Global Information Assurance Certification Paper

John Best
Version 1.4
Industrial Systems Automation and Security:
an "Electronic Pearl Harbor?"

Abstract

Until recently a coordinated attack on the Internet or an attack on the country's critical infrastructure was considered highly unlikely. A pre September 11th article by David Isenberg published by the Cato Institute, entitled "Electronic Pearl Harbor? More Hype Than Threat," states that our nation's infrastructure was more at risk by our own over-reaction to cyber threats than by a rogue state or terrorism group (Isenberg, page 1). Moreover, others compared the possibility of cyber warfare to Y2K and suggested that it would be a non–event.

Unfortunately, the tragic events of September 11th ended the speculation. Almost immediately after the tragedy, details came to light illustrating how al-Qaeda used advanced encryption techniques to transfer data and avoid detection on the web. The use of these tools certainly confirms our worst fears; our foes know our technologies as well as we do.

White house cyber-security Chief Richard Clarke once told a panel discussing cyber threats that, "We have the equivalent today of enemy aircraft flying over the target." Unfortunately this was a pre–September 11th prophecy. During the time before 9/11, it seems most analysts were more worried about a disruption of service to the Internet causing a stock market crash and affecting e-commerce transactions. Physical attacks or hackers seizing control of a power grid were considered highly unlikely.

However, all that changed when the United States military discovered, in recovered al-Qaeda laptops, evidence that suggests that terrorists are focusing on industrial automation systems. It is clear that hostile terrorist groups are researching our systems and want to collect the necessary knowledge to control essential portions of the United States' critical infrastructure. In 1997 Richard Clarke coined the phrase "Electronic Pear Harbor," to identify the devastating effect an attack on our critical infrastructure could produce.

In this paper we will define what makes up our nation's critical infrastructure and explain how industrial automation systems are used to manage almost every aspect of it. Next, we will discuss the lack of security used by these industrial automation systems and how these systems could be compromised using common attack techniques. In conclusion we will discuss what steps must be taken to ensure that these industrial automation systems are secured.

What is Critical Infrastructure?

Just the term 'critical infrastructure' conjures images of well guarded facilities running incredibly important services, protected by the military. Unfortunately, although the services they provide are incredibly important, they are not well guarded or protected by the military.

Oil, transportation, telecom, water, natural gas, electric power, emergency response and financial systems are all part of our nations critical infrastructure. Take a minute and imagine life with out any one of these services. How would one perform simple daily activities without water or electricity?

A study, entitled "Lessons Learned from Industry Vulnerability Assessments and September 11th" released by the Department of Energy's Office for critical infrastructure protection, included the following diagram: (Fisher ,Ron and Peerenboom ,Jim, "Lessons Learned from Industry Vulnerability Assessments and September 11th").

This diagram displays a collection of systems connected in various ways. These systems are all dependent on each other. By breaching or disrupting any of the main systems, one could potentially disrupt all connected systems. It is this interdependency that makes them an attractive target for terrorists.

