SCADA & PLC VULNERABILITIES IN CORRECTIONAL FACILITIES

White Paper

Teague Newman
Tiffany Rad, ELCnetworks, LLC
John Strauchs, Strauchs, LLC

7/30/2011

Abstract

On Christmas Eve not long ago, a call was made from a prison warden: all of the cells on death row popped open. Not sure how or if it could happen again, the prison warden requested security experts to investigate. Many prisons and jails use SCADA systems with PLCs to open and close doors. As a result of Stuxnet academic research, we have discovered significant vulnerabilities in PLCs used in correctional facilities by being able to remotely flip the switches to “open” or “locked closed” on cell doors and gates. Using original and publically available exploits along with evaluating vulnerabilities in electronic and physical security designs, we will analyze SCADA systems and PLC vulnerabilities in correctional and government secured facilities while making recommendations for improved security measures.

Biographies

John J. Strauchs, M.A., C.P.P., conducted the security engineering or consulting for more than 114 justice design (police, courts, and corrections) projects in his career, which included 14 federal prisons, 23 state prisons, and 27 city or county jails. He owned and operated a professional engineering firm, Systech Group, Inc., for 23 years and is President of Strauchs, LLC. He was an equity principal in charge of security engineering for Gage-Babcock & Associates and an operations officer with the U.S. Central Intelligence Agency (CIA). His company and work was an inspiration for the 1993 movie, “Sneakers” for which he was the Technical Advisor. He was a presenter at Hackers On Planet Earth (HOPE) in 2008 and DojoCon in 2010 and is a consultant for Recursion Ventures.

Tiffany Strauchs Rad, BS, MBA, JD, is the President of ELCnetworks, LLC., a technology development, law and business consulting firm with offices in Portland, ME and Washington, D.C. Her consulting projects have included business and technology development for start-ups and security consulting for U.S. government agencies. She is also a part-time Adjunct Professor in the computer science department at the University of Southern Maine teaching computer law, ethics and information security. Her academic background includes studies at Carnegie Mellon University, Oxford University, and Tsinghua University (Beijing, China). She has presented at Black Hat USA, Black Hat Abu Dhabi, Defcon 17 & 18, SecTor, HOPE, 27C3 and regional information security conferences.

Teague Newman, is an independent information security consultant based in the Washington, D.C. area with extensive penetration testing experience. In 2009, he competed in the Netwars segment of the US Cyber Challenge and ranked within the Top 10 in the US in all rounds in which he participated. He is also an instructor and penetration tester for Core Security Technologies and has instructed professionals on the topics of information security and penetration testing at places like NASA, DHS, US Army, US Marine Corps (Red Team), DOE, various nuclear facilities as well as for large corporate enterprises. His projects include GPU-based password auditing and liquid nitrogen overclocking.

Table of Contents

Introduction

Stuxnet has been a topic of professional and academic interest since its existence was discovered by Sergey Ulasen of VirusBlokAda on June 17, 2010.[i] Since then, computer security researchers have been sifting through its code in efforts to decipher its origins and functionality. While it was not the first malicious software to target automation systems, it was unique in that it exploited four zero-days and was the first to contain root kits specifically targeted for particular Siemens SCADA (Supervisory Control and Data Acquisition) systems. The attack on Iran's centrifuges was based on exploiting Siemens PLCs (programmable logic controllers). In particular, the attacks were on STEP 7, software for the controlling computer, used for programming the PLCs. Microsoft states that patches MS08-067, MS10-046, and MS10-061 for Windows may have fixed the vulnerabilities that allowed STEP 7 to be attacked.[ii]

Although PLCs have been around for more than 40 years, until Stuxnet, few security research projects were focused on them. PLCs were originally developed in the 1960s to facilitate industrial automation. Many PLCs in use today utilize a simple programming language called Ladder Logic to make it easier to program them. Fortunately, or unfortunately—depending upon one's perspective—the simple and basic nature of PLCs makes them exceptionally vulnerable to being exploited.

