

SCADA Security and Critical Infrastructure

Eugene, Oregon Infraguard Meeting
9:30AM December 7th, 2004, 308 Forum, LCC

Joe St Sauver, Ph.D.
University of Oregon Computing Center
joe@uoregon.edu

<http://darkwing.uoregon.edu/~joe/scadaig/>

Portions of this talk were originally presented at the Internet2/ESCC
Joint Techs Meeting in Columbus, Ohio, July 21, 2004

I. Introduction

My Interest In SCADA; This Talk

- I grew up around industrial facilities (for example, my Dad was a stationary engineer who helped run an industrial steam facility for a major airline)
- My terminal degree is in Production and Operations
- SCADA-related incidents have continued to pop up in the news, sustaining my interest over time
- One note: The technical level of this talk has been tailored to insure that it doesn't provide a detailed "cookbook" that can be used by the bad guys to attack SCADA systems, while still providing sufficient technical detail/evidence to highlight some of the issues that need to be addressed.
- I also recognize that there are basically two different audiences present: LE folks and industry people. A separate glossary has been provided. :-)

So What the Heck IS “SCADA?”

- SCADA is “Supervisory Control and Data Acquisition” – realtime industrial process control systems used to centrally monitor and control remote or local industrial equipment such as motors, valves, pumps, relays, sensors, etc.
- SCADA is used to control chemical plant processes, oil and gas pipelines, electrical generation and transmission equipment, manufacturing facilities, water purification and distribution infrastructure, etc.
- Industrial plant-scale SCADA is often referred to as a “Distributed Control System” or DCS
- SCADA nuzzles up to embedded system issues, too.

Think of SCADA As...

- ... the computer equivalent of George, the guy in the hard hat, going around reading gauges and recording values on a clip board, or opening valve #173 and turning on pump #8 at 11:15AM on December 7th when the schedule says it is time to make another batch of product <foo>.
- Of course, because we're talking about computerized systems, we'll typically be talking about complex systems with hundreds, thousands or tens of thousands of remotely managed control points. At that volume, it is not surprising that SCADA is often "event driven" (e.g., "signal an alarm, something's out of spec")

**II. Wow. That Sounds About As
Exciting As Watching Paint Dry....**

Actually, SCADA Can Be Frighteningly “Exciting”...

- SCADA insecurity may have contributed to the end of the Cold War*
- SCADA may be of substantial interest to major terrorists
- SCADA systems may suffer sabotage by disgruntled insiders, acting individually
- SCADA may have “big” technical failures
- ... but we’d really prefer it to be VERY dull!

*SCADA’s role in bringing an end to the Cold War needs to be balanced against activities elsewhere, as described, for example, in George Crille’s book “Charlie Wilson’s War,” (Grove Press, 2003, 0-8021-4124-2)

“The Most Monumental Non-Nuclear Explosion and Fire Ever Seen From Space.”

- Thomas C. Reed, Ronald Reagan’s Secretary of the Air Force, described in his book At The Abyss (Ballantine, 2004, ISBN 0-89141-821-0) how the United States arranged for the Soviets to receive intentionally flawed **process control software** for use in conjunction with the USSR's natural gas pipelines, pipelines which were to generate critically needed hard currency for the USSR.

Reed stated that "The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

The result? A three-kiloton blast in a remote area of Siberia in 1982, which, only by some miracle, apparently didn't result in any deaths. (For context, the Halifax Fire Museum lists the massive 1917 Mont Blanc ship explosion in the Halifax Harbor at a force of 2.9 kilotons.) (but also see www.themoscowtimes.ru/stories/2004/03/18/014.html §

Nation-States Aren't the Only Ones Interested in SCADA Security

- ‘A forensic summary of the investigation, prepared in the Defense Department, said the bureau found "multiple casings of sites" nationwide. Routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan, the visitors studied 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 devices that allow remote control of services such as fire dispatch and of equipment 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.’

“Cyber-Attacks by Al Qaeda Feared”

<http://www.washingtonpost.com/ac2/wp-dyn/A50765-2002Jun26>

[See also: <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html>]

SCADA and Terrorists: Dissenting Opinions, In The Interest of Balance

- “Despite tantalising accounts of Al Qaeda interest in targeting SCADA networks and other critical infrastructure, there actually appears to be little interest among the hacker community in developing tools and exploits against PLC or industrial protocols such as Modbus/TCP or Ethernet/IP. Unlike IT products, tools for automatically "hacking " PLCs, remote IO devices, robots, or Ethernet-based sensors are not readily available. Bedroom hackers with little or no knowledge of automation systems are, in reality, unlikely to cause deliberate harm.”
[<http://ethernet.industrial-networking.com/articles/i15security.asp>]
- “Our research shows that terrorist groups are definitely interested in attacking critical infrastructures," said Eric Byres, research director at the Internet Engineering Laboratory of the British Columbia Institute of Technology in Burnaby. "The good news is that we don't think they have the technical ability yet -- in other words, the combined IT and control system skills needed to penetrate a utility network. The bad news is that they're beginning to acquire some of these skills.”
computerworld.com/securitytopics/security/story/0,10801,97953,00.html

Terrorists Aside, What About Sabotage of SCADA Systems By Others, Such As Insiders?