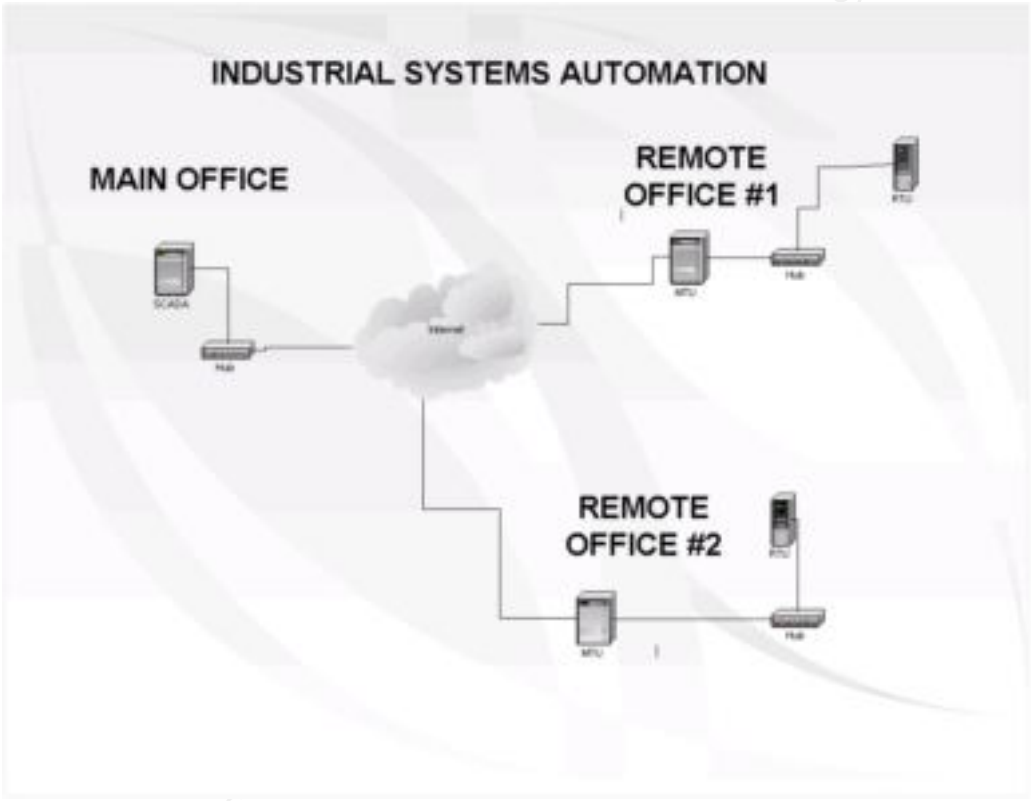
What is Industrial Automation?

Industrial automation is core to our nation's critical infrastructure. These digital switches are responsible for running water, power, nuclear plants and emergency response and transport systems. Industrial Automation systems can be comprised of the following components.

- **SCADA** - Supervisory Control and Data Acquisition: This is the main system that collects data from all of the other systems. (Weise, SCADA Primer)

- **DCS** - Distributed Control Systems (Weise, SCADA Primer)
- **PCL** - Programmable Logic Units – Units that would be drone units to a SCADA system or MTU. (Weise, SCADA Primer)
- **MTU** - Master Control units – These units reside at each site and collect data from the RTU's and PCL's . Once the data is collected this system would then communicate with the Scada system(Weise, SCADA Primer)
- **RTU** - Remote control units. – These units connect via PC to valves pumps and other automated devices. (Weise, SCADA Primer)

Here is example showing the connectivity between these devices:



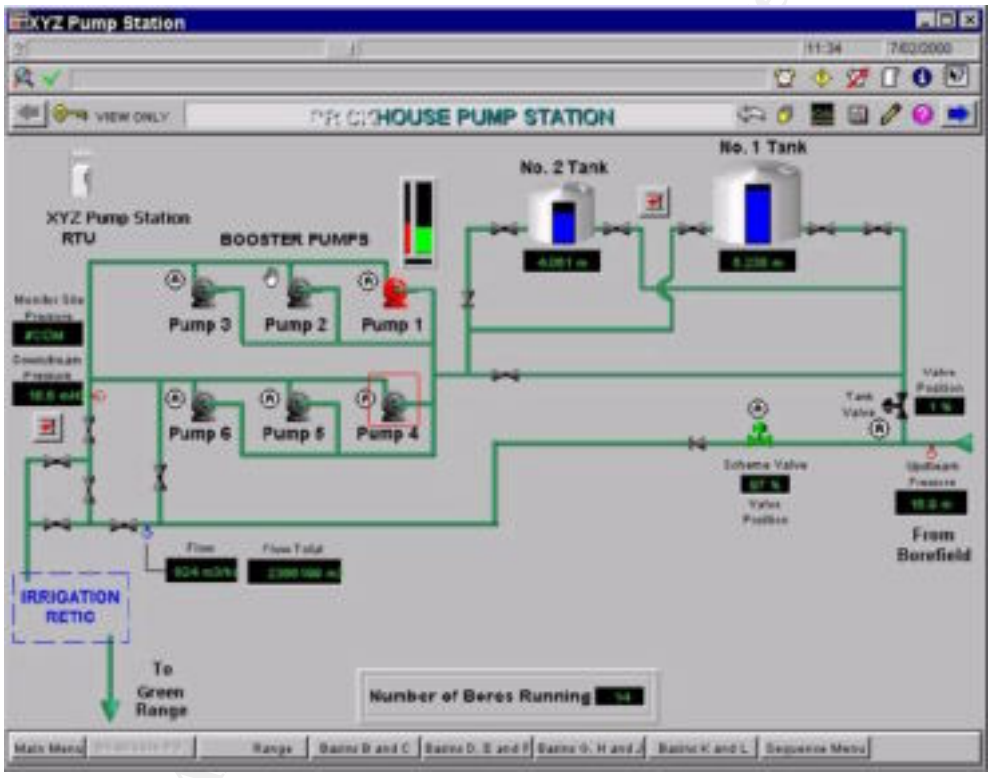
John Best

Typically an industrial system automation design will consist of an RTU connected to a device such as a valve or pump, usually via the serial port. The RTU is polled by the MTU, which transmits the data back to the SCADA. SCADA's may collect data from multiple MTU's in multiple locations. The MTU's serve as aggregators for the site and feed the SCADA. The communication between the MTU and the SCADA system usually occurs across a WAN or, possibly, the Internet. The SCADA system is designed to take input from the remote devices and make decisions based on the data.

For instance, an RTU may transmit data to the MTU that indicates a storage tank is 35% full. The MTU would then be polled by the SCADA for data on the storage tank. After reviewing the data, the SCADA may either alert an operator or, based on a predefined rule set, initiate an action. A possible example action would be to activate a pump to re-fill the storage tank. The power of the SCADA system is its ability to monitor hundreds of thousands of analog and digital points, make complex decisions and perform actions in sequence. In the case above, it could close valve A and open valve B until pressure reaches X percent of load.

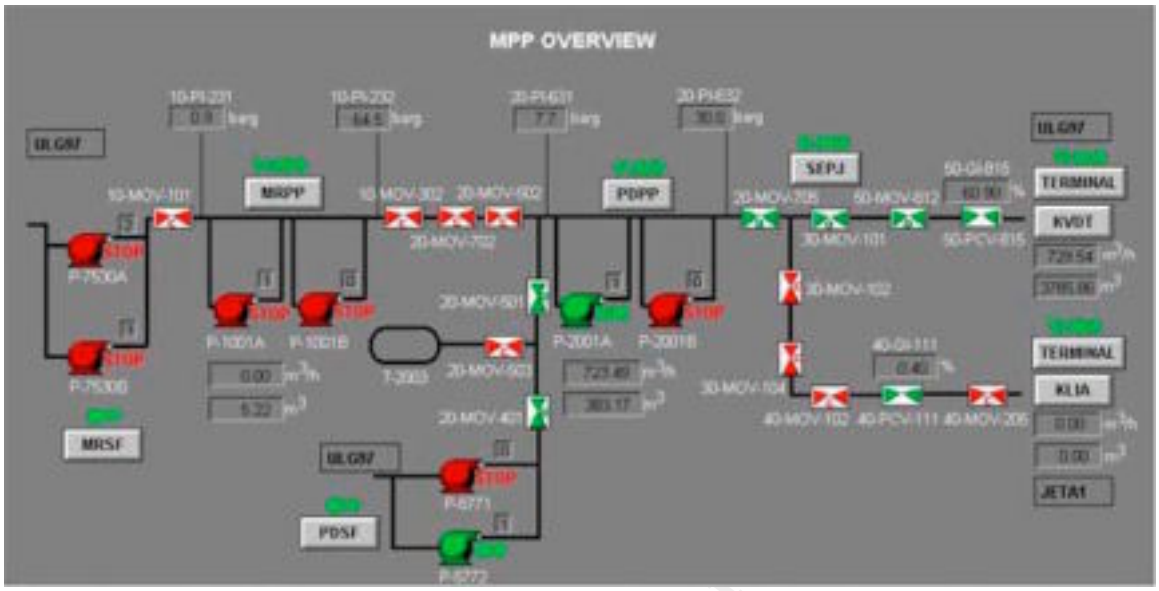
There are an estimated three million SCADA systems in use today. SCADA systems are involved in controlling the core of our nations power grids, water supply, emergency response, and transportation systems.

