoration is one possible result. All baseline or device specific hardening activities should not result in any unforeseen or unplanned changes. Hardening should not affect normal or emergency functionality in any way; for example, operator screens, logic and alarms should not be affected by hardening efforts.

A prerequisite of hardening is that configuration data about the devices being hardened must be obtained before hardening the device. Attempting to harden cyber assets without complete and accurate information can result in dangerous, if not catastrophic, situations, especially when trying to harden devices associated with a running unit which should be avoided if possible. Software that makes use of databases and configuration and vulnerability scanners to provide a partly automated solution can be of significant assistance in managing configuration data.

Security, Configuration and Asset Management

There are only two effective tools that past experience has identified for managing security and configuration data in an automated fashion. The first is Microsoft's Management Console (MMC) operating in an active directory and domain environment. This is the most common tool used, particularly in the IT realm. The second is Enterprise Configuration Manager (ECM), which also requires a domain. ECM provides additional tools and graphics above and beyond MMC. Asset management is inherently ingrained in the software, though particular attention needs to be paid to disposal or redeployment of unused hardware (which is not covered in the software). Antiquated, obsolete or non-vendor supported devices should be replaced as soon as possible. Patch management and virus signature file updates should be built into the software, no need for another tool if it can be avoided. Ideally, the system should be able to perform assessments of security vulnerabilities, audits against governing or custom standards and remotely initiated maintenance activities. Each organization will have to determine the best configuration management solution for themselves, hopefully with a formal software validation, verification and analysis program. Refer to NIST Special Publication 800-40, "Creating a Patch and Vulnerability Management Program" for additional guidance on creating an effective patch management program to ensure all devices are patched to an adequate level.

Whatever managing software an organization selects, there are established best practices to follow that will save time and money. All records of device configurations must be kept indefinitely on electronic media, stored by date, managed and well protected to provide evidence for auditors. New cyber devices must be hardened before they hit the network or are scanned for configuration data. Every change must be tested in lab, then implemented, then tested in the field. Changes can be grouped for a device or multiple devices, if the infrastructure is in place, to expedite this process. Tests must ensure no loss of normal or emergency functionality will or has occurred. Rollbacks may be required and backups should be performed prior to implementation and after testing. Devices should also be rescanned for configuration data directly after successful field testing.

Lastly, there are some tools designed specifically for auditing a computer. Some only have local capabilities; others can be run remotely, often in scheduled runs. Some gather highly useful raw configuration data and others simply output a list of

vulnerabilities. Manually gathering data locally is not recommended, though, Winaudit works well if it is necessary. Additional or similar tools that work well include Nmap, Zenmap, Nessus, HP Discovery, and a number of others. Well planned and thought out network scans performed during an outage are the preferred method of obtaining the data; though systems can be programmed to slowly and non-invasively gather data during operation. Also note that the level of data gathered is directly related to the level of privileges of the user's account, logging in with higher account privileges before a scan will generally produce more data regardless of the tool used. There is always an inherent danger in network scans, particularly while a unit is running, but safe scans are feasible. Usually it only takes controlling the speed of the scanning process to ensure an unintentional denial of service attack doesn't occur.

Device Targets

Cyber devices that may be targeted for any industrial hardening project include but are not limited to clients, servers, PLCs, DCSs, HMIs and network switches. These are definitely not the only devices that need to be hardened, but they are devices that must not be missed. Whatever targets are chosen, it is important to realize that each class of targets presents unique challenges and implementation dangers. Classifications combined with vulnerability data can play a key role in determining the order in which devices should be hardened. These projects are not short lived or uncomplicated by any means. Speaking only in terms of orders of magnitude, a large power plant can have:

- Upwards of 150 computers and servers associated with plant systems alone
- Around 50 PLCs
- Anywhere from 1 to 5 discrete DCS loops
- Upwards of 100 HMIs
- The total number of network switches varies greatly from plant to plant, usually only correlating with design effectiveness and management rather than plant size.

It is a big project to harden the devices in an entire plant, and this is with the assumption the network is designed effectively. This combined with the fact that due to the length of the project, some devices will have to be hardened while a unit is running. Of course, the least critical devices should be chosen for this whenever possible, but a well analyzed risk to generation may be necessary from time to time. Discussion of how to address common device types is given in section 4.4.2.3A.

Subject Matters of Hardening Efforts

Subject matters of both baseline and device specific hardening projects may include, but are not limited to:

- Surface area reduction (ports, programs, and services)
- Configuration and security settings (GPOs, firewall rules, user and password policies, patch management, etc.)
- Protection software (intrusion detection and prevention, virus protection, patch management, firewalls)
- Communications (protocol use, encryption, authentication) and data hardening (encryption, compression, backup and restorations and data redundancy)
- Maintenance (scheduled defrag, registry cleanup, etc.), hardware (locks, enclosures, redundancies, etc.) and physical security hardening.
- Network architecture and segmentation
- Replacing antiquated, non-vendor supported or high risk legacy systems

Each subject matter presents unique challenges and implementation dangers and will be discussed in the following paragraphs, excluding the last the two which are discussed elsewhere.

Surface area reduction (ports, programs and services)

Reducing the amount of software and number virtual ports on devices makes them inherently harder to compromise. To give a physical analogy, a house is far harder for a burglar to compromise if it has no windows or perhaps bars on the first floor windows. The order of reduction needs to be first programs, then services and last ports. This is because programs make use of services and services and programs make use of ports. Going in any other order will negate work or make hardening profiles invalid or ineffective. Surface area reduction needs to be done systematically. Ideally, multiple iterations of (1) identify required ports, programs or services (2) determine which are not being used and remove (programs and services), deactivate (services or ports) or block (ports) (3) Provide a justification for all that remain.

Identifying required ports, programs and services is fairly straight forward at first, if performed by someone familiar with the system, but may become more difficult as one progresses. This is where the use of simulators and drive images and virtualization can play a key role. Virtualization or simulation allows for removal, deactivation or blocking of one port, program or service to see what effects it has on the system. If the effects are adverse, re-enable it and explain the adverse effects in the justification. If no normal or emergency functionality is lost, it is probably safe to disable. All ports, programs and services that cannot be justified will need to be

removed. If an entire network is accurately virtualized, the results of this process may be reapplied directly to the device.

Programs and services to remove will vary from device to device, but the following should be removed from all devices at a minimum (it is not an uncommon occurrence to find these in the field): games, messaging services (MSN, AOL IM, etc.), sample or demo software, unused document processing utilities, unused and/or insecure remote access software, unnecessary logic and software compilers, and any other programs or services identified as unneeded. Remember, everything that isn't removed needs to be justified. Justification is the only way to maintain compliance and knowledge concerning why a particular device has a particular configuration, especially as sites gain and lose employees over the life of the plant.

Service removal often takes particular care and expertise. If it is unclear whether a service is needed or not, it must be fully tested in a lab environment. Once it is determined that a certain service is not needed, it should be fully uninstalled (not just deactivated) whenever possible. There are thousands of services running across many operating systems, refer to http://www.blackviper.com for a good explanation of typical services and a starting point for hardening profiles.

All ports, regardless of the state (listening, established, etc) need to be disabled if they cannot be justified. Ports used for testing purposes only need to be disabled when not in use. Port closing is usually accomplished with a typical firewall, but there are other more specialized methods.

Tools recommended to assist in surface area reduction without the consideration of vulnerability remediation include: Windows Task Manager, GPOs in an active directory, Windows control panel programs like add/remove programs and windows firewall, the Microsoft management console which can provide customized views of the devices configurations including services, programs and security settings, and third party tools like WinAudit or ConfigureSoft's ECM. Introduction to these tools is outside the scope of this paper, but there are plenty of resources on the internet. It is recommended that an organization standardize on what tools are allowed to be used for this purpose, preferably limiting the total number of tools and maximizing the automation and scheduling capabilities.

Security and Configuration Settings

Security and configuration settings will always be operating system dependent. Even between versions of the same OS such as Windows XP and Windows 7 or between various patch levels or service packs, variations exist. As a result, a baseline settings policy must be defined for each operating system. This assumes all the operating systems on all the devices in a facility are patched to the same level (if not, update all patches prior to developing security and configuration policies to ensure work is not negated).

Settings can be viewed and changed locally, both manually using management consoles and semi-automatically using security templates or local group policy objects (LGPOs), but even though this may appear to be cost effective for an organization without an effective infrastructure, it turns out to be far more expensive in the near and long terms than simply implementing the appropriate infrastructure first.