- In 2000, in Maroochy Shire, Queensland, Vitek Boden released millions of liters of untreated sewage using a wireless laptop, apparently taking revenge against former employers. He was arrested, convicted and jailed.
 - http://www.news.com.au/common/story_page/0,4057,3161206%255E1702,00.html
 - http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

The Boden Incident Wasn't Unusual... Wireless Network Porosity Is Common

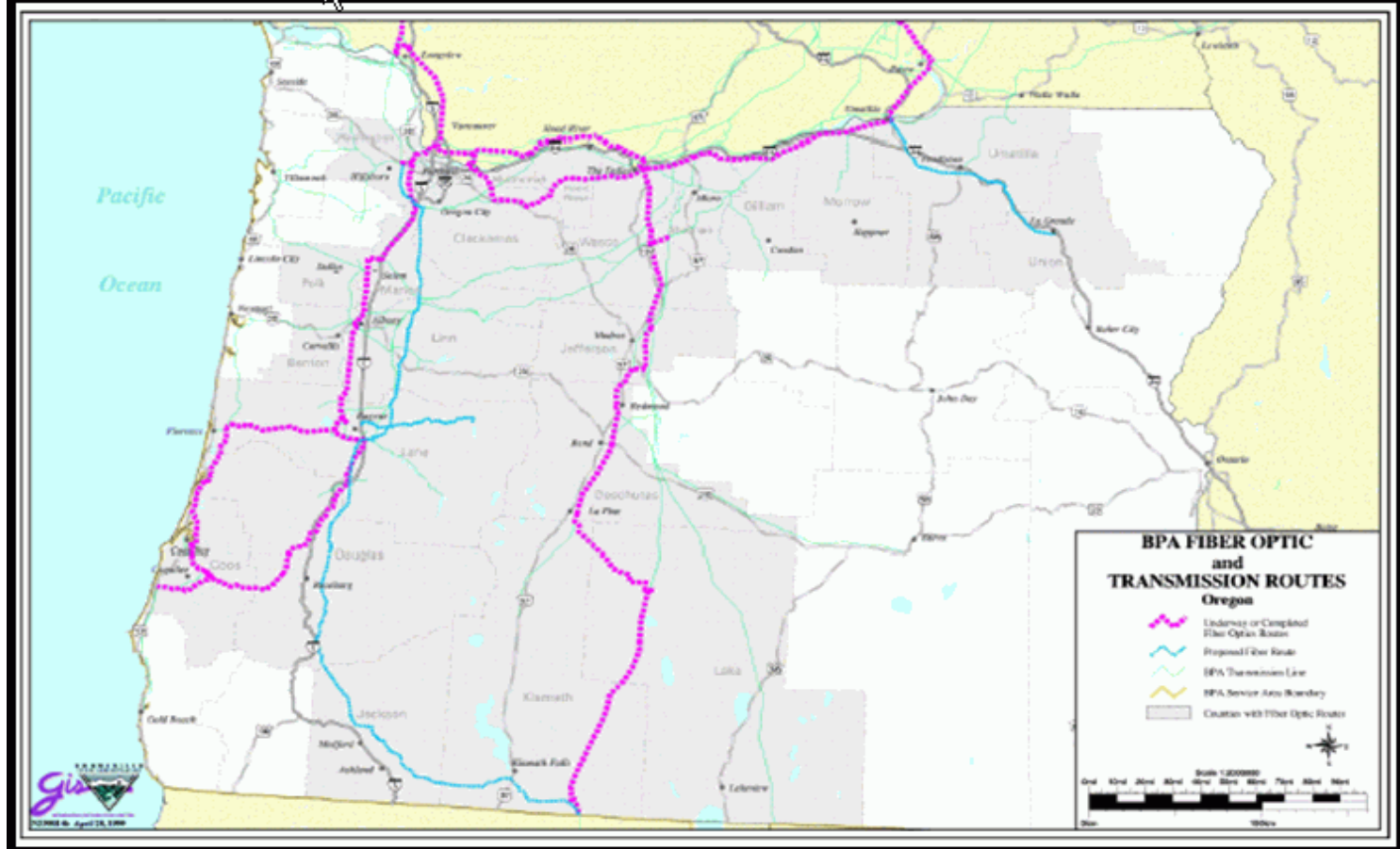
- ‘Paul Blomgren [...] measures control system vulnerabilities. Last year, his company assessed a large southwestern utility that serves about four million customers.’ “Our people drove to a remote substation,” he recalled. “Without leaving their vehicle, they noticed a wireless network antenna. They plugged in their wireless LAN cards, fired up their notebook computers, and connected to the system within five minutes because it wasn't using passwords. [...] Within 15 minutes, they mapped every piece of equipment in the operational control network. Within 20 minutes, they were talking to the business network and had pulled off several business reports.’ <http://www.memagazine.org/backissues/dec02/features/scadavs/scadavs.html>

Vandalism By The Public Is Also A Risk

- For example, simple vandalism is a real/well known risk:
 - “[...] vandals shot out approximately 80 individual insulators on the BPA Cougar-Thurston 115,000 volt transmission line causing it to go out of service at that time. The vandalism occurred near Cougar Dam, which is approximately 25 miles east of Eugene. BPA crews replaced the damaged insulators at an estimated cost of \$6,000. Even though no electrical service to EWEB and Lane Electric Cooperative customers was disrupted by the vandalism, Eugene Water and Electric had to purchase additional power to serve its customers during the 13 hours that it took to repair the damaged line.” <http://www.bpa.gov/corporate/BPAnews/archive/2002/NewsRelease.cfm?ReleaseNo=297>
 - ‘A Washington man who admitted to tampering with more than 20 high-voltage transmission towers in four Western states said yesterday he was trying to point out the power system's vulnerabilities. "I intended to loosen the bolts and by doing so illustrate the vulnerabilities of these towers," Poulin told the judge. Poulin said in a telephone interview before his arrest that he considered his actions necessary to point out that he was able to damage the towers despite being "62 years old, overweight, arthritic, diabetic, half-blind and a cancer patient living on a minimum of 12 medication pills a day.”’ seattletimes.nwsources.com/html/localnews/2001796373_transmission20m.html
- **Those same attacks could also target SCADA control system network infrastructure, which often runs over vast distances on the same physical facilities carrying the power lines.**

For Example, BPA Uses Its Fiber Optic Network to Control Energy Generation and Distribution Assets...