Here is an example of a SCADA system that controls a pumping station in a water plant taken from Ian Weise's SCADA Primer at http://members.iinet.net.au/~ianw/primer.html.



In this particular example, notice that PUMP 1 is red and probably in need of attention. One interesting point of this example is that the system is very user friendly. Basically, it is icon based and uses point click functionality combined with programmable rule sets.

Here is a second example of a SCADA system. This one controls the Malaysia Multi-product Pipeline from Port Dickson to the Kuala Lumpur International Airport and the Klang Valley Distribution Terminal.



NKK VIVID, http://www.nkk.co.jp/

This example was taken from NKK VIVID's web site. NKK VIVID is a provider of SCADA systems. Here is a example of text taken from the site:

> "The SCADA master installed in the central control room in KVDT is connected with RTUs installed in terminals and stations via Malaysia Telecom Lines. Each RTU in the terminal interfaces with the refinery's DCS (Distributed Control System) or TAS (Terminal Automation System). A leak detection system supplied by LICconsult (Now called LICenergy) is provided as a part of SCADA master. With these functions, the pipeline and relevant facilities can be continuously operated by a single person."
>
> (NKK VIVID, http://www.nkk.co.jp/)

The pipeline is used to feed four different kinds of gasoline to Kuala Lumpur International Airport and the Klang Valley Distribution Terminal. The four products are, unleaded gasoline, leaded gasoline, diesel, and aviation fuel.

This particular example shows the SCADA master is being fed continuous data from the RTU's and making decisions based on this data. It includes monitoring for leakage. Disrupting this service would no doubt disrupt KLIA's (Kuala Lumpur International Airport) and KVDT's (Klang Valley Distribution Terminal) ability to function. The final statement on the website indicates that the entire facility can be controlled from one console.

(Note the amount of data one can find about these systems on the web).

Lack of Security is Rampant

First of all, after reviewing these systems and their uses, it would seem to be a forgone conclusion that these devices and controllers would reside on a separate and contained network. In fact, this is not necessarily true. A study done in January 2001 by Riptech asserts that this is, in fact, incorrect. There are at least three compelling reasons to locate the SCADA system on the corporate network:

- The need for remote access has driven IT managers to collocate these devices on the corporate network, often allowing Web access to the Control panel.
- Real-time Data collection for corporate decision makers.
- Consolidating the networks would save on costs on corporate Data communications.

If someone makes the decision to connect these devices to the corporate network, then all devices connected to the corporate network should be subjected to the same level of security scrutiny as the normal corporate network devices. Unfortunately, this is not necessarily true. Since these devices are usually configured on low level PC's running under older operating systems, outside the normal peruse of IT staff, it's not unusual to find the access controls to these systems wide open. Many times, corporate pressure and lack of fiscal resources prevent IT administrators from properly addressing security on these devices. Another reason for a lack of access controls is that the industry itself hasn't accounted for security in its core design. During the process of creating this paper, I reviewed many SCADA systems and RTU devices. It appears that only recently have vendors in this area begun to take security in to account during the creation of their products.