Precise definition and risk assessment of every security setting on every OS of every patch level is far outside the scope of this paper due to the massive data requirements. However, each OS manufacturer usually provides sufficient documentation to at least glean the purpose of most settings. Additional third party guides may prove to be highly useful; a recommended site to begin with Windows security settings which, in previous experience, has proven very useful is http://www.ultimatewindowssecurity.com/.

The remainder of this section is dedicated to stating a few examples of important user management policies (to give the reader a feel for how to think about each policy) that can only be applied via these settings. It is not a comprehensive discussion; all settings should be analyzed, not just the most important ones.

Use two factor authentication for local and remote login, particularly if the user is connecting through multiple zones or ESPs. Two factor authentication is based on selecting two out of three of the following for authentication: something you know (e.g. password), something you have (e.g. RFID card) or something you are (e.g. biometrics).

When defining levels of access (i.e. user accounts) DO NOT use generic account names like admin or user and try to avoid shared accounts. This leaves the system vulnerable, often only requiring an attacker to guess a password to obtain user or even admin rights. Do not use the same username as is used on the organizations enterprise networks or any username associated with an email account. These tend to provide an easy method for an attacker to obtain a list of valid usernames. Ensure passwords are changed at most every 90 days and that no password is reused for a minimum of two years. No more than three unsuccessful login attempts should be allowed before the user is kicked and required to wait an appropriate period of time. Tools for applying settings where discussed above.

Protection Software

Protection software such as virus protection, intrusion detection and prevention, malware prevention and firewalls should always be included in a device's profile if the device can take the software without adversely affecting the device's functionality. This can be a challenge since a large number of process computers currently in use are old unsupported systems with obsolete hardware. There are a

few computers running plants that were built in the 1980's. Devices such as these cannot handle modern protection software and using 20 year old virus software is pointless, so eventual system replacement is needed. Of course, it is not always as clear cut as this, and performance reports will probably be required to determine which devices can handle the added load of protection software. Performance reports should take place over the course of a day to get an accurate report due to load variations, and this should be repeated over a few days. Variables to track may include CPU and memory usage, hard drive utilization, and network bandwidth usage.

Virus protection software typically scans and continuously monitors activity on a computer, though continuous monitoring capabilities have proven thus far to be resource intensive. In most situations, it is usually recommended that process control computers only be fitted with the ability to scan for viruses at night or during similar low load times. Certain areas and access points should be continuously monitored by virus software, but this functionality should only be included on non-process related devices whose sole purpose is security, such as devices used for the monitoring and control of ESPs. It is also worth noting that, even if all virus definitions are kept up to date the effectiveness of the software will change, but not necessarily degrade, with time. This is because the manufacturers tend to go through cycles in how effectively and comprehensive they roll out virus definitions. Some companies may miss a virus definition on occasion or funding may restrict their development. This is why it is key for an effective defense-in depth approach to layer security using mechanisms from more than one manufacturer.

The difference between malware and a computer virus is not so clear to the laymen; often a virus can also be malware or malware can be a virus. To clarify this often over discussed distinction, malware is software designed for a malicious intent and a virus is designed to replicate itself, whether or not maliciously. A virus typically has the ability to spread to other devices. There are other types of threats including adware (code written for the purposes of advertisement, often with little consideration for the users systems) and spyware (code written to secretly obtain information without authorization from the user). Malicious software prevention is used to detect, prevent, and mitigate introduction, exposure, and proliferation of malware on cyber devices. Adware prevention is used to detect, prevent and mitigate the results of advertising code on computers (e.g. "popups"). Spyware prevention monitors continuously for eavesdropping attempts. Each type of protection software has its purposes; all should be used at some level of the process control network hierarchy, particularly at access points to ESPs. Recommended manufacturers for each type of protection software discussed above are as follows:

- Virus prevention and protection: Recommended manufactures include Symantec, Trend micro, AVG, Avast, BitDefender and certain hardware

based virus protection devices such as the devices sold by Barracuda Networks.

- Malware prevention and protection: MalwareBytes is highly recommended for this purpose. Most other manufactures discussed throughout this section include similar capabilities in their software, but they have not proven to be quite as effective, probably because MalwareBytes is solely focused on malicious software and not things like adware.
- Adware prevention and protection: Ad-aware (highly recommended), MacAfee, Trend micro, windows defender and popup blockers.
- Spyware prevention and protection: Ad-aware running in continuous monitoring mode, Windows system monitoring controls inherent in recent versions, and other software which continuously monitors for unauthorized information disclosure.

Of course, the line between protecting against these classical types of threats is getting blurred with time because manufacturers are trying to account for all at once, though often unsuccessfully since each requires a unique approach. Protection software needs to be analyzed to determine which classical threat definitions (as described above) the software can effectively mitigate. Caution is advised when selecting protection software, the internet is full of software posing as protection software but which is often highly malicious software (often called scareware).

Intrusion detection and prevention software (IDPS) is focused on preventing, detecting, alerting and responding to potential unauthorized intrusion incidences or attempt at intrusion. Until recently, IDPS has been fairly experimental, however, it has now become an effective defense tool that should be included in any cyber defense arsenal, even though it is still somewhat experimental and requires a knowledgeable person to effectively operate and understand. Common detection methodologies include signature based, anomaly based, and stateful protocol analysis. For additional information on IDPS systems, refer to recommended NIST Special Publication 800-94, “Guide to Intrusion Detect and Prevention Systems (IDPS)”. Top five tools include Snort, OSSEC HIDS, Fragrouter, BASE and Sguil according to sectools.org.

Firewalls are extremely useful for controlling communications, able to close virtual ports on demand. A firewall is only as good as its rules. Firewall rules should be as specific as possible. Always consider source, destination, protocol use, ports, and services and programs. All ports should be disabled with the exception of the ports needed for normal and emergency operations. All ports that remain open should be provided with a short justification for reasons already stated in previous sections. Effective firewall software is easy to come by, so vary the manufacture to help ensure a vulnerability in one firewall is not perpetuated throughout the network.

Communication and Data Hardening

Communication hardening typically involves limiting protocol use, limiting open ports, authentication, encryption and data integrity. Authentication is critical to ensuring communications are going to and coming from an authorized source. Data hardening usually involves encryption, redundancy, off site redundancy, image comparators, automatic data restoration, corrupt data detection, RAID technologies, etc. Communication and data redundancy via redundant physical communication channels can also be effective strategies. Data redundancy of large generating facilities needs to be automated to be cost effective.

Data redundancy requires a formal backup and recovery program to store and roll back configuration changes in case of failure, attack or compromise. Only one approach to backup and recovery should govern a single class of devices (e.g. PCs, DCSs) to minimize cost and confusion, though application across manufactures is also common (i.e. only one backup system using one type of backup media on a single device class or by manufacturer). Whatever system is chosen for a given device grouping, each will need a step-by-step backup generation, data validation, data restoration and data redundancy plan. Safety needs to be a key part of the data restoration plan. Any time a backup is generated, validated or restored, an audit trail should be maintained and kept indefinitely. Data security is critical, and backup and backup storage systems should be treated as level one critical cyber devices. This is inherent against the classifications previously developed since a good backup system is robust, covers large areas of the network (breaking ESP boundaries) and often communicates off site for redundancy.

Backup systems should be centralized, secured and at least partially automated to reduce cost and increase reliability. Manual backup processes are high cost, high risk and are not recommended. Any backup process, whether automated or manual, can easily overburden a control network and cause denial of services if not controlled properly, so incremental rollout and slow or incremental backup operations will be required. Transportation of backup media off site needs to be well controlled, protected and documented. All backups associated with a process control network should be categorized as: SC process backup = (confidentiality, high), (integrity, high), (availability, high).

Selecting the right backup media for a given backup system should be a formal process, considering current and future capacity, automation abilities, time to generate, time to restore, time to compare or validate, storage requirements, as well as reliability and security. Optical disks, secure EEPROMs such as Ironkey, magnetic tapes and disks, swappable drives, RAID drives and logical media like hard drive images all serve a purpose and present unique advantages and disadvantages. Ideally, a primary backup should remain on site and a secondary backup should be placed off site at a secure location. On each device, separate data and the OS root drive on two physical drives; this is just best practice, helps

with system restoration and segmenting any damage caused by an attack. The majority of attacks focus on the root drive, so this tactic will save your data in most cases.

Backup generation needs create backups that can suitably restore a system in worse case scenarios (i.e. total data loss). Logic, graphics screens, custom programs, device configurations. All level 1, 2 and 3 devices should have scheduled backup operations. If a valid backup is not on file, backups should be made before a new device arrives on site, before a change occurs and after a change occurs. Device backup files should be titled with the name or identifier of the device followed by the date and time for auditing purposes.