The ease with which programming PLCs can be done is one of the reasons why many in the computer security research community have now shifted their focus upon where and how PLCs are used. So far, the focus has primarily been on large SCADA systems and the use of PLCs in critical infrastructure such as in manufacturing plants, power grid, pipelines, water systems, and so forth.

Our research analyzes PLC usage and vulnerabilities that has escaped attention because most people know very little about PLCs in correctional facilities.[iii] Understanding the electronic, physical and computer security designs in correctional facilities will outlines why PLCs were implemented in many jails and prisons and elucidates their requisite vulnerabilities.

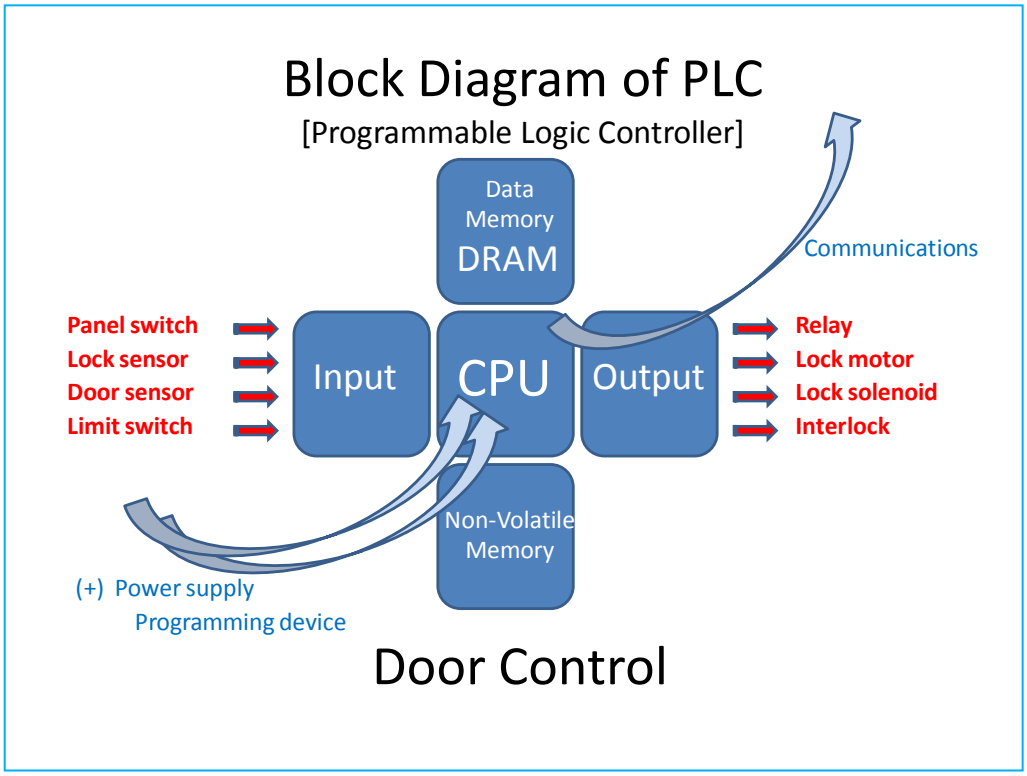
Programmable Logic Controller (PLC) Design

One of the reasons PLCs are used in correctional facilities is because it greatly reduces the amount of wiring that needs to be done amongst a multitude of points. A

large jail or prison has many hundreds of doors to control as well as numerous systems to manage and integrate such as intercoms, video systems, door and lock alarms, lighting controls, and others. These systems are massive and involve many thousands—or tens of thousands—of points and contact closures to monitor. Because PLCs consolidate connections (depending how many I/Os each PLC has), they also can reduce wiring and conduit costs. Consequently, correctional facilities are ideally suited for PLC technology.