Secondly, there is considerable data on SCADA on the web. During my research, I was able to find at least 5 major companies providing PDF files on how to run their SCADA consoles and 5 more with specifications that detailed the information on RTU interfaces. This includes the examples in the paragraphs above.

As these complex systems have grown, a standards body has been created and published as well. Since this data is readily available, it's a forgone conclusion that this data is already in the wrong hands. These documents clearly show that SCADA systems lack security as a core feature of their design. For instance most SCADA systems don't offer encrypted communication for protocols.

Finally, the core issue is that, once these systems are connected to the corporate network, which is in turn connected to the public Internet, they are now vulnerable to the same threats that are found in the wild everyday.

Compromising Industrial Automation Systems

Let's take for example XYZ electric company. XYZ Electric Company has just taken their customer service website in house. They have purchased a firewall, a firewall, a large Internet connection, trained their IT staff, and setup their web servers. The firewall has three interfaces, Service Net, Corporate, and Internet. Using the firewall's IP proxy

function the firewall administrator routes incoming packets destined for a public internet address through the firewall to the web server on ports 443 and port 80. Since the web developers work on the corporate side of the network a hole is drilled through the firewall from the corporate network for the developers to the web servers. Developers have access to the full range of services on the web servers via the firewall.

Although IT has patched the web servers, the developers have since re-installed several pieces of software without the network engineers knowledge in an effort to fix some problems on the servers.

This move has not gone unnoticed to hacker x. Hacker x has been monitoring the switch over from the service bureau every since the DNS request was made by XYZ electric company's network administrator to move the domain.

After spending long hours with low level scans Hacker X has correctly determined that the only perimeter defense in place is the firewall. There is no intrusion detection to avoid; this will make his job far easier and quicker. Hacker X was able to fingerprint the firewall as a Checkpoint 2000 system. Hacker X has also correctly fingerprinted the web server software and operating system. Armed with this knowledge, hacker x tries several low level attacks on the web server. To his surprise the attack that failed the day before now works. It appears as though some one has re-installed software and not applied the appropriate patches.

Now that Hacker X has control of the web server, he could easily change the content of the web page, Spam other websites. Create a secret website to hide data. Very simply, he could utilize any of a number of publicly available hacker tools out there to cause havoc in the network.

After lying low for a few days, hacker x returns to the scene of the crime and uploads several sniffers and cracking tools on the web server. Utilizing a blowfish tunnel bouncing through outbound DNS requests he establishes a secure tunnel with the web server. With his tools in place he begins to scan, hoping to find his way back to other PC's in the network.

Immediately he finds the connected developers PC's since the developers are in their own separate domain, hacker x has to determine how best to compromise this box without the user knowing. First he tries a simple share attack on the developer's box (windows 2000). Although this didn't work he is able to discern the developer is running windows 2000 and Mcafee. The NetBIOS name of the box is Rsmith.

He decides to check the phone directory on the main line of XYZ electric company, he quickly discovers there are two people who work there who have the last name of Smith. There is only one staff member with a R as the first letter. Robert Smith is the name of the developer whose box Hacker x was so desperately trying to compromise.

Hacker X decides based on the low level of security he has encountered so far, to try some social engineering. He calls XYZ Company and has the following conversation

- **Hacker X**: Hi can I speak to some in Information Technology
- **Operator**: sure I will patch you right through.