BPA Fiber Routes



BPA Fiber Is Also Use By Others

NoaNet Northwest Open Access Network - About Us - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://www.noanet.net/general/about_us/

TECH SUPPORT

... services from. That NoaNet, in telephone, time on demand, in telephony, and much more are available to anyone connected to the NoaNet backbone. **We also carry mission critical TDM services on our backbone,** providing a network resilient enough to meet even the most stringent demands for levels of service.

The members of NoaNet are nonprofit, community-owned electric and water utilities. They use the NoaNet fiber optic system for utility purposes such as real-time metering, energy management, load control and networking among remote utility facilities. NoaNet provides excess capacity to others on a cost-based, nondiscriminatory basis. Communities are using the NoaNet system to interconnect schools, hospitals, judicial systems, libraries, and **emergency services.** The availability of fiber optics enables economically depressed communities to attract new businesses. NoaNet is also the rural community's on-ramp to the Internet, offering access through Tier 1 providers.

NoaNet has built a fault-tolerant, ring-based system that can scale to meet the increasing demands of rural communities for the foreseeable future. Our network is based on standard architectures and technologies, allowing us to provide new, advanced services on top of tried and true technologies. Utility members and wholesale customers of NoaNet operate communication systems within their own service areas and connect to the NoaNet backbone.

[emphasis added]

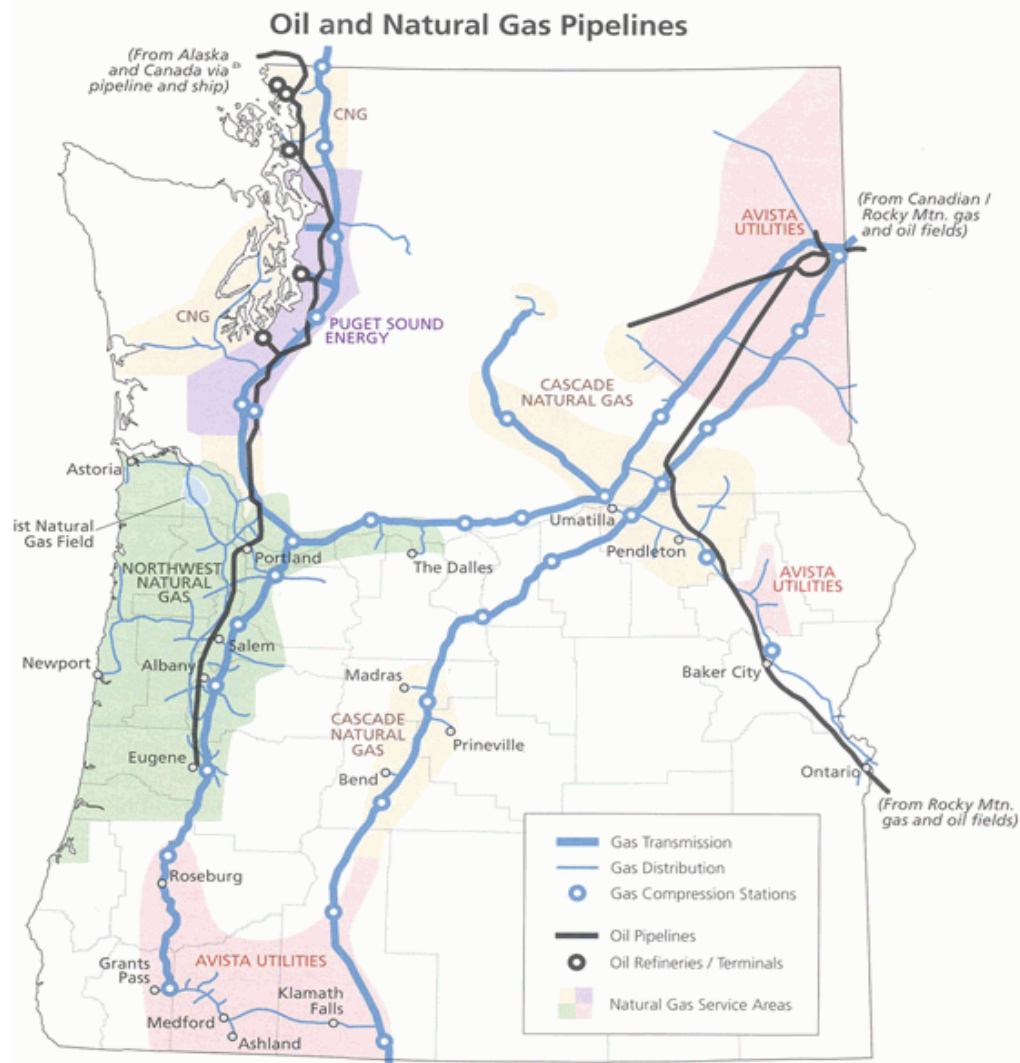
Architectural Measures Designed to Protect Against Accidental Failures May Not Resist Intentional Vandalism (Particularly By Insiders)