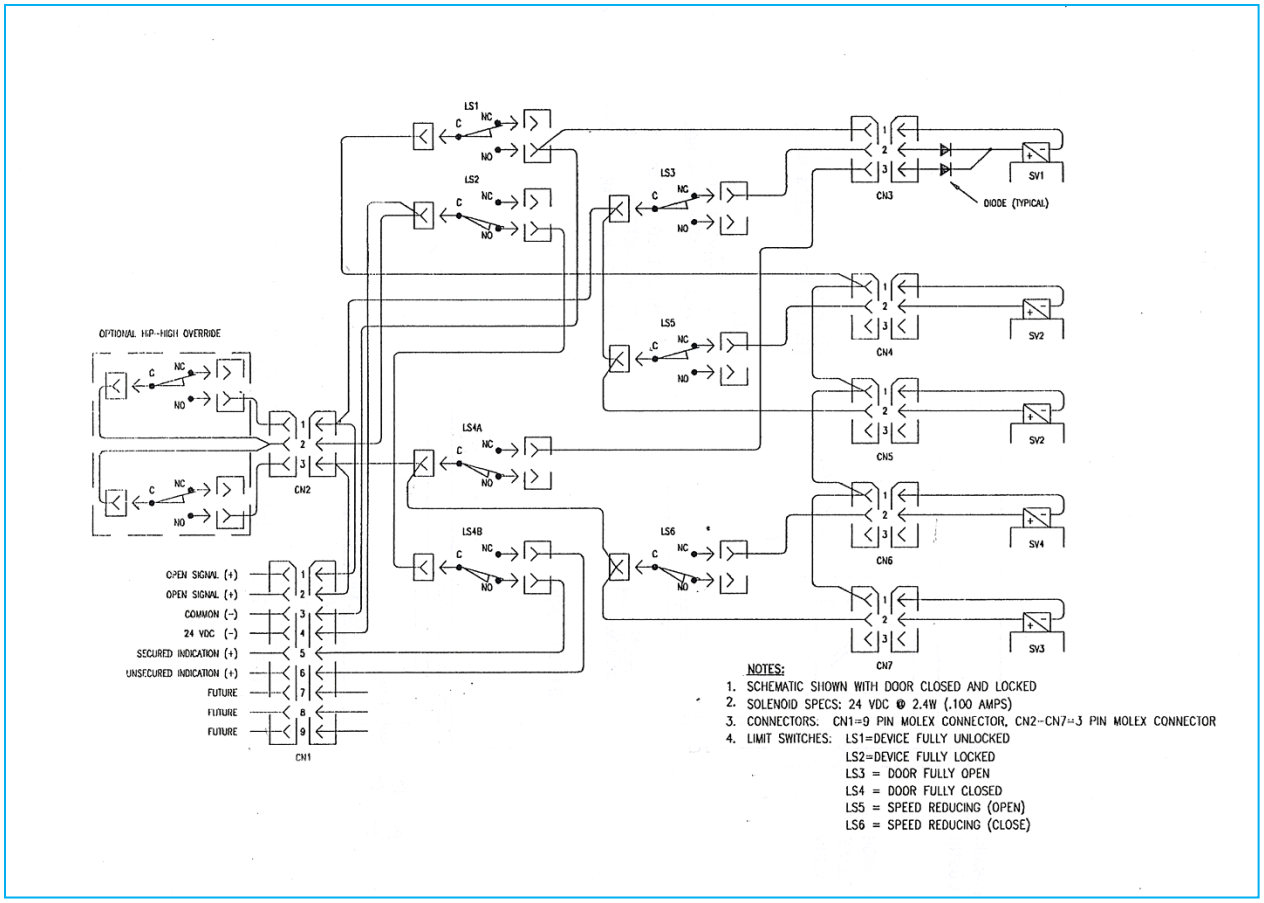
What does a PLC look like? The illustration below (*Figure 1*) shows the typical parts of a PLC just for door control. Bear in mind, a prison security electronic system has many parts beyond door control such as intercoms, lighting control, video surveillance, water and shower control, and so forth. Access to any part, such as a remote intercom station, might provide access to all parts.