Backup validation is the process of verifying a backup operation was successful and valid, verifying that a stored backup did not degrade with time, verifying that the backup represents the working configuration of the device. Backups need to be validated as soon as they are generated, and periodically during storage. Virtual machines and networks can significantly help with validating backups to ensure no loss of data has occurred; another technique is to compare bit-by-bit the data contained on two identical backup media stored in two separate physical locations.

Backup restoration is required if there is a compromising event on a device, if the system is not functioning or if the system is suffering from data corruption. A restoration will only be as good as the backup used, this is why backups are validated; only validated backups should be used to restore a system, redesign is required if data is compromised and there is no validated backup.

Maintenance, Hardware and Physical Security Hardening

No modems should be allowed “period”. Disable physical Ethernet, USB, serial and proprietary protocol connections when not in use. This can be achieved either physically or via software. Ensure the computer is housed in a locked 6-wall cabinet in a 6-walled room. Ideally, the computer enclosure should be industrial grade with cylinder locks. Hardware redundancy is highly recommended and actually very common in plants today. Hot swappable devices will make maintenance easier. Remove unused hardware.

System Maintenance should be performed via automated scheduling on a periodic basis to reduce clutter (and attack surface) and maintain performance. This should include, but is not limited to: registry cleaning, disk cleanup and defragmentation. The order should be maintained to maximize system maintenance effectiveness.

4.4.3. Physical Security Controls and Measures

Many of the requirements in controlling electronic access to devices inside an ESP and protecting devices within an ESP are endemic in physical security as well. A lot of the overlap has been eliminated in this section, instead trying to focus on the differences. The subjects are closely related, and cannot be completely separated. This section is dedicated to strongly securing access points to physical security perimeters and securing physical devices. Electronic security without physical security is not an option for reasons that should be obvious to the reader.

4.4.3.1. Physical Security Perimeters (PSPs)

PSPs will be used to segment the plant and will be critical in planting security controls. All access points must be identified and protected appropriately. It is extremely important, for an effective defense-in-depth approach, that PSPs are defined in a layered approach. Generally, primary and secondary will suffice, tertiary PSPs can be used in special circumstances.

The primary PSP should comprehensively encompass the entire plant, all PSPs. The access points to a primary PSP are the first line of defense against local attacks, whether physical or cyber, and are by far the most important to protect. Access points should be minimized with only one point for personnel, one or two points for fuel and other material deliveries. Access points to a primary PSP deserve somewhat excessive protection mechanisms. Cameras, RFID or SSD preferably, guards, sign-in sheets, plant contact confirmation and ID verification should all be part of the access process.

Access points to discrete secondary PSPs, a door to a room within the plant, deserve robust and effective controls. RFID has proven to be highly insecure; as a result, if RFID is used, two factor authentication should be required.

One special circumstance that may warrant the use of tertiary PSPs are the access points to the main control rooms. Often plant operators resist the use of locking access systems and login requirements, and for good reason. If there is an emergency, operators need to get where they need to be and access the things they need to access. In addition, plant operators cannot be expected to bear the cost of security related overhead. A solution is the use of cameras monitoring the access points to two layered PSPs within the plant. During normal operation, security personnel can identify people entering the control room and unlock the 2nd entry point remotely. During a plant emergency, the doors should be hardwired to unlock and to fail open. Of course, plant operators should have a failsafe unlocking mechanism in the control room. There is a trade off related to physical security, between overburdening users or being overly invasive and being well protected. A balance needs to be achieved.

4.4.3.2. Protection of PSP Access Points

Various methods and tools are discussed in the following section. Remember, to always vary the use of tools and vendors across the primary PSP and secondary PSPs to make the plant more resistant to local attacks.

A. Limiting access to the Primary PSP via a DMZ

The DMZ limits, controls and monitors all access to any part of the operating plant. The DMZ usually takes the form of a gatehouse and surrounding barbed wired fence, followed by a long stretch of open area, followed by the actual plant. The idea of a physical DMZ is to give security staff time to respond to an unauthorized entry before the individual actual reaches the plant. Cameras monitoring the DMZ should be well placed, hidden and secured somehow (height, mounting the camera high without an access ladder, has proven to be an effective defense tactic).

After the accessing individual passes through the DMZ he should be allowed to access the plant using authentication or a security device, but preferably both. If the individual has not been to the plant before, he should be escorted for safety reasons.

B. Limiting access between Secondary PSPs

Physical access to any secondary PSP through any access point should only be permitted using two factor authentication. Log all access events. Monitor, detect, and alarm all attempts and actual unauthorized access events continuously and electronically when practical. Provide remote locking mechanisms and an effective method to assess any situation. Be sure to protect all access points. All level 1, 2 and 3 cyber devices will need to be housed in secondary PSPs whether it is an enclosure or a room.

C. Limiting access between Devices and/or Tertiary PSPs

An example of a somewhat unidentified tertiary PSP could be locked cabinets between DCS modules, which are all usually lumped together inside a secure room or secondary PSP. Tertiary PSPs should only be defined for highest risk cyber devices and will need to be tailored to each system. No more discussion is provided.

D. Devices used for the Access, Control and Monitoring of ESPs & PSPs

In-depth discussion of how to secure physical access control devices is outside the scope of this paper and somewhat poorly documented. However, these systems need to be well protected and typically are classified as level 2 or 3 cyber devices, depending on how the organization decides to interpret the questions. These devices do deserve well thought-out and somewhat clever security strategies.

4.4.3.3. Protection of cyber devices

When determining how to physically protect cyber devices, classifications can play a key role. The classifications outlined in section 4.4.1 are intended for large industrial facilities. When security controls are applied, apply them in a layered approach but try to maintain some continuity at each layer.

A. Applying protections to devices

When applying physical protections to devices, they should be grouped in some fashion, for example, to allow the entire DCS system to be in locked cabinets inside a secure room. As many devices as is possible should be included by default, including devices that happen to be nearby. Generally speaking all plant level 1, 2 and 3 PCs and Servers will need to be in a locked room and/or cabinet. Ideally, these devices should have enclosure locks. Network switches are often unlocked; this is a mistake. Lock all level 1, 2 and 3 network switches in a locked cabinet at a minimum and close all unused ports, preferably with a physical and virtual lock. Printers should either be locked in a room (which is usually impractical) or secured in a larger facility, such as a secured office complex, and put in a high traffic area so workers can detect suspicious activity. All PLCs regardless of the level need to be locked inside an enclosure and, whenever possible, inside a secured room. All recorders, relays and similar Ethernet devices should have some form of physical security. Currently, most do not and there are not many solutions available. All devices used for access control and monitoring of PSPs and ESPs need physical protections.

B. Physical Hardening

The goal of physical security hardening is to mitigate the chances of a local attack by simple visible deterrents such as guard stations, barbed wire and security camera, to delay any impending attack with layered controls and strategies, and to strengthen or put mechanisms in place that will log and monitor access attempts and detect, alter and notify any attempts at unauthorized access or actual unauthorized access incidences.

Generally, one should only have to harden a room or enclosure once in the life of a plant, assuming it was secured and maintained. If the device is ever locally compromised successfully, the device should be redesigned to mitigate the risks associated with the same attack occurring twice. When deciding how to harden PSPs, the tradeoff between functionality and access and good security should be considered in the design. For example, authorized personnel should not be overly hindered by physical security obstacles in case of emergencies yet systems still need to be secured.

A prerequisite of physical security hardening is that all devices within the PSP must be identified and all unauthorized or unjustifiable devices be removed. Asset management software can be used to track this data. The PSP needs to be as secure

as possible, often by using a well built 6 walled structure or a solid metal enclosure. Hardening an insecure room is pointless.

Area/Device Targets

Physical hardening targets may include rooms, enclosures, cabinets, control rooms, panels, etc; these are definitely not the only devices that need to be physically hardened, but they are devices that must not be missed. Whatever targets are chosen, realize that each class of targets presents unique design challenges.

Device classifications previously developed combined with area vulnerability estimates can play a key role in determining the order in which targets should be addressed and how much effort should be put into hardening them. These things need to be well thought out. It is similar to what the U.S. military did for planes during World War II. All planes returning from war would be inspected for bullet holes. If any bullet holes were found, they knew statistically that that particular spot on the plane did not require armoring (i.e. hardening), since the plane took the hit and made it back alive. For industrial control systems, the data set is not the same, however, the same principle applies, and data can be generated based on a theoretical worst case scenario, total system failure.