- “According to reports, Canadian telecommunications company Aliant (aliant.com) suffered an attack of vandalism on its network **Tuesday night**. The vandals reportedly cut fiber optic cables, leaving thousands of users in Nova Scotia and Newfoundland without phone and Internet service. **Approximately 125,000 people in Newfoundland (half its population) and 5,000 in Nova Scotia were affected.** Services were taken down at about 10:30 p.m. Service was not restored until 7:00 a.m. **Cables were cut in two separate locations. In Newfoundland, a connection to the main network and the backup was targeted. In Nova Scotia, one piece of fiber optic cable was cut. According to Aliant, the individual or individuals responsible had extensive knowledge of telecommunications networks.** Aliant is currently embroiled in a major labor dispute with its 4,200 employees. Several reports have already noted the possible link between the dispute and the attack. The Royal Canadian Mountain Police are investigating. **As of Thursday, Aliant said service had been almost completely restored.”**

<http://www.thewhir.com/marketwatch/van061004.cfm>

III. Oregon Has Critical Facilities

For Example, Pipelines...



Those Pipelines Are Potentially Vulnerable

- “Sixty percent of the Northeast’s refined oil products are piped from refineries in Texas and Louisiana. A coordinated attack on several key pumping stations—most of which are in remote areas, are not staffed, and possess no intrusion detection devices—could cause mass disruption to these flows. **Nearly fifty percent of California’s electrical supply comes from natural gas power plants and thirty percent of California’s natural gas comes from Canada.** Compressor stations to maintain pressure cost up to \$40 million each and are located every sixty miles on a pipeline. **If these compressor stations were targeted, the pipeline would be shut down for an extended period of time. A coordinated attack on a selected set of key points in the electrical power system could result in multistate blackouts. While power might be restored in parts of the region within a matter of days or weeks, acute shortages could mandate rolling blackouts for as long as several years.** Spare parts for critical components of the power grid are in short supply; in many cases they must be shipped from overseas sources.”

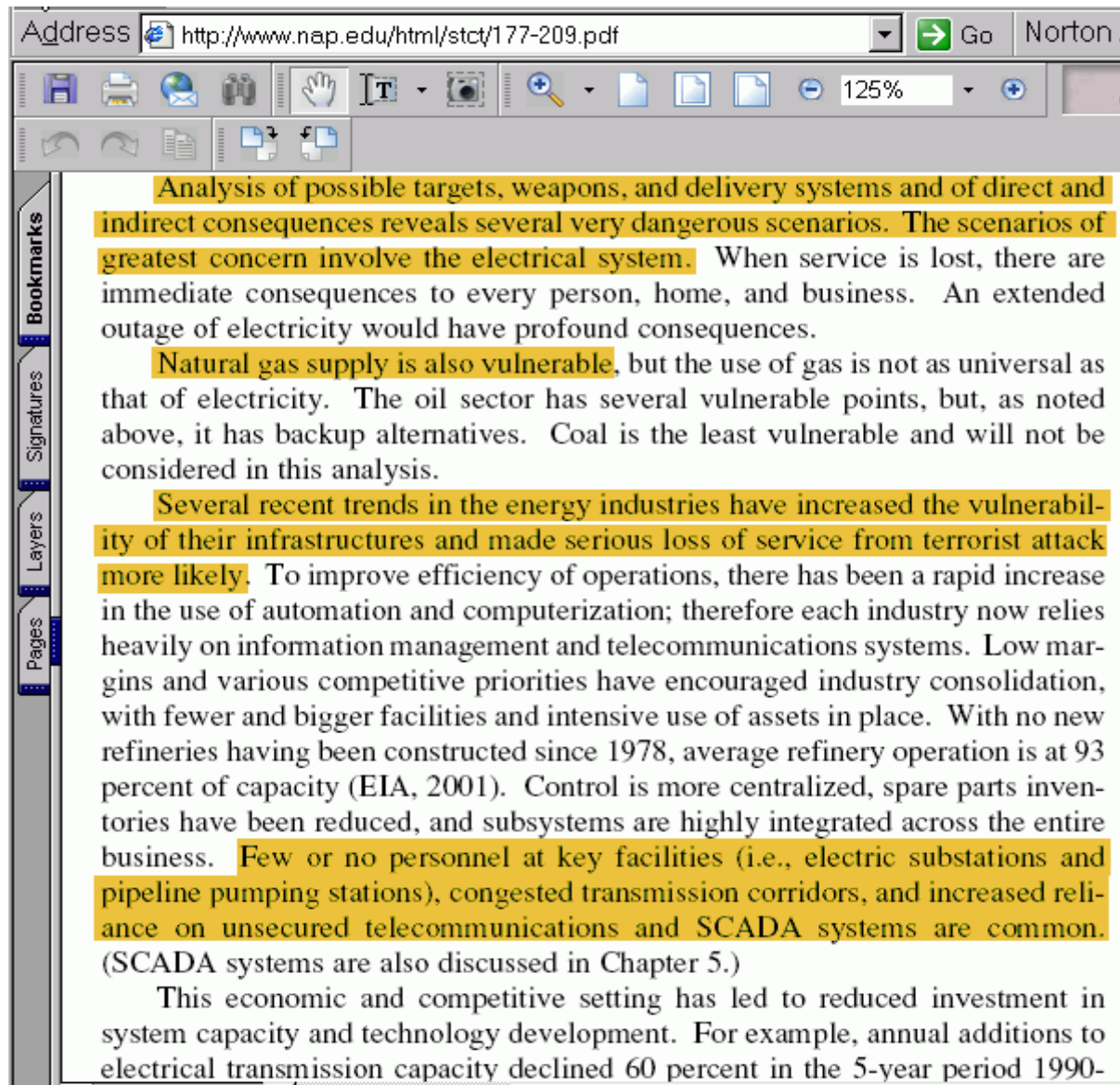
“America Still Unprepared – America Still in Danger,”

http://www.cfr.org/pdf/Homeland_Security_TF.pdf

There Is Too Little Understanding of How Little Reserve Capacity/Redundancy Exists, And the Current Lack of Delivery System Diversity