Figure 1



The illustration below (*Figure 2*) is of a pneumatic prison sliding door and dramatizes the fact that, depending upon the sophistication of the door control system, this single door can have as many as 34 points to monitor.

Figure 2



There are a few basic aspects to PLCs:

- The communications port is typically 9-pin RS-232 or EIA-485;
- The communications protocols are usually Modbus, BACnet, or DF1.
- The most common programming language, especially in older systems, is "Ladder Logic," which, because it is intended to be simple, is very vulnerable to being exploited. Other programming languages are far less common:
    - FBD (function block diagram)
    - SFC (sequential function chart)
    - ST (structured text; viz. Pascal)
    - IL (instruction list)
    - BASIC

- C++

There are from 40 to 50 manufacturers. The PLCs most commonly used in corrections are the following:

- Allen-Bradley
- GE Fanuc
- Hitachi
- Mitsubishi
- Panasonic
- Rockwell Automation
- Samsung
- Siemens
- Square-D

Prisons, Penitentiary and Jails Design

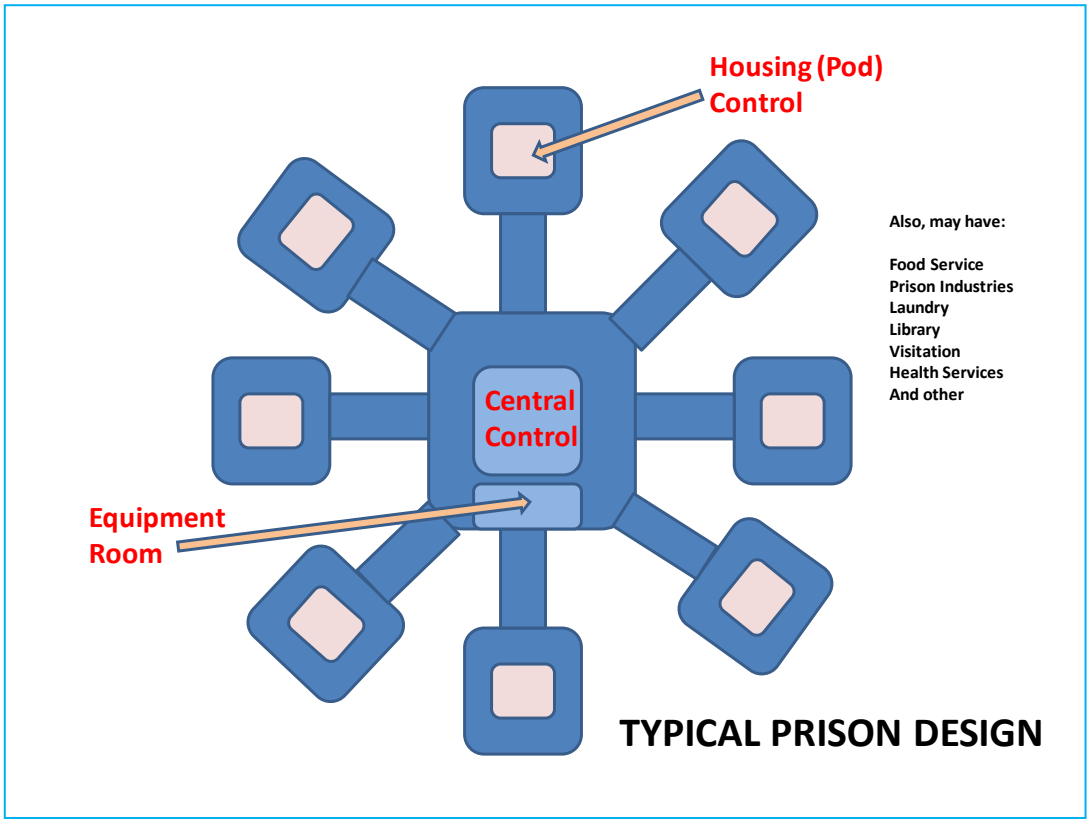
While many prison and penitentiaries use PLCs, smaller correctional facilities such as local jails may not. Prisons and penitentiaries are correctional facilities that are intended for confinements of at least a year (or life) and are owned and operated by the federal government or by states. A number of them, about 160, are operated by private companies. Jails, on the other hand, are intended for incarcerations of a year or less and are owned and managed by city, county or town governments.