Ideally, a physical security engineer should be designing the system or perhaps an engineer with significant security experience with assistance from high level security personnel. These projects are not short lived or uncomplicated by any means; Speaking only in terms of orders of magnitude, a large power plant can have:

- Upwards of 50 computer or DCS rooms.
- Upwards of 50 PLC enclosures scattered throughout the plant, often unsecured.
- Visible wire ways, cable trays, conduits, etc. that are an easy target with little cost effective solution for remediation.
- Upwards of 100 HMIs scattered through the plant floor, often unsecured.
- A few dedicate server rooms for controlling access between the plant and other networks; *ideally, these should be controlled by the plant, not by administrators of the other networks*.
- Usually, there is one main control room for a single unit or two units sharing one control room, separated by a dividing line.

It is a pretty big project to physically harden the entire plant, and this is with the assumption that the physical structures (walls, rooms, etc) are built well enough to thwart or delay direct physical assault on the structure or segment the consequences of explosions, whether caused by accident or incident.

Subject Matters of Hardening Efforts

Subjects of hardening any particular target may include, but are not limited to:

- Security devices (locks and keys, cameras, intrusion detection systems, etc)
- Target hardening (deterring or delaying an attack focusing on a target area or target device)
- Hardening security for sensitive chemicals
- Damage mitigation (segmenting against physical attacks)
- Access point management(logging all authorized access and deterring, monitoring, alerting and responding to unauthorized access attempts)
- Environmental hardening (Lighting and inherent access deterrents)
- Security personnel policies (guard houses, patrols, etc.)
- Social engineering mitigation (control communications, training, etc.)

Each subject matter presents unique design challenges and will be discussed in the following paragraphs.

Security devices

Locks are acceptable devices to be used in adhering to physical protection requirements to assist in controlling access to areas, facilities, and materials through doors, gates, container lids, and similar material or personnel access points, and are considered essential components of a physical barrier. Locks may take a number of forms, some more secure than others; even considering a completely mechanical lock, ease of compromise varies greatly.

Mechanical locks are not “manipulation proof" and are either combination locks, key operated or electrically operated. These classes of locks are broken down into further subdivisions, considering design and construction factors. Studies about the security of mechanical locks have been done for centuries and are outside the scope of this paper. Magnetic locks are also typically encountered in certain facilities, but are not recommend because they usually fail open.

Cameras and microphones are critical to confirming an incident or identifying access by unauthorized individuals. It is highly recommended that all cameras installed be the pan, tilt, zoom (PTZ) type unless used for access control via facial recognition. The placing of cameras needs to be well thought out, considering whether or not the camera should be placed in a visible location as a deterrent, or hidden as an incidence recorder. Consideration should also be given to the security of the cameras, as discussed in section 4.4.3.3. The most cost effective method to monitor and respond to camera output is to put the system under the control of the primary PSP guardhouse, however, a second location internal to the plant is highly recommended. Camera outputs should be recorded and stored for a minimum of three months, but preferably longer. If an attack plan long in the making occurs, perhaps planned over the course of

a year, a longer retention period may prove useful in analyzing and reporting the attack. Redundant hard drive storage is the preferable method for storing security footage.

Intrusion detection systems (IDSs) should be used in conjunction with locks to deter, detect and alert and alarm unauthorized access attempts. IDSs use sensors to detect a change in an environment, processors to interpret the change, and output modules to alarm in case of incident detection. Sensors vary from motion detectors (e.g. electric field, infrared, microwave, laser, etc) to vibration or strain detectors; some systems even use cameras for face contour recognition. Alarms can be silent, auditory, or visual in most cases.

Additional examples of security devices include ID reader and access systems, biometric identification devices, keypads, tokens, or even remotely operated mantrap systems. Appropriate selection and placement of security devices is key to protecting the plant, and a full analysis and design process should be followed. The following are additional recommended sources to assist with the selection and placement of security devices:

- U.S. Atomic Energy Commission Regulatory Guide 5.12, “General use of locks in the protection and control of facilities and special nuclear materials”.
- U.S. Atomic Energy Commission Regulatory Guide 5.44, “Perimeter Intrusion Alarm Systems”.
- Barry Wels & Rop Gonggrijps (Toool Organization), Bumping locks, Last revision: January 26, 2005.
- The Open Organization Of Lock-pickers: http://www.toool.nl/
- http://www.wired.com/threatlevel/2009/08/electronic-locks-defeated/

Target hardening & Damage mitigation

Target hardening is a term mainly used by high level physical security experts or counter terrorism agents. Its goal is to deter or delay an attack focusing on a target area or a target device. Target hardening usually involves visible defenses for deterring potential attacks. Physical target hardening is usually analogous to surface area reduction for electronic devices previously discussed in section 4.4.2.3B. In regards to a power plant, target hardening should involve implementing security controls and strengthening physical structures for an area or device for the purposes of mitigating or segmenting any damage caused by local attacks.

Hardening security for sensitive chemicals

Power plants often use toxic or chemically explosive substances, which are required by plant systems. Large quantities of these substances are on site, often in giant tanks inappropriately located within the DMZ (i.e. accessible without entry into the primary PSP or plant). Some of these substances are already controlled under environmental protection laws, but often with little to no consideration for physical and/or electronic

security. For example, urea and ammonia is used in large quantities for pollution control in fossil plants and is extremely explosion when mixed with nitrate. Other chemicals that are toxic can be released killing people (examples of non-cyber related incidents would be the Bhopal disaster or the Halifax explosion). Whenever possible, tanks containing potentially explosive or toxic chemicals should be housed within a 6 walled enclosure. Usually, placement within the plant is sufficient if the primary PSP is well controlled.

The NRC limits maximum amount of fissile material and "special nuclear material" (SNM) allowed on site, and regulates specific requirement for how all material is stored and handled; see U.S. Atomic Energy Commission Regulatory Guide 5.42, "Design considerations for minimizing residual holdup of special nuclear material in equipment for dry process operations". It should be noted that there is currently a bit of over exaggerated fear related to the consequences of a nuclear plant compromise (i.e. a nuclear explosion). An attack who's aim is to cause a nuclear explosion with the material on site would fail; the material has not been enriched to the needed level to obtain critical mass, so it would effectively take a hydrogen bomb (which would be a much larger explosion to worry about) to cause a cascading reaction. Also, the theft of nuclear material simply isn't feasible; a nuclear fuel assembly weighs between 700 and 1,500 pounds[16], and all material housed on site whether in the reactor or in fuel storage is not easily moved due to the radiation hazards (at least for the next 100 years). There is vulnerability during fuel loading, but most of the risks associated with this have already been mitigated and the process is well controlled nationally.

Access point management

As already discussed and repeated here for effect, all access points to primary and secondary, and certain tertiary, PSPs should monitor and log all access attempts continuously (24/7) and electronically to avoid human error. Devices used for this purpose must be able to effectively detect, alert, alarm, notify and often react to attempts at and actual unauthorized access attempts. This is called access point management and the tools necessary to accomplish these goals have already been discussed in previous sections. Two factor authentication, as discussed previously, is always recommended.

Environment hardening

Environment hardening is the process of strengthening everything that is common to the plant as a whole. The environment includes the ground, the raw water supply, trees, the air we breathe and everything in-between. Initially, one might ask how such factors can be controlled, but the goal will become clear. Environment hardening is inherently more difficult on a plant that is already constructed, as opposed to a plant in

[16] Nuclear Energy Institute, NEI. Nuclear Power Plant Fuel. 2010. NEI. http://www.nei.org/howitworks/nuclearpowerplantfuel/.

the design phase of its life. This is because the environment around a constructed plant has already been defined, often 50 years ago or more, and modification costs would simply be higher compared to hardening on an unconstructed site.

Lighting is an important part of environmental hardening. The entire area contained in the DMZ, the barb wired fence encompassing the plant, should be effectively illuminated. Any internal or external areas monitored by cameras will, of course, require lighting. All PSP access points require effective lighting, whether primary, secondary or tertiary, whether an enclosure or a room.

One environmental hardening technique is designing the plant in such a way that, if there is a release of toxic chemicals, there is little to no danger of those chemicals being released into a water way. Another technique would be to level the ground within the DMZ and remove all vegetation to increase observation range. Consider strategically placing vegetation as either obstacles to overcome or as obvious hiding points for an attack (obvious being the keyword, so that area is protected the most). Design roads that are lined with large trees that wind while approaching the plant to give the plant more time to respond to a suspiciously approaching vehicle. Environmental hardening serves its purpose well.