- One practical example I experienced while traveling in Phoenix during August 2003: a 50-year-old, Kinder Morgan 8" gasoline pipeline failed, effectively reducing the available supply of gas in the Phoenix area by 1/3rd.
 - Loss of that single gasoline pipeline caused serious disruptions to the availability of fuel in Phoenix (stations completely out of fuel, long lines, gas prices skyrocketed, etc.), despite the fact that a second pipeline remained in operation and gas was being trucked into the area to provide additional capacity. (See <http://www.cnn.com/2003/US/Southwest/08/18/phoenix.gas.crunch.ap/>) Why? The delivery trucks that would normally be delivering fuel from the tank farm to the gas stations were now making round trips to Tucson to ferry loads of fuel, one truckload at a time...
 - Ground water contamination also is a serious concern (as of 1/28/2004, monitoring wells found liquid petroleum floating about 3 feet above ground water, about 140 feet below ground, according to reports in the Arizona Daily Star (<http://www.dailystar.com/dailystar/relatedarticles/7534.php>)
- Not a SCADA failure, but an example of how precarious and reserve-free things have become... But let's bring our focus back to SCADA...

The Energy Sector and SCADA...



[emphasis added]

**IV. Failure of Industrial Systems
Such As Pipelines or Electrical
Power Service (Whether SCADA-
Induced or Otherwise Caused)
Can Have Serious Consequences**

Direct Effects, Indirect Effects, and 2nd Order Effects Associated with Incidents

- In some cases, SCADA-related incidents cause *direct* problems: discharge of a pollutant, destruction of property, fatalities.
- In other cases, SCADA-induced incidents may cause *indirect* problems, as in the case of a loss of power: the power failure may not directly cause damage, but its absence may make it impossible for businesses to operate, etc.
- In still other cases, that same loss of power might cause still other critical systems to fail, causing 2nd order effects resulting from the cascading failures, from one critical system to another.

Colonial Pipeline, Murfreesboro TN

Nov 1996 Diesel Fuel Pipeline Rupture

- Quoting from <http://www.nts.gov/publictn/1999/PAB9903.pdf>
“With the pipeline continuing to operate, pressure was increasing at Murfreesboro. The controller did not note the overpressure condition that had developed at Murfreesboro, because the pressure transmitter for the station was downstream of the closed mainline block valve. (See figure 2a.) **The controller was not aware of the actual pressure transmitter location because the supervisory control and data acquisition (SCADA) system schematic for the Murfreesboro station erroneously depicted the pressure transmitter as located upstream of the electric block valve**, as it was at most other stations on the pipeline. [...]
“The controller attempted to reopen the electric block valve at Murfreesboro for the first time at 9:35:02 a.m. Although **the controller saw no indication of high pressure at the station because of the location of the pressure transmitter**, pressure data evaluated since the accident indicated that a high differential pressure, at least 1,700 psig, existed across the valve at that time. This pressure exceeded the design limits (1,440 psi) of the motor used to remotely operate the valve, and the valve did not open. [continues]
- **84,700 gallons of diesel were spilled, with \$5.7 million in damages; as of the time of the report (December 1998), only 43% of the spilled diesel had been recovered.**

The (\$50B) 9/14/2003 U.S. Blackout

- “Starting around 14:14, FE [FirstEnergy] control room operators lost the alarm function that provided audible and visual indications when a significant piece of equipment changed from an acceptable to problematic status. **Analysis of the alarm problem performed by FE after the blackout suggests that the alarm processor essentially “stalled” while processing an alarm event. With the software unable to complete that alarm event and move to the next one, the alarm processor buffer filled and eventually overflowed.** After 14:14, the FE control computer displays did not receive any further alarms, nor were any alarms being printed or posted on the EMS’s alarm logging facilities.

“FE operators relied heavily on the alarm processor for situational awareness, since they did not have any other large-scale visualization tool such as a dynamic map board. The operators would have been only partially handicapped without the alarm processor, had they known it had failed. However, by not knowing that they were operating without an alarm processor, the operators did not recognize system conditions were changing and were not receptive to information received later from MISO and neighboring systems. **The operators were unaware that in this situation they needed to manually, and more closely, monitor and interpret the SCADA information they were receiving.**”

ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/

NERC_Final_Blackout_Report_07_13_04.pdf [emphasis added]