Jails are typically much smaller than prisons, albeit there are some very large jails. Orange County Jail in California, for example, has more than 2500 inmates. Moreover, there has been a trend toward regional jails that serve multiple jurisdictions and can also be very large. One might be tempted to ignore jails in this vulnerability analysis, but they are also where people are held for trial—meaning that a jail prisoner could be a petty thief or could be a terrorist.

In broad numbers, the United States has about 117 federal correctional facilities, roughly 1,700 prisons, and more than 3,000 jails. All but the smallest facilities use PLCs to control doors and manage their security systems. The trend in new correctional facilities has been toward star cluster designs for large facilities (Figure 3). A central control center is the hub and serves as the “brain” for the facility. They typically have the capability of controlling anything.

Day-to-day operations of the cell areas, however, are managed by a local housing control station, sometimes termed "pod" control. Similarly, perimeter gates (sally ports) are usually operated directly by a control station near the gate. However, because most correctional facilities are typically short-staffed, it is not uncommon for the control of housing areas and even gate operations to be transferred to central control when activities are at a lull, such as during the "graveyard" hours. This creates a vulnerability that can be exploited.

Figure 3



Exploiting Prison Systems: Possible Scenarios

Let's assume that one introduced an exploit into a prison system. What could be done? In addition to the obvious scenario in which a prisoner may escape if doors and gates are opened, the purpose could also be to either cause chaos for a murder or bring an item into the prison. Granted, the probability of success may be low due to a high concentration of law enforcement usually present, but it is conceivable. By contrast, in

the past 30 years there have been about 8 times that helicopters have been used for a prison escape, of which 6 were initially successful.

On the other hand, one could prevent doors from being opened for a short time. This scenario has sinister assassination possibilities if one understands the unique nature of how fire evacuations are conducted in prisons and the technology of "slam-lock" doors and something called the "remote latch holdback." Someone with malicious intentions could wreak widespread pandemonium by severely damaging door systems and shutting down security, communications, and video systems.

As one example, a very large prison cannot instantly and simultaneously open or close all doors. The power in-rush would be massive, destroying the electronics and possibly physically damaging door components. The doors are gradually cascaded, group-by-group. If we controlled the PLCs, we could override the cascade program.

Network Security and Information Technology within Correctional Facilities

The question arises, therefore, how likely is it that we could take control of PLCs? If you query anyone from the corrections industry, the answer is inevitably the same: They say it cannot be done because there are no outside network connections. But, is that true?

A location our team surveyed, indeed, had connections to the Internet from in the Control Room. During our survey, a Control Room guard was accessing Gmail and commenting that there are problems with viruses and worm from guards accessing online images and movies. Additionally, many federal prisons use a "security through obscurity" method by obscuring a data port under the legs of the control panel console.

Having no connectivity to the Internet for updates for industrial control systems (ICS) is not practical. There are a few principles to consider when ICSs are in secure facilities. The term CIA, in some realms, stands for the Culinary Institute of America, but with IT and ICS, it stands for Confidentiality, Integrity and Availability. Securing ICSs like a typical IT (information technology) center is not a fix for these vulnerabilities.[iv] The CIA principles are crucial for an IT system. When exchanging information between IT systems and users, the priority for an IT network is 1) Confidentiality of the exchange; 2)

Integrity of the data being exchanged; and 3) Accessibility of the data and network. Additionally, IT networks are often shut down for regular maintenance. This is not practical for an ICS network.