- **Hacker X**: thank you
- **Support Analyst**: Hello and thanks for calling Tech support can I help you
- **Hacker X**: This is Robert Smith, I cannot get in to my web based email, I am at a conference and desperately need to get access to my email. Can you help me?
- **Support Analyst**: Sure Mr. Smith, it appears your account is fine, doesn't appear to be disabled or removed.
- **Hacker X**: You know I changed my password just before I left and don't remember it.
- **Support Analyst**: No problem what would you like your password to be?
- **Hacker X**: how about Hax0r?
- **Support Analyst**: Good password Mr. Smith. I have changed it.
- **Hacker X**: Thanks

Now that Hacker X has a username and password to the Development domain he uses his tools to crack the password database and collects all of the usernames. He creates a new account for himself, surmising that the developers maintain their own domain based on the poor setup of the forest. He spends sometime looking at the development domain. But ultimately decides to move on. After cracking many more machines he finally finds a machine where there was a shared hub and several devices connected to it. In effort to save money on difficult cable runs, XYZ Electric Company had chosen to put this PC and several PLU devices on the same shared hub. From this point hacker x could now see his prey. He captured packets from the PLU devices output and input and noted source and destination. He briefly toyed with the idea on injecting fraudulent packets into the network destined for the SCADA device. Instead he resisted when it became clear he could achieve the goal of compromising the SCADA system.

Based on the destination address of the packets he then began a low level scan and carefully considered his plans for compromising this system. Using nmap he discovered X-windows running and that the OS was HP UX. After running through several attack methods he was able to compromise the system. He was now looking at a screen shot of an operators console monitoring SCADA screen. Full control of the all of the electric company's most crucial systems was now in his reach. With a simple click of the button he could turn off power to half the city. His patience had finally paid off.

Another method of compromising SCADA systems is through the Publicly Switch Telephone network. Many SCADA systems also use modems that are set to auto answer for remote access to save money on data communications. An intruder using a WARDIALER could find the number and use brute force or social engineering to gain access to the operating system. If the device is connected to private network this would allow an intruder access to the internal network and possibly to the SCADA controller. Even if the device is remote stand-alone unit, a intruder could gain control of the particular device and cause it to malfunction.

In the past many people thought that these fears regarding critical infrastructure were unfounded, but as current events show the threat is real. In an article by Barton Gellman of the Washington Post entitled "U.S. Fears Al Qaeda Cyber Attacks", the following details of an actual SCADA system attack.

> "In Queensland, Australia, on April 23, 2000, police stopped a car on the road to Deception Bay and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment along Australia's Sunshine Coast."
>
> "Boden's arrest solved a mystery that had plagued the Maroochy Shire wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and the manicured grounds of the Hyatt Regency hotel. Janelle Bryant of the Australian Environmental Protection Agency said "marine life died, the creek water turned black and the stench was unbearable for residents." Until Boden's capture --- during his 46th successful intrusion --- the utility's managers did not know why."

In this particular case, Vitek Boden had just been fired from his job. Evidence suggests Boden's motive was to create a consulting opportunity to fix the problems he was causing. During Boden's forays in to the system, he had ultimately gained total control of the water system. The article goes on to state that Boden could have done anything he wanted, including contaminating the drinking water supply. Fortunately, in this case, the intruder showed restraint.

This demonstrates what can happen when a SCADA system can be easily breached. Cyber terrorism experts are currently studying this case, the first known SCADA intrusion.

Although SCADA attacks are serious by themselves, many people believe that a cyber attack on SCADA systems would be part of a multi-faceted attack on America's landmarks and people, For example, imagine that cyber terrorists had simultaneously breached 911 SCADA systems that control New York Emergency Response services during the September 11th attack on the WTC. At the same time, SCADA systems that control water and electricity were also breached. This would add to the fear and confusion of the disaster, in addition to limiting the response.

What follows is a timeline of SCADA related issues.