SCADA Failures Can Kill People

- June 10, 1999, a 16" Olympic Pipeline Company pipeline ruptured and released 237,000 gallons of gas into a creek in Bellingham, Washington. 90 minutes after the rupture, the gas ignited and burned 1.5 miles along the creek, killing two 10-year-old boys and an 18-year-old man, as well as causing \$45M in damages. See the NTSB Pipeline Accident Report ("Pipeline Rupture and Subsequent Fire in Bellingham, Washington, June 10, 1999") at <http://www.nts.gov/publictn/2002/PAR0202.pdf> :
- "As the delivery points were switched, pressure in the 16-inch pipeline began to build upstream from the delivery point. Controllers said such an increase was normal and that the incident response was usually to start a second pump at the unattended Woodinville station. **The accident controller issued a command on OLY02 [one of two redundant SCADA systems used] to start the second pump at Woodinville. At 3:18:58, the event log indicates that the system failed to execute the command. At the same time, the SCADA system displayed an alarm from Allen station because of a high discharge pressure of 1,444 pounds per square inch, gauge (psig). Almost simultaneously, the controller operating the other pipeline section noted that the OLY02 system had become unresponsive to his commands.** [continues]
- See also <http://www.cob.org/press/pipeline/whatcomcreek.htm>

The Bellingham WA June 10, 1999 Gasoline Pipeline Rupture and Fire...



Sometimes Failures Aren't Directly SCADA-Related, But Critical Infrastructure Incidents Can Still Teach Valuable Lessons

- Consider, for example, the El Paso Natural Gas 30" Pipeline rupture and fire near Carlsbad NM, August 19, 2000 described by the NTSB at <http://www.nts.gov/publictn/2003/PAR0301.pdf>
- 12 people were camping near the site and were killed in this incident. It is hard to believe that camping near a site of this sort was possible/tolerated, but at the time of the accident the site was privately owned and unfenced, although warning signs were posted (presumably unseen/disregarded).
- Four natural gas transmission pipelines traversed the same site, along with a gas gathering line and a water pipeline (reuse of right of way is common, but it does introduce risk: e.g., damage to one pipeline might result in the damage or destruction of others)
- While the NTSB concluded that SCADA issues did not contribute to this accident, there were multiple interruptions to transmissions between the control center and one of the compressor stations at about the time of the incident; it was established that at least the later of the interruptions was caused by emergency power shutdown of the compressor station, a step which cut power to the local SCADA computer and modem (the station has a UPS, but the SCADA computer and modem weren't powered by it).

El Paso Natural Gas 30" Pipeline Rupture and Fire Near Carlsbad NM, August 19, 2000



Figure 2. Accident area.



Figure 5. Post-rupture fire. At lower left of fireball can be seen the 85-foot-tall support structures for the pipeline suspension bridges.



Figure 6. Looking west at a portion of the crater created by the rupture. The missing section of pipe between the arrows was ejected from the crater.


Another Example of An Instructive Incident: The 14 Day St. Helens, Oregon Ammonia Leak...

Chemical company fined by EPA for 14-day ammonia leak - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://yosemite.epa.gov/r10/homepage.nsf/0/ce190c2a7e1bdb8088256f0e006d218f?OpenDocument> Go Norton AntiVirus

 **U.S. Environmental Protection Agency**

Region 10: The Pacific Northwest

Serving the people of Alaska, Idaho, Oregon, Washington and 270 Native Tribes

[Recent Additions](#) | [Contact Us](#) | [Print Version](#) Search: [GO](#)

[EPA Home](#) > [Region 10](#) >

News Release

Chemical company fined by EPA for 14-day ammonia leak

September 13, 2004

The Seattle office of the U.S. Environmental Protection Agency announced today that El Paso Merchant Energy - Petroleum Company (former owner of Coastal St. Helens Chemical Company) has agreed to pay \$50,345.20 in penalties for failure to notify authorities immediately after an ammonia leak was discovered at its [Coastal St. Helens facility in St. Helens, Oregon](#) (now owned by Dyno Nobel). The company will also purchase \$59,581.00 in new communications equipment for local emergency services.

Over a 14-day period from October 28, 2003, to November 11, 2003, the facility released approximately 40,880 pounds of ammonia into the air from a leak in one of its production units. Over that period, 911 logs contained reports from four citizens of a strong ammonia smell.

After the leak was discovered, it was not immediately reported to the National Response Center (NRC) as required by the federal Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA). The Oregon and Washington State Emergency Response Commissions (SERC), as well as the appropriate Local Emergency Planning Commissions (LEPC) were also not notified in a timely manner as required by the federal Emergency Planning and Community Right-to-Know Act (EPCRA). Emergency responders rely on this information for their safety and that of nearby residents during an emergency.

Ammonia is a colorless gas with a pungent odor. It is used as a refrigerant, a cleaning and bleaching agent, and as an additive in fertilizers, plastics, and pharmaceuticals. In high concentrations, it can cause severe burns to skin, eyes, throat, and lungs, and with high enough exposure, death.

First Time Visitors
Index A - Z

Air Quality
Superfund
Waste and Chemicals
Water Quality

Innovative Solutions
Business & Industry
Concerned Citizens

Simple Loss of Electrical Power Can Have 2nd Order Effects

- Plum Island Animal Disease Center (<http://www.ars.usda.gov/plum/>), just off the coast of Long Island, NY, is the nation's only center for the study of infectious animal diseases. A recently released book, Lab 257 by Michael Christopher Carroll (Harper Collins, NY, 2004, ISBN 0-06-001141-6) describes how on Sunday, August 18th, 1991 Hurricane Bob, a category 3 hurricane, hit Plum Island. Quoting from Carroll's book:
-- 'Normally, Plum Island's power was supplied by the Long Island Lighting Company, via an undersea cable on the ocean floor. But the LILCO power grid shorted out and mainland power to the island laboratory failed. Fortunately, there was a backup plan. Oil-fired power generators kicked in at Building 103, the Plum Island emergency power plant, and supplied the island with electricity. The huge generators in Building 103 were old, but well maintained and effective. Building 103 supplied Lab 257 with power through overhead power lines and through underground cables that provided "redundancy." [...] Hurricane winds, gusting over one hundred miles per hour, topped the island's overhead electric poles. [...] Three months prior to Hurricane Bob, in a flurry of sparks and a wisp of gray smoke, one of the underground conductors shorted out; with it went the underground cable as a source of electricity. [...] [The laboratory administrator], Dr. Breeze and his facility manager, Ernest Escorsica, thought replacing the cable was too expensive. The cost: \$70,000. It would have to wait for next year's budget.'