In contrast, ICSs have a different priority of AIC.[v] Availability is of the utmost priority because ICSs cannot be shut down for regular maintenance if they are in continuous use; shutting them down for updates must be coordinated. Since availability is of the utmost importance, it creates another security complication: reduced usage of Intrusion Prevention Systems. Since intrusion prevention can impede availability, IPSs are less commonly deployed. In many prisons and jails, the PLCs also control video monitoring, alarm systems and communications in addition to door controls. For these reasons, integrity and confidentiality are lesser priorities than availability.

In turn, simply cutting prisons off from the Internet is not a practical solution to mitigating the risks associated with PLCs and control computers. The “availability” requirement is also important because correctional facilities must send and receive information to and from federal, state, and/or local data bases such as criminal records databases.

Other communication requirements to outside the facility include operations, such as food services, which have online connections to vendors and suppliers. We have found some points where prison Commissaries connect to network segments on which the PLCs are located. Some correctional facilities also provide Internet access for inmates. Granted, they are not connected to prison control and monitoring systems, but they are a point at which a vulnerability can be exploited, albeit difficult.

Unauthorized Access to Networks

Perimeter patrol vehicles sometimes have wireless connections to the facility perimeter intrusion detection system and central control. However, there have been cases in which patrol cars’ video is uploaded to the correctional facility via 802.11 g and n, and as a result of the connection not being encrypted, a neighbor uploaded the video

to YouTube. Hacks on patrol vehicles have also been reported in the media as have people being able to access video on law enforcement videos by accessing the DVR in the vehicle.[vi]

In relation to security of networks in correctional facilities, access to jail networks are necessary for patrol cars to upload data, but isolating networks used by law enforcement from that used by prisoners is crucial. There is one example of a maximum security correctional facility in Colorado where the prisoners have access to computers from within their cells. One news article states that the system is hardened and very secure.[vii] However, a follow-up article published on the same day states how the prison has instated a "successful program" in which they are patching the security holes prisoners are finding; prisoners caused buffer overflows.[viii] From the information given, it is not possible to tell if the systems were vulnerable; however, they do use software with known vulnerabilities. It is also unknown if it was possible to connect to the same systems on which the prison PLCs may be connected, but if not patched, there may be an attack vector. [ix]

Considering PLC and SCADA vulnerability research that has been made public since Stuxnet was discovered, there are some correctional facility design vulnerabilities that should be evaluated in conjunction with the wired network and Internet connectivity both within and to outside them.

Attack Vectors

While this research began with academic Stuxnet code review, some of the attack vectors used by Stuxnet are similar to what we produced in our "lab" By accessing the loaded libraries of the software that control, monitor, or program the PLCs, we believe we have found an attack vector that is not vendor-specific. Once compromised, it is possible to manipulate the physical state of anything connected to the PLC -- such as the lock state of doors -- and it is also possible to suppress any notifications or alarms that are delivered or derived from the PLC. "Open Door" notifications are one such example.

Custom exploits are not hard to create for PLCs due to the ease of programming them by simplistic programming languages like Ladder Logic. For example, everyone on this research team was able to put together a PLC exploit in only a few hours. While we created the exploits for research purposes, there are many exploits that are publicly available and can be found online such as on Exploit-DB.com.

There are multiple attack vectors that could lead to a compromise of the PLCs. If the machine controlling, monitoring, or programming is misused by personnel and connected to the internet, then the usual client side attack vectors are in scope. When it is connected to the Internet, it is also subject to conventional attacks such as, man-in-the-middle, network based attacks exploits, and forced updates – perhaps some with improper SSL certificates as was the case with Stuxnet.

In addition to remote attack vectors, Stuxnet showed that physical access to a facility is just as great of a risk. It is theorized that Stuxnet was introduced to computers in an Iranian nuclear facility by an infected USB drive. Likewise, we learned from our evaluation of a correctional facility that the same could be done with techniques such as social engineering or any method that would gain a malicious attacker physical access. While we were viewing the Control Room, we were invited to follow the IT repair technicians into the Equipment Room where they had been working alone.