- **December of 1999**, a computer hacker publicly announced his intention to release a report outlining how to break into power company networks and shut down the power grids of 30 United States utility companies. – RIPTECH, Understanding SCADA System Security Vulnerabilities ,January 2001

- **April 23 2000**, Vintek Boden breaches the Maroochy Shire wastewater system. - Gellman, U.S. Fears Al Qaeda Cyber Attacks, Washington Post, Jun 26 2002
- **May of 2001**, someone tried to hack into the CAL-Independent System Operator (ISO) site, the nonprofit corporation that controls the distribution of 75 percent of the state's power. While the attacker's motives remain unclear, the attacks came when California was in the midst of an energy crisis, when cities across the state were experiencing rolling blackouts every day. Lemos , Hack raises fears of unsafe energy networks
- **June 26th 2002**, Detective Chris Hsiung finds multiple casings of sites routing through Saudi Arabia, Indonesia and Pakistan. The main target was emergency telephone systems, electrical generation and transmission, water storage and distribution, nuclear power plants and gas facilities. Some of the probes suggested planning for a conventional attack, U.S. officials said. But others homed in on a class of digital device that allows remote control of services, such as fire dispatch, and machinery, such as pipelines. More information about those devices -- and how to program them -- turned up on al Qaeda computers seized this year, according to law enforcement and national security officials. - Gellman, U.S. Fears Al Qaeda Cyber Attacks, Washington Post, Jun 26 2002

In my own opinion, it is interesting that two train wrecks occurred on Tuesday, September 11th 2001 and Thursday, September 13th 2001. I am in no way asserting that I have any evidence linking these events together nor am I asserting that SCADA devices were breached in these tragic crashes, as I have no first hand knowledge at all of these investigations.

White house cyber-security Chief Richard Clarke once said, “Our enemies will use our technology against us, just as the hijackers used our planes”. All of this evidence makes clear that this threat is very real. These systems can be compromised. It isn’t a matter of if, but when, this will happen.

What Steps Must Be Taken

SCADA systems deserve as much attention in matters of security as do the critical systems they serve. The Office of Critical Infrastructure Protection released these following guidelines in the document “Lessons Learned from Industry Vulnerability Assessments and September 11th”, December 12-13, 2001

- Develop an overarching enterprise security model that is comprehensive, consistent with the mission and values of the organization and widely accepted within the organization.
- Incorporate security into enterprise risk management processes.
- Develop a consistent designation and valuation of critical assets and develop the means to assure the security of these assets.

- Implement structured security requirements for critical suppliers and partners.
- Periodically review, and update, emergency plans to include newer threats and vulnerabilities and test these plans regularly.
- Implement appropriate configuration management across all IT systems. Be particularly attentive to systems that interface with critical assets.
- Raise employee awareness about proactive security by establishing and implementing policies and procedures for controlling and validating "trust" allocation.

Fortunately since most of the threat comes from exposing the devices to the Internet or remote access modems, there are very good tools today that can be implemented to protect these networks. Intrusion Detection Systems, Data encryption devices, Authentication, and Firewall technology are a few of the technologies that could provide first line defenses to the infrastructure.

Intrusion Detection Systems would allow for monitoring of the access to SCADA systems, it seems the control console and associated systems would be a good place to start monitoring as well as all access points to the Internet. When attackers sense intrusion detection systems, it severely limits their ability to attack a system. This will also improve the ability to detect a threat before there is a breach instead of after the fact. Hackers probing for data on these systems could be detected before there is a problem.

SCADA systems communication channels would benefit greatly from encryption techniques like 3DES or AES. Using encryption would make it much harder for hackers to inject packets in to the stream of communication from MTU's and RTU's to SCADA systems. This would also prevent this data from traveling the network in clear text. This would also benefit remote devices that are connected via the public telephone switch

Strong Authentication techniques should be used for accessing critical components of the SCADA system like the console. If this system has to be accessed from web, users should be authenticated with strong passwords and tokens. SmartCards , Biometrics and Tokens could all be used to validate that users of the consoles are in fact who they say they are. This authentication should also be applied to all remote devices to prevent a intrusion via the modem pool.

Using multiple firewalls in back to back configurations to separate SCADA networks from corporate networks could further protect these systems from being compromised. By using a firewall, communication between devices could be locked down to the MAC address of the devices. The division of these devices will make it much harder for hackers who have penetrated the corporate network to access the SCADA network.