Security personnel policies

Policies relating to security personnel are also important. These policies dictate how a plant is monitored, patrolled and access controlled. They dictate how security recordings and records are handled, maintained and stored. Patrol schedules should be adhered to, but they should change on a regular basis. The gatehouse, obviously, should not be left unguarded.

Social engineering mitigation

Mitigating social engineering attacks on an industrial scale is difficult and the consequences of failing to do so are high. Too many people are involved in constructing, operating and maintaining these colossal constructs. The best that can be hoped for is effective and evolving training and qualified and intelligent employees. Communication control is an effective strategy, but can only be applied sparingly. One of the best ways to mitigate social engineering is to have an inherent security culture where everyone is aware of the threat and is held accountable if unauthorized information is disclosed. Accountability also encourages erring on the side of safety, and verifying what information employees are allowed to disclose prior to disclosing it.

4.4.4. Security Reviews/Audits

Security reviews and penetration testing should be performed annually, at a minimum. The process of penetration testing will include a simulation of attacks on all ESPs and the DMZ using known hardware and software vulnerabilities, testing for incorrect

configuration or inadequate hardening, and any other potential weaknesses in existing processes.

In addition to the periodic security review cycle, vulnerability databases should be monitored continuously for newly discovered security flaws. Publicly available resources like the National Vulnerability Database operated by the NIST (http://nvd.nist.gov) and the Open Source Vulnerability Database (http://odvdb.org) are valuable resources for keeping up to date with emerging security threats. Tools to assist in vulnerability assessments were discussed in section 4.4.2.3B.

The review should include the following steps at a minimum the results of which should be documented and preserved indefinitely for future audits.

- Evaluate all existing physical and electronic access points and verify that no new unauthorized or undocumented access points have been added. Confirm that all ESPs and PSPs are still in place and operating as intended.
- Review all physical, electronic and informational user accounts for unauthorized changes to account information, access rights and account passwords. Verify all account information is current, and no obsolete or unused accounts exist. Ensure levels of access for all users are still appropriate for user responsibilities.
- Confirm hardening policies remain in place and are effective. This can be accomplished through the use of scanning software like Nmap, Zenmap or Nessus which can identify information about networks or devices, open ports, running services, and firewall status. As previously discussed, care must be taken when using software of this type on a live system to ensure that it will not interfere with running processes.
- Ensure the master list of cyber devices is up to date.
- Verify that all procedures of the cyber security plan are being followed as intended and the no modification to procedures or policies is required.

In the case that a vulnerability is discovered in the course of an audit, remediation of the vulnerability should take place immediately. All vulnerabilities should be treated as SC process vulnerability = (confidentiality, high), (integrity, high), (availability, high). If a vulnerability cannot be remediated an exception should be created and potential effects of the vulnerability should be mitigated to the best extend possible. Remediation should include the following considerations.

- Temporary measures should be taken to secure the system until permanent remediation is available.
- Patches are often available from the original equipment manufacturer (OEM) and should be considered if feasible.
- Patches should be obtained as soon as possible and documented including the procedure for installing the updates. The entire patching process and the patch itself should be tested in a lab environment before installation into the live environment to test for effectiveness and any possible interferences or side effects.

- Update any existing documentation and procedures to incorporate changes made by the remediation. Ensure all system users are aware of these changes. Rescan for configuration data and backups and ensure all active ports, programs and services have a valid justification.

4.4.5. Incident Response Planning

Incidence response plan, also known as an emergency response plan, should be developed and should include a list of all level 1, 2 and 3 devices and associated validated recovery plans and additional response action plans. Details and contact information for whom to report the incident to and the conditions for considering an incident reportable should be defined. All data associated with an incident should be considered SC industrial incident = (confidentiality, high), (integrity, high), (availability, high). All data pertaining to an incident should be kept indefinitely.

Roles and responsibilities of key response personnel need to be clearly defined and personnel need to understand and be prepared for their role; they will not have time to consult a procedure to determine where they are supposed to be if there is an emergency. This is why technical and specialized cyber security training and drills are required. Drills should occur at least once during every outage. If the control system is robust enough, live simulations may be appropriate. Drills should include, but are by no means limited to, incident response, immediate analysis followed by mitigation, backup restoration and perhaps even partial evacuation.

"Awareness" training needs to occur regularly within the entire organization; this usually takes the form of monthly emails, posters, appropriate use banners and perhaps "lunch and learns" on the subject. Additionally, employees are required to annually train on policies, which is usually followed by a simple test. This can have a positive effect on security, but often policies are not enforced so the training can be a moot point. Ideally, all employees on the site should be trained in the organizations security objectives, common attack methodologies, common signs of attack and how to respond. The following guides are recommended to assist in developing response plans:

- NIST SP800-61, "Computer Security Incident Handling Guide"
- NIST SP800-86, "Guide to Integrating Forensic Techniques into Incident Response"

5. Case Study: Security Flaws and Mitigation of a PLC

An additional topic discussed during the presentation of this paper at DEFCON 18 was a physical example of the security flaws of a discrete PLC from an undisclosed manufacturer, and the consequences therein. A generic Ethernet capable model frequently found on the plant floor was selected; various attack scenarios were demonstrated for the systems commonly run by the device. The demonstration was not intended to expose any single vulnerability on the selected device; the demonstration was intended to convey a sense of urgency in remediating

security flaws and replacing devices with inherently lax security because there is currently an opportunity to prevent a disaster before it occurs. For additional information, check the DEFCON 18 speaker content page for the full presentation.

6. Conclusions

Although focused mainly on the power industry, the same techniques are valid for nearly any type of large industrial plant. Many sectors are beginning to leisurely become acquainted with a world where cyber security is truly a necessary field; this includes government, utilities, industry, manufacturing, food production, and other large scale operations. The current languid and often idle pace is understandable; risks and threats are increasing, vulnerabilities are often dealt with ineffectively, yet there haven't been any major incidences so the **perceived** danger is low. This misperception was hopefully alleviated for the reader by seeing security flaws inherent in process control networks and devices, by seeing both theoretical and real world examples of vulnerabilities and attack scenarios that could be exploited locally or remotely (intentionally or unintentionally) and by examining a generally bleak security situation. It should be clear to the reader that a modern power plant needs to be built with security as a primary goal, with security inherent in the design.

Policies required to meet these demands are currently often weak, unenforced or predictable and may need significant modification by subject matter experts. Distinct procedures and processes for managing both the electronic and the physical security of a large industrial facility were presented as well as how to manage associated change, working policies into existing procedures whenever possible. Governances were briefly discussed; the reader should take away an understanding of the complexity of compliance and an understanding of the need to simplify and quantify overlapping requirements by creating effective and distinct policies and procedures, automating whenever possible.

The defense-in-depth military tactic & strategy should be applied liberally to systems via projects, operations and maintenance using some form of every electronic and physical security hardening subject previously discussed on all levels of security. The reader should now have an understanding of the importance of designing a coherent, comprehensive, open ended and easily automatable method for the classification of sites, systems and devices based on severity of attack, likeliness of attack and ease of attack as well as the categorization of information. The reader should fully understand how classifications can be used to their advantage to provide cost savings and mitigate highest risk first. The methods, techniques and tools for mitigation of risk on all levels were presented, and the importance of varying these tactics should be clear. Due to the high risk to the plant and the bulk electric system, and large scope of any compliance effort, it is far better to set a goal of exceeding compliance using automated systems rather than meeting compliance using manual labor intensive methods; this is the only real approach to guarantee compliance and effectively maintain a coherent security strategy.