Research Workshop and Expenses

The research we performed cost approximately $2500 and it was done in a basement workshop. It should be noted that this is the cost to acquire the hardware as well as legitimate licenses for the software. If someone only desired to acquire the hardware, the cost would be closer to $500.

The relatively low expenses involved in this research shows that this does not require a large laboratory environment, or an advanced persistent threat.

Recommendations

Our recommendations for improving security in locations with PLCs and SCADA in which the U.S. keeps its greatest assets (banks, government research facilities, etc) and in which it keeps its worst liabilities, such as in correctional facilities, include a combination of re-evaluation of prison physical designs and electronic security, network security and greater enforcement of computer usage policies in these facilities.

Our recommendations for correctional facilitates:

- Prison design re-evaluation: many modern prisons/jails were designed 10 years ago before these attack vectors were known;
- Improved communication/interaction between IT and physical security;
- Enforcing and updating procedures and policies regarding acceptable use of facility computers;
- Patch PLC and controlling computer's software;
- When PLCs are in use in secured areas, use heightened security procedures
- Proper network segmentation;
- Use a device for its intended purpose;
- Restrict physical media.

Summary

A logical conclusion to this research is that our findings do not only pertain to PLC and SCADA vulnerabilities in correctional facilities, but in any high-security location that uses these technologies as well as in manufacturing plants, transportation and just about anywhere that multiplexing is used.

When securing the country's most dangerous liabilities, we encourage that more attention be paid to access control, network security/segmentation and personnel policies. And as was the case with Stuxnet, proper adherence to secure operating procedures will greatly reduce the chances of infection of PLCs and control computers from the inside and outside of a secure facility.

Endnotes

[i] Gross, M. (2011, April). A Declaration of Cyber-War | Culture | Vanity Fair. Retrieved July 22, 2011, from http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104

[ii] Gilbert, D. (2011, July 14). Hackers Targeting Critical Infrastructure. *Security Techology Executive*. Retrieved July 22, 2011, from http://www.securityinfowatch.com/Features/hackers-targeting-critical-infrastructure

[iii] Deshmukh, A. (2011, June 27). ID37: SIMATIC S7 300 is Used to Automate the Operations of a Jail." Navigating the World of Automation, Siemens Automation Conference: June 27-30, 2011. Retrieved July 22, 2011, from http://www.industry.usa.siemens.com/topics/us/en/summit/Documents/Siemens_AutomationSummit_BreakoutSessions.pdf

[iv] Robert Anderson, Trond Bjornard, Mark Schanfein, and Paul Moskowitz. (n.d.). INDUSTRIAL CONTROL SYSTEM CYBER SECURITY: QUESTIONS AND ANSWERS RELEVANT TO NUCLEAR FACILITIES, SAFEGUARDS AND SECURITY. Idaho National Laboratory.

[v] *Ibid.*

[vi]Dan Goodin. (2011, May 3). Hacker pwns police cruiser and lives to tell tale • The Register. Retrieved July 28, 2011, from http://www.theregister.co.uk/2011/05/03/cop_car_hacking/

[vii] William Jackson. (2011, May 25). Maximum security prisoners play red team in hardening Colorado prison's network -- Government Computer News. Retrieved July 28, 2011, from http://gcn.com/articles/2011/05/30/colorado-prison-sidebar.aspx

[viii] William Jackson. (2011, May 25). Colorado uses IP to provide secure services to prison inmates -- Government Computer News. Retrieved July 28, 2011, from http://gcn.com/Articles/2011/05/30/Colorado-Prison-Internet.aspx?Page=3

[ix] Exploits Database by Offensive Security. (n.d.). . Retrieved July 28, 2011, from http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=citrix&filter_exploit_text=&filter_author=&filter_platform=0&filter_type=0&filter_lang_id=0&filter_port=&filter_osvdb=&filter_cve=