Loss of Electrical Power Can Have 2nd Order Effects (cont)

- Continuing from Carroll's book, "To maintain biological containment in 257, B Crew [four persons] needed to preserve sewage treatment, storage freezers, steam and negative air pressure." All of that required electricity.
 - The sewage holding tank, containing biologically contaminated animal waste (feces, urine, blood, vomit, etc.) quickly filled and overflowed, contaminating large areas of the lab; staff had to pump that sewage without respirators or other protective gear
 - The lab's freezer, which held samples of foot-and-mouth disease, African swine fever, Rift Valley fever, and other extremely dangerous pathogens, normally at negative 158 degrees Fahrenheit, began to thaw without power; the emergency liquid nitrogen transport container, was missing/unavailable.
 - The biologically hot areas of the lab, normally sealed with pressurized rubber gaskets, lost their seal integrity. With the seals gone, the lab's normal negative air pressure normalized to ambient levels; emergency air dampers which were supposed to automatically close in case of power loss, failed open. Insects were seen flying in and out of the biologically hot labs.
- In September, the four men who worked during that incident were RIF'd. Two subsequently came down with illnesses: one with a severe flu-like disease which lasted six years, and which was never able to be positively diagnosed; the other with an arthritis-like condition that lasted 18 months.
- See also: <http://www.gao.gov/new.items/d03847.pdf>

**V. And Say What You Will,
The Security of SCADA Systems
IS Often Poor**

The Core Of This Talk: SCADA'S Problems

- Having established that dire things can happen when critical infrastructure fails, what can we say about SCADA's structural issues without saying too much?

SCADA Security Today : Where Enterprise Network Security Was 5-10 Years Ago

- “The present state of security for SCADA is not commensurate with the threat or potential consequences. The industry has generated a large base of relatively insecure systems, with chronic and pervasive vulnerabilities that have been observed during security assessments. Arbitrary applications of technology, informal security, and the fluid vulnerability environment lead to unacceptable risk. [...] **Security for SCADA is typically five to ten years behind typical information technology (IT) systems** because of its historically isolated stovepipe organization.”

Federal Technical Support Working Group (TSWG)’s

“Sustainable Security for Infrastructure SCADA”

<http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf>

(emphasis added)

The “Hidden Half” of the Network

- Traditionally network and security folks have focused virtually all their attention on the “enterprise” side of the network, ignoring the parallel “hidden” half of the network associated with process control systems and distributed/embedded systems.
- Process control systems and distributed/embedded systems may use different protocols, do use different jargon, and no one ever really mentions them. They are out of sight and out of mind, and everyone assumes that things are being “handled” by the hardware guys.

“Hidden” Does Not Always Equal “Physically Separated”

- In the old days, process control systems used proprietary protocols and ran with serial communications (e.g., RS232 connections or modems) or even on physically separated (“air gapped”) private/dedicated networks, but that’s no longer routinely the case.
- These days, process control systems often run using MODBUS/TCP on the enterprise LAN and over the Internet; process control traffic may be commingled with web pages, email, P2P traffic, VoIP traffic, etc.

But Don't Take My Word For It...

- **'MISCONCEPTION #1** – *“The SCADA system resides on a physically separate, standalone network.”*

‘Most SCADA systems were originally built before and often separate from other corporate networks. As a result, IT managers typically operate on the assumption that these systems cannot be accessed through corporate networks or from remote access points. Unfortunately, this belief is usually fallacious.’

“Understanding SCADA System Security Vulnerabilities”
<http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf> (RIPTech, Inc., January 2001)

Serious Consequences of SCADA-Related Compromises

- While enterprise network security is undeniably important, unlike enterprise network security, SCADA compromises can have real world life safety impacts.
- Enterprise network security breach: financial consequences, customer privacy is compromised, systems need to be rebuilt, spam gets sent, etc., but life goes on.
- SCADA security breach? Property can be destroyed and people can be hurt or killed (e.g., recall some of the examples mentioned earlier).

Simple Protocols

- Because SCADA devices with embedded controllers tend to have limited computational power, and have historically been connected via low speed serial lines, SCADA protocols tend to be quite simple, with little or no protection against spoofing, replay attacks, or a variety of denial of service attacks.
- ‘In a demonstration at a recent security conference, [Jeff Dagle, a PNNL EE] hacked into his testbed system and tripped an electrical breaker. The breaker then signaled the SCADA software that it had opened. But the SCADA controller did not respond because it had not instructed the breaker to open. It was a classic denial-of-service attack. "We were demonstrating a weakness at the protocol level itself," said Dagle.’ <http://memagazine.org/backissues/dec02/features/scadavs/scadavs.html>