The challenge is great, the risks are great, and choices need to be made. In order to effectively secure our grid, we will need leadership and continuity from the top down of the

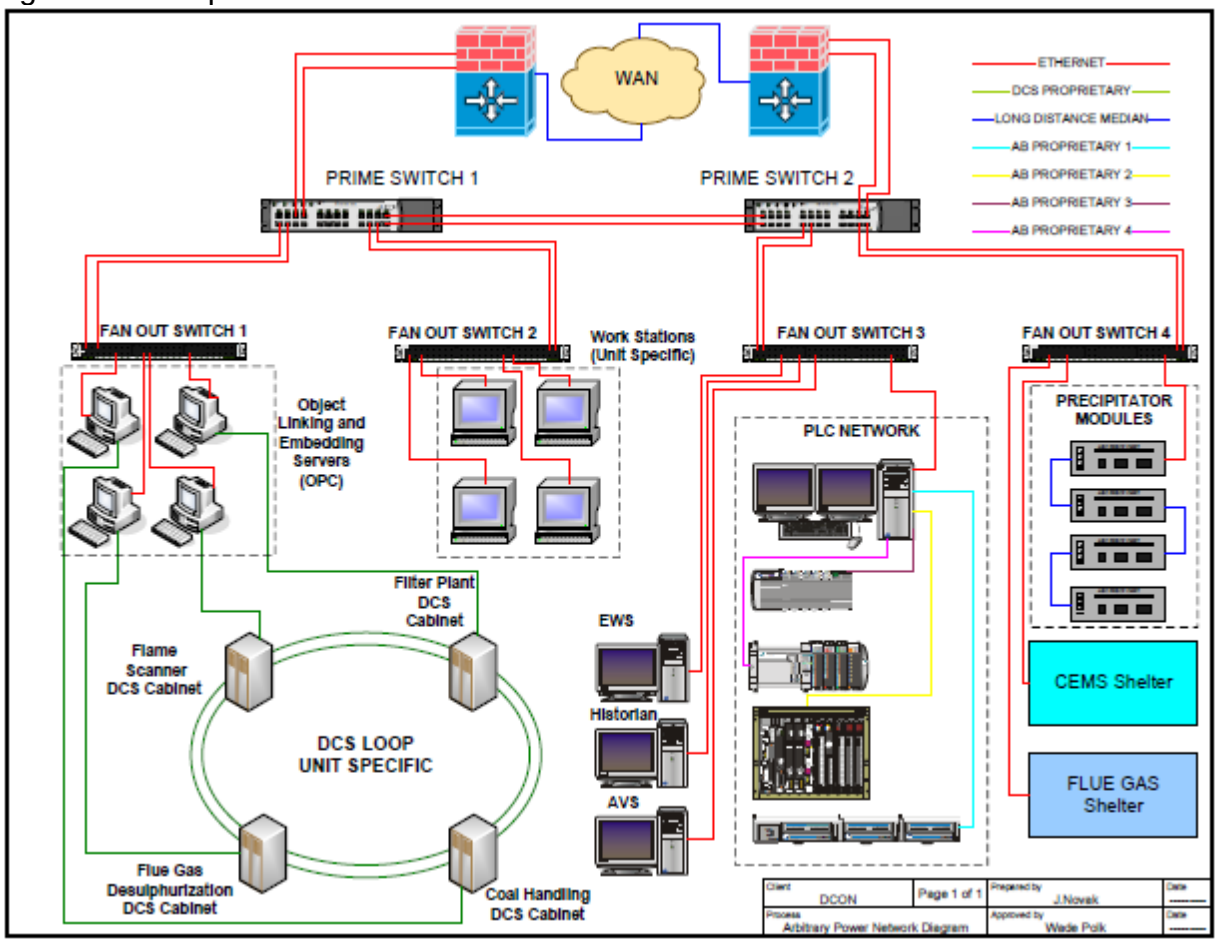
government's chain of command as well as from the top down of the power sector's chain of command. We need to close the divide between the IT world and the industrial world. The risks are increasing continuously, as they always do as technology progresses. The paper was not intended to expose any single vulnerability on any given site; the paper was intended to convey a sense of urgency in remediating systemic security flaws and replacing devices with inherently lax security because there is currently an opportunity to prevent a disaster before it occurs. With a concentrated effort and increased awareness, the security of the control systems in an industrial plant can be brought to up to the standard deserving of the nation's most important infrastructure, and it's time we do so.

"The release of atom power has changed everything except our way of thinking...the solution to this problem lies in the heart of mankind. If only I had known, I should have become a watchmaker."

-Albert Einstein

7. Appendix A: Examples

1. Drawing Example: typical, simplified and reduced control network diagram prior to any significant compliance efforts.



2. Sites List: factious facilities list and associated properties.

Site Name	Location	Address	Type	Peak Load	Contact Info	Q0	Classification
Twin Peaks Power	Twin Peaks, WA	123 Red Rum Way	Coal	100 MW	Dale Cooper Plant Manager 314-159-2652	NO	Non-Critical Site
Springfield Nuclear	Springfield, USA	742 Evergreen Terrace	Nuclear	2,000 MW	Homer Simpson Plant Manager 555-555-5555	YES	Critical Site
Gotham Sub-Station	Gotham, NY	777 Fake St	Sub-Station		Bruce Wayne Station Operator 800-588-2300	YES	Critical Site
Disney Power	Disneyland, USA	111 Fun Blvd	Dwarf Bio-Mass	1,200 MW	Mickey Mouse Plant Manager 123-456-7890	NO	Non-Critical Site
South Park Power	South Park, CO	900 Mr. Hanky's Way	Smug	2,000 MW	Eric Cartman Safety Coordinator 867-5309	YES	Critical Site

3. Systems List – approximately realistic systems list (5% of the list is shown)

System Name	Description	Contact Info	Q1	Q2	Classification
DCS	Coordinates Controls of all Sub Systems, distributed device.	Ed Vedder Plant Operations 777-6666-5000	YES	YES	Critical Cyber System
Boiler Feed Water	Main feed water to steam generator, only indicating devices.	Tim Timson Water Maintenance 777-666-5570	YES	YES	Critical Cyber System
Instrument Air	Supplies all instrument air to the plant, via 2 redundant systems, local unsecured panel	Tim Timson Water Maintenance 777-666-5570	YES	YES	Critical Cyber System
Raw Water Supply	Primary and redundant systems, local operator station	Tim Timson Water Maintenance 777-666-5570	YES	YES	Critical Cyber System
SNCR	Pollution Reduction	Bill Billson Boiler Maintenance 777-666-5540	YES	NO	Non- Critical Cyber System
CEMS	Continuous Emissions Monitoring Equipment	Bill Billson Boiler Maintenance 777-666-5540	YES	NO	Non- Critical Cyber System
Mercury Baghouse	Mercury pollution reduction system via carbon injection	Bill Billson Boiler Maintenance 777-666-5540	YES	NO	Non- Critical Cyber System
Air Preheaters	Mechanically driven heat exchangers	Bill Billson Boiler Maintenance 777-666-5540	NO	YES	Critical Non-Cyber System