I would add that vendors of Industrial Systems Automation technologies need to take into account that their devices will be connected the public internet and that security efforts should be adapted in to the current standards that govern connectivity to digital controllers and SCADA systems.

Recently, President Bush mandated that these systems be fixed. It was also acknowledged that, while government systems can be addressed, the private sector faces

a tremendous financial outlay to correct the security problems that are inherent to their infrastructure.

It is critical that legislation and financial support for security be made available to the private sector companies that are responsible for our most critical infrastructure. Only immediate action will prevent a future disaster from occurring.

Up until now we have a looked at Hackers and the damage they do as being mostly financial and/or defacements. Identity theft and data theft were most feared. Those times are gone. As our nation has grown in to a more connected entity, we have exposed our most critical devices to our enemies. To make matters worse, we freely shared the information on how to penetrate these devices and have not built in effective security to protect them from intruders.

Attacking our infrastructure is the next great Hacker frontier. If it isn't al Qaeda, it will be another group or, perhaps, even an act of domestic terrorism, as in the Australian case. SCADA systems are just the beginning. All systems big or small not matter how insignificant they seem to be, must include security in the design model from this point forward. It is also critical that legislation and financial support for high security practices be made available to the private sector companies that are responsible for our most critical infrastructure. Only immediate action will prevent a future disaster from occurring.

Sources

1. Bernard Erlich berlic, Scada and DCS definition , Wed, 22 Jan 1997
   http://members.iinet.net.au/~ianw/archive/c4203.htm

2. Fisher ,Ron and Peerenboom ,Jim, "Lessons Learned from Industry Vulnerability Assessments and September 11th", December 12-13, 2001
   http://www.naseo.org/committees/energydata/energyassurance/stern.pdf

3. Barton Gellman, U.S. Fears Al Qaeda Cyber Attacks, Washington Post, Jun 26 2002
   http://online.securityfocus.com/news/502

4. Wiese Ian, Scada Primer, 9th March 1997
   http://members.iinet.net.au/~ianw/primer.html

5. Wiese Ian,SCADA Talks, Industrial Computing December 1999
   http://www.isa.org/isaolp/journals/pdf/ic/991234.pdf

6. Carlson Caron. "IT Pros living in fear of a cyber-attack" E-WEEK July 2, 2002: Volume 19 – Number 26

7. RIPTECH, Understanding SCADA System Security Vulnerabilities ,January 2001
   http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf

8. Spread Spectrum Scene, SCADA Stuff, March 10, 2002
   http://www.sss-mag.com/scada.html

9. Paul Oman, Edmund O. Schweitzer, III, and Jeff Roberts "SAFEGUARDING IEDS, SUBSTATIONS, AND SCADA SYSTEMS AGAINST ELECTRONIC INTRUSIONS" Schweitzer Engineering Laboratories, Inc ,http://www.selinc.com/techpprs/6118.pdf

10. Swartz ,Jon, USA TODAY Experts: Cyberspace could be next target, 11/03/200,http://www.usatoday.com/life/cyber/tech/2001/10/9/cyberwar-usat.htm

11. Isenberg ,David, Electronic Pearl Harbor? More Hype Than Threat, CATO institute, January 3, 2000
    http://www.cato.org/dailys/01-03-00a.html

12. Vamosi ,Robert, Why cyberterrorists don't care about your PC,ZDNET, July 10, 2002
http://www.zdnet.com/anchordesk/stories/story/0,10738,2873733,00.html

13. Hurley ,Paul, How one hacker penetrated a utility network: A true story, Energy IT March/April 2002 Feature
http://www.platts.com/infotech/issues/0203/0203eit_msp.shtml

14. Lemos ,Robert , Hack raises fears of unsafe energy networks, June 13, 2001, 10:15 PM PT, http://news.com.com/2100-1001-268400.html

15. NKK VIVID, Malaysia Multi-product Pipeline ,http://www.nkk.co.jp/