4. Devices List – approximately realistic device list (10% of the list is shown)

Tag	Unit	Type	Mfr.	Model	OS	# Ports	IP	Host Name	Description	Location	Physical Security	Physical Security Type	Protocols	Protocol Type	Site	System	Q3	Q4	Q5	Classification
1-691-PC-002	1	Work Station	HP	PowerStation	Windows 7	3	192.168.5.510	EWS1	Unit 1 Engineering Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	NO	YES	NO	Level 3 Critical Cyber Device
2-692-PC-002	2	Work Station	HP	PowerStation	Windows 7	3	192.168.6.510	EWS8	Unit 2 Engineering Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	NO	YES	NO	Level 3 Critical Cyber Device
3-693-PC-002	3	Work Station	HP	PowerStation	Windows 7	3	192.168.7.510	U3EWS1	Unit 3 Engineering Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	NO	YES	NO	Level 3 Critical Cyber Device
1-585-PLC-001	1	PLC	CEMCO	ABC123	Prop OS	4	192.168.5.460	CEMS1	Unit 1 Stack CEMS	CEMS Shelter	YES	Locked	TCP	Routable	TPP	CEM System	NO	YES	YES	Level 2 Critical Cyber Device
2-585-PLC-001	2	PLC	CEMCO	ABC123	Prop OS	4	192.168.6.460	CEMS3	Unit 2 Stack CEMS	CEMS Shelter	YES	Locked	TCP	Routable	TPP	CEM System	NO	YES	YES	Level 2 Critical Cyber Device
3-585-PLC-001	3	PLC	CEMCO	ABC123	Prop OS	4	192.168.7.460	U3CEMS1	Unit 3 Stack CEMS	CEMS Shelter	YES	Locked	TCP	Routable	TPP	CEM System	NO	YES	YES	Level 2 Critical Cyber Device
1-218-PLC-001	1	PLC	Electro Equip	Mini-PLC	ElectroOS	1	192.168.5.400	PLC1	Unit 1 Deaerator PLC	Deaerator	NO	NA	Profibus	Non-Routable	TPP	Deaerator System	YES	NO	NO	Level 3 Critical Cyber Device
2-218-PLC-001	2	PLC	Electro Equip	Mini-PLC	ElectroOS	1	192.168.6.400	2_Deaerator	Unit 2 Deaerator PLC	Deaerator	NO	NA	Profibus	Non-Routable	TPP	Deaerator System	YES	NO	NO	Level 3 Critical Cyber Device
3-218-PLC-001	3	PLC	Electro Equip	Mini-PLC	ElectroOS	1	192.168.7.400	U3PLC1	Unit 3 Deaerator PLC	Deaerator	NO	NA	Profibus	Non-Routable	TPP	Deaerator System	YES	NO	NO	Level 3 Critical Cyber Device
1-691-PC-200	1	OPC Server	HP	PowerServer	Windows 7	2	192.168.5.200	OPC1	Unit 1 OPC Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	NO	YES	Level 2 Critical Cyber Device
2-692-PC-200	2	OPC Server	HP	PowerServer	Windows 7	2	192.168.6.200	OPC2	Unit 2 OPC Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	NO	YES	Level 2 Critical Cyber Device
3-693-PC-200	3	OPC Server	HP	PowerServer	Windows 7	2	192.168.7.200	U3OPC1	Unit 3 OPC Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	NO	YES	Level 2 Critical Cyber Device
9-691-SWT-001	9	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.1.100	DMZ1	Plant DMZ Switch 1	Electrical Equipment Room	YES	Cabinet Pad Lock	Fiber over TCP	Routable	TPP	Plant Network	YES	YES	YES	Level 1 Critical Cyber Device
9-691-SWT-002	9	Network Switch	3COM	8800	3COM OS	16	192.168.1.110	DMZ2	Plant DMZ Switch 2	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP	Routable	TPP	Plant Network	YES	YES	YES	Level 1 Critical Cyber Device
9-691-SWT-003	9	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.1.120	DMZ3	Plant DMZ Switch 3	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP	Routable	TPP	Plant Network	YES	YES	YES	Level 1 Critical Cyber Device
9-691-SWT-004	9	Network Switch	3COM	8800	3COM OS	16	192.168.1.130	DMZ4	Plant DMZ Switch 4	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP	Routable	TPP	Plant Network	YES	YES	YES	Level 1 Critical Cyber Device
9-228-PLC-001	9	PLC	WTRKlee n	3200	Prop OS	4	192.168.1.200	WT-SRV	Water Treatment System	Water Treatment Bldg	YES	cameras	TCP, Profibus	Routable	TPP	Water Treatment	YES	YES	YES	Level 1 Critical Cyber Device
1-691-DCS-001	1	DCS	Electro Equip	Kflex	ElectroOS	2	192.168.5.120	1DCS_A	Unit 1 DCS Cabinet	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-PC-001	1	Work Station	HP	PowerStation	Windows 7	3	192.168.5.500	OW1	Unit 1 Operator Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-PC-003	1	Work Station	HP	PowerStation	Windows 7	3	192.168.5.520	SWS1	Unit 1 Supervisor Workstation	Office 100	YES	RFID	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-PC-010	1	DAS	HP	PowerServer	Windows 7	2	192.168.5.600	DASRV1	Unit 1 Data Acquisition Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-SWT-001	1	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.5.100	SW1	Fan Out Switch 1	Control Pulpit A	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-SWT-002	1	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.5.110	SW2	Fan Out Switch 2	Control Pulpit B	NO	NA	Fiber overTCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-691-SWT-003	1	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.5.130	SW3	Fan Out Switch 3	Control Pulpit C	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
1-446-PLC-001	1	PLC	BoilerMa ker	HMI2000	BM 3.2	1	192.168.5.410	BoilerCntl	Unit 1 Boiler Controller	Boiler Room	NO	NA	Profibus	Non-Routable	TPP	Boiler System	YES	YES	YES	Level 1 Critical Cyber Device
1-491-PLC-001	1	PLC	GE	GE7600	GE Turb	3	192.168.5.420	STC1	Unit 1 Steam Turbine Control	Turbine Control Room	NO	NA	Profibus	Non-Routable	TPP	Steam Turbine	YES	YES	YES	Level 1 Critical Cyber Device
2-692-DCS-001	2	DCS	Electro Equip	Kflex	ElectroOS	2	192.168.6.120	DCS3	Unit 2 DCS Cabinet	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-PC-001	2	Work Station	HP	PowerStation	Windows 7	3	192.168.6.500	OW4	Unit 2 Operator Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-PC-003	2	Work Station	HP	PowerStation	Windows 7	3	192.168.6.520	SWS2	Unit 2 Supervisor Workstation	Office 100	YES	RFID	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-PC-010	2	DAS	HP	PowerServer	Windows 7	2	192.168.6.600	DASRV2	Unit 2 Data Acquisition Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-SWT-001	2	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.6.100	SW9	Fan Out Switch 1	Control Pulpit A	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-SWT-002	2	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.6.110	SW8	Fan Out Switch 2	Control Pulpit B	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-692-SWT-003	2	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.6.130	SW6	Fan Out Switch 3	Control Pulpit C	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
2-446-PLC-001	2	PLC	BoilerMa ker	HMI2000	BM 3.2	1	192.168.6.410	2-BCPLC	Unit 2 Boiler Controller	Boiler Room	NO	NA	Profibus	Non-Routable	TPP	Boiler System	YES	YES	YES	Level 1 Critical Cyber Device
2-492-PLC-001	2	PLC	GE	GE7600	GE Turb	3	192.168.6.420	2-STC	Unit 2 Steam Turbine Control	Turbine Control Room	YES	cameras	Profibus	Non-Routable	TPP	Steam Turbine	YES	YES	YES	Level 1 Critical Cyber Device
3-693-DCS-001	3	DCS	Electro Equip	Kflex	ElectroOS	2	192.168.7.120	DCS7	Unit 3 DCS Cabinet	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus,	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-PC-001	3	Work Station	HP	PowerStation	Windows 7	3	192.168.7.500	U3OWS2	Unit 3 Operator Workstation	Main Control Room	YES	cameras	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-PC-003	3	Work Station	HP	PowerStation	Windows 7	3	192.168.7.520	U3SWS1	Unit 3 Supervisor Workstation	Office 100	YES	RFID	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-PC-010	3	DAS	HP	PowerServer	Windows 7	2	192.168.7.600	U3DASRV	Unit 3 Data Acquisition Server	Electrical Equipment Room	YES	Cabinet Pad Lock	TCP, Profibus	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-SWT-001	3	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.7.100	FO_SW1	Fan Out Switch 1	Control Pulpit A	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-SWT-002	3	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.7.110	FO_SW2	Fan Out Switch 2	Control Pulpit B	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-693-SWT-003	3	Network Switch	Cisco	KEX-142	Cisco IOS	16	192.168.7.130	FO_SW3	Fan Out Switch 3	Control Pulpit C	NO	NA	TCP	Routable	TPP	Control System	YES	YES	YES	Level 1 Critical Cyber Device
3-493-PLC-001	3	PLC	GE	GE7600	GE Turb	3	192.168.7.420	U3TC	Unit 3 Steam Turbine Control	Turbine Control Room	NO	NA	Profibus	Non-Routable	TPP	Steam Turbine	YES	YES	YES	Level 1 Critical Cyber Device
3-446-PLC-001	3	PLC	BoilerMa ker	HMI2000	BM 3.2	1	192.168.7.410	U3BC	Unit 3 Boiler Controller	Boiler Room	NO	NA	serial	Non-Routable	TPP	Boiler System	YES	YES	YES	Level 1 Critical Cyber Device

8. Special Thanks

Special thanks to the reviewers who took time out of their busy schedules to review this paper before its completion, to the experts who provided input and to the others who contributed in other ways. We value their feedback and support tremendously: Barry Kimsey, Randall Iserman, and Dave Schlessman.

9. Contact Information

Wade Polk
Controls Engineering & Industrial Cyber Security
Winthrop.polk@worleyparsons.com
Phone (direct): 423-785-5467
Cell: 850-292-9333
Fax: 423-757-5869

Jaroslav Novak
Controls Engineer & Startup Engineer
jaroslav.novak@worleyparsons.com
423-785-5464 (OFFICE)
423-757-5869 (FAX)

Paul Malkewicz
Controls Engineering & Industrial Cyber Security
Paul.malkewicz@worleyparsons.com
Phone (direct): 708-449-4165

10. Definitions

- BOM: Bill of Materials, a list of items included as part of a package
- CAP: Corrective Action Program gives requirements for identifying, reporting, evaluating and correcting problems with a plant.
- CIP: Critical Infrastructure Protection, standards created by the North American Electric Reliability Corporation to regulate non-nuclear power plants.
- Device: Usually refers to a device in the lowest level of automation, either a sensor or a control valve. See Also Cyber Device.
- Control System: A set of devices used to automate the operation of processes and pieces of equipment.
- Cyber Device (Subjective Definition): A programmable electronic device whose primary programming interface is not implemented using a local non electronic method such as a keypad.
- DCS: Distributed Control System, a type of control device whose components are typically distributed throughout a plant, but work together to control a process. DCSs usually include PC based HMIs.
- Defense In Depth: A security strategy for slowing down or stopping an attack. Defense in Depth assumes one or more security precautions will fail and implements one or more layers of back-up precautions.
- DMZ: Demilitarized Zone, a portion of a plant's network which connects an untrusted zone to a trusted zone.
- ESP: Electronic Security Perimeter, a virtual enclosure around a critical digital asset. Access to and from the ESP is carefully monitored and controlled.
- Hardening: ensuring that only those ports, programs, and services required for normal and emergency operations are enabled, ensuring the security policies are met and to add or strengthen security mechanisms (e.g. virus protection) to result in a more secure system than initial examination revealed. Hardening can be both physical and electronic.
- HMI: Human Machine Interface, a device which allows an operator to communicate with and receive feedback from a system by means of reading from or sending information to the system.
- IDPS: Intrusion Detection and Prevention Software, a system that monitors for unusual, malicious or unauthorized activity and reports.
- NERC: North American Electric Reliability Corporation, organization which provides standards for and oversight of the operation of power plants in North America.
- NIST: National institute of Standards and Technology, government organization which creates standards for a number of topics and fields.
- NRC: Nuclear Regulatory Commission, body governing the operation of nuclear power plants in the United States.
- OPC: OLE for Process Control, a set of standards for communication between automation devices in an industrial plant.

- PLC: Programmable Logic Controller, a device capable of performing control output based on given inputs and a programmed set of sequential logic.
- PSP: Physical Security Perimeter, a physical enclosure around a critical area or asset. Access to and from the PSP is carefully monitored and controlled
- SCADA: Supervisory Control and Data Acquisition, typically higher level control devices which coordinates between several processes and displays and records information about the operation of the entire plant.
- Surface Area Reduction: A type of hardening for electronic devices that involves removing unnecessary software and services and shutting down unused ports.
- Trusted Zone: The portion of a network where communications are assumed to be safe.
- Untrusted Zone: The portion of a network where communications are assumed to be unsafe.

11. Bibliography

1. ANSI/ISA. NSI/ISA-88.01-1995, Batch Control, Part 1: Models and Terminology. Research Triangle Park, North Carolina: The Instrumentation, Systems and Automation Society, 1995.

2. Bridis, Ted. "Government video shows mock hacker attack." MSNBC. 26 Sep. 2007: http://www.msnbc.msn.com/id/21000386/%3E..

3. Center for Strategic and International Studies. Securing Cyberspace for the 44th Presidency. Washington: GPO, 2008.

4. Computer Security Division, National Institute of Standards and Technology (NIST). FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: Federal Information Processing Standards (FIPS), 2004.

5. Computer Security Division, National Institute of Standards and Technology (NIST). FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems. Gaithersburg, MD: Federal Information Processing Standards (FIPS), 2006.

6. Computer Security Division, National Institute of Standards and Technology (NIST). NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2010.

7. Computer Security Division, National Institute of Standards and Technology. NIST Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2010.

8. G`orman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." Wall Street Journal April 8 (2009): http://online.wsj.com/article/SB123914805204099085.html.

9. Gary, Stoneburner, et al. NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2002.

10. Kent, Karen, et al. NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2006.

11. Liptak, Bela G. Instrument Engineers Handbook: Process Control and Optimization. Boca Raton, FL : CRC Press, 2006.

12. Lyon, Gordon. Security Tools. Nmap Developer. 2010. http://insecure.org/.

13. Lyon, Gordon. Top 100 Security Tools. Nmap Developer. 2010. http://sectools.org/.

14. Mell, Peter, et al. NIST Special Publication 800-40: Creating a Patch and Vulnerability Management Program and Organizations. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2005.

15. Minkel, JR. "The 2003 Northeast Blackout--Five Years Later." Scientific American. 13 Aug. 2008: http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later.

16. Mojain, Dan. "Hackers Victimize Cal-ISO." Los Angeles Times. 9 Jan. 2001: http://articles.latimes.com/2001/jun/09/news/mn-8294.

17. North American Electric Reliability Corporation, NERC. CIP-001a: Sabotage Reporting. Washington, DC : NERC, 2010.

18. North American Electric Reliability Corporation, NERC. CIP-002-3: Critical Infrastructure Protection. Washington, DC : NERC, 2009.

19. North American Electric Reliability Corporation, NERC. CIP-003-3: Security Management Controls. Washington, DC : NERC, 2009.

20. North American Electric Reliability Corporation, NERC. CIP-004-3: Personnel & Training. Washington, DC : NERC, 2009.

21. North American Electric Reliability Corporation, NERC. CIP-005-3: Electronic Security Perimeter(s). Washington, DC : NERC, 2009.

22. North American Electric Reliability Corporation, NERC. CIP-006-3: Physical Security of Critical Cyber Assets. Washington, DC : NERC, 2009.

23. North American Electric Reliability Corporation, NERC. CIP-007-3:Systems Security Management. Washington, DC : NERC, 2009.

24. North American Electric Reliability Corporation, NERC. CIP-008-3: Incident Reporting and Response Planning. Washington, DC : NERC, 2009.

25. North American Electric Reliability Corporation, NERC. CIP-009-3: Recovery Plans for Critical Cyber Assets. Washington, DC : NERC, 2009.

26. Nuclear Energy Institute, NEI. Nuclear Power Plant Fuel. 2010. NEI. http://www.nei.org/howitworks/nuclearpowerplantfuel/.

27. Nuclear Regulatory Commission, United States. "NRC Issues Information Notice On Potential Of Nuclear Power Plant Network To Worm Infection." Office of Public Affairs. 2 Sep. 2003: http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html.

28. RISI. 2009 Report on Control System Cyber Security Incidence Released. 30 Mar. 2010. Repository of Industrial Security Incidents (RISI). http://www.securityincidents.org/members/news.asp?ID=13.

29. Ross, Ron, et al. NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2009.

30. Scarfone, Karen, et al. NIST Special Publication 800-61: Computer Security Incident Handling Guide. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2008.

31. Singel, Ryan. "Industrial Control Systems Killed Once and Will Again, Experts Warn.." Wired. 9 Apr. 2008: http://www.wired.com/threatlevel/2008/04/industrial-cont/.

32. Smith, Randy. Windows Security Setting Guidance. Monterey Technology Group, Inc. 2010. http://www.ultimatewindowssecurity.com/wiki/WindowsSecuritySettings/.

33. Sparks, Charles "Black Viper". Black Viper's Web Site. 2010. http://www.blackviper.com/.

34. Stine, Kevin, et al. NIST Special Publication 800-60 Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2008.

35. Stine, Kevin, et al. NIST Special Publication 800-60 Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2008.

36. Stouffer, Keith, et al. NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security. Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2008.

37. The White House. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington: GPO, 2009.

38. Toool, The Open Organization of Lockpickers. Homepage. 2009. http://toool.us/.

39. United States Atomic Energy Commission. Regulatory Guide 5.12: General Use of Locks in the Protection and Control of Facilities and Special Nuclear Materials. Washington: GPO, 1973.

40. United States Atomic Energy Commission. Regulatory Guide 5.42: Design Considerations for Minimizing Residual Holdup of Special Nuclear Materials in Equipment for Dry Process Operations. Washington: GPO, 1975.

41. United States Nuclear Regulatory Commission (NRC) Regulations. 10 CFR Title 10, Code of Federal Regulations. Washington: GPO, 2010.

42. United States Nuclear Regulatory Commission (NRC) Regulations. Regulatory Guide 5.71: Cyber Security Programs For Nuclear Facilities. Washington: GPO, 2010.

43. United States Nuclear Regulatory Commission (NRC) Regulations. Regulatory Guide 5.44: Perimeter Intrusion Alarm Systems. Washington: GPO, 1997.

44. Wels, Barry and Rop Gonggrijp. Bumping Locks. http://www.toool.nl/bumping.pdf: Tool-The Open Organization Of Lockpickers, 2005.

45. Zetter, Kim. Electronic High-Security Locks Easily Defeated at DefCon. 2 Aug. 2009. Wired Magazine. http://www.wired.com/threatlevel/2009/08/electronic-locks-defeated/.

46. Ziegler, Kelly. "Blackout's 5th Anniversary Marks Progress, New Challenges Ahead ." North American Electric Reliability Corporation (NERC). 14 Aug. 2008: http://www.nerc.com/news_pr.php?npr=142.