Long Life Cycle Devices

- Industrial plants, and the instrumentation they include, tend to be long life cycle projects – ten, fifteen or twenty year project lives are by no means uncommon. As a result, the devices that may be deployed as part of that construction may be virtual antiques by the time the facility is finally decommissioned, and there's no provision for refreshing those devices the way you might upgrade out of date PCs in an office.
- "Anti-virus software doesn't work on these SCADA systems," said Robert Childs, information security analyst at the Public Service Company of New Mexico, who spoke at NetSec about the challenges in working with SCADA vendors to get them to comply with the new rules. "Many of these systems are based on old Intel 8088 processors, and security options are limited to us." <http://napps.nwfusion.com/news/2004/062104secwrap.html>

Windows-Based Control Stations

- SCADA devices are often controlled from central monitoring stations (MTUs, or “master terminal units”). Historically those were Unix-based systems, but many contemporary MTUs are now Microsoft Windows based.
- “The end-of-life for Windows NT is having a big impact on manufacturers.”
http://www.digitalbond.com/SCADA_Blog/2004_07_01_archive.html

Hard-to-Upgrade Remote Devices

- Remote devices (RTUs and PLCs) also tend to be hard to upgrade :
 - the device may use an OS and application that was burned to ROM, and which is not rewritable (“upgrade” == replacing ROMs)
 - the device may be physically sealed and not upgradeable, or be located in a difficult location, or have no removable media
 - the vendor may no longer be in business, or may not be producing upgrades, or the vendor may not be allowing upgrades

Certifying Patches

- An example from the embedded system world:
“Health care IT professionals say medical device makers prohibit them from changing the systems and even from running anti-virus software in some cases. These IT administrators say manufacturers often are slow to supply software patch updates and routinely claim the Food and Drug Administration (FDA) requires approval of patch-base changes. However the FDA says it has no such rules...”

<http://www.nwfusion.com/news/2004/070504hospitalpatch.html>

Need For Positive Control ==> Simple Known/Shared Passwords

- Because of the need for positive access and control, there is a trend toward simple, known, and shared passwords. Users like to avoid situations such as: “Do you know the password to turn off the nuclear reactor before it melts down? I forgot mine today...”
- But there’s hope: people in the SCADA community are beginning to talk about strong auth systems:
http://www.digitalbond.com/dale_peterson/ISA%20July%20Event.ppt

Common Passwords Across Multiple Devices

- There's also the sheer issue of managing passwords for thousands of devices – passwords will tend to be common across devices as a practical matter (this is much like SNMP community strings)
- And of course those passwords aren't changed very often (if at all), even when staff transitions occur or years have gone by...

Access Control Granularity and Accountability

- Related to the problem of shared, simple passwords is the issue of poor access control granularity; again, like SNMP, in most cases access control is “read” (everything) or “read/write” (everything).
- Accountability with common passwords is poor/non-existent, which may be one reason that transaction logging also may be limited. (Any bets how long it will take to get something like syslog-ng or SDSC Secure Syslog for SCADA systems?)

Plain Text (Unencrypted) Traffic

- These days, few of us would be willing to send our passwords over plain text transmissions paths (as we would when using telnet), yet plain text transmissions are still very common in the SCADA world.
- One notable exception: the AGA/GTI SCADA Encryption initiative...
<http://www.gtiservices.org/security/>
- In the realtime world, encryption overhead and jitter may be the crucial problems to overcome...

All Traffic Is On Just One Port

- In many cases, SCADA traffic will be on just one port such as 502/tcp (e.g., Modbus/TCP). This is both good and bad.
- The use of a single port (or just a couple of ports) makes it easy to track that traffic, or to poke a hole in firewalls to allow that traffic to pass, but it also makes it easy for the bad guys to scan for connected devices, and it makes it impossible to do port-based selective filtering.

Few Firewall Options

- Speaking of firewalls, SCADA-protocol aware firewall choices are pretty limited out there right now; I'm aware of:
<http://modbusfw.sourceforge.net/>
and that's about it.
- Where are the commercial SCADA-protocol-aware firewall vendors? I'd love to find out that there are dozens out there that are available which I've missed...

Critical Control Traffic on a Best Effort Network

- In some cases, SCADA systems may be impacted incidentally, as a side effect of a more general problem (e.g., frame relay network congestion and outages associated with the Slammer worm). See for example “Slammer worm crashed Ohio nuke plant network,” in <http://www.securityfocus.com/news/6767/> citing http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf

VI. What Must We [Network/IT Folks] Do?

SCADA Systems Must Be Hardened

- All the security areas just mentioned need to be reviewed and addressed on a system by system basis, which in some cases will mean substantial new investments/forklift upgrades, or even concerted pressure on vendors for whom new security requirements may come “like a bolt out of the blue.”

That Said, Many Vendors Are Ramping Up

- Cisco deserves a big “atta boy” for its Critical Infrastructure Assurance Group:
http://www.cisco.com/security_services/ciag/
- You may also want to check out the Cyber Security Industry Alliance (CSIA) at
<https://www.csialliance.org/> whose members include over a dozen leading security-related vendors.
- Vendors of SCADA-enabled devices might be moving a little slower...
- Make sure vendors know what SCADA security products YOU need them to be making!

Hard-won Lessons From Enterprise IT Need to Be Tech Transferred to SCADA Networks and Systems

- Much of what's being faced in the SCADA world has already been hashed through and fixed in the enterprise IT world. Those solutions, where suitable, need to be “thrown over the wall” to SCADA networks and systems so SCADA folks don't “reinvent the wheel.” IT folks need to visit with the process control guys and gals.

Our Local SCADA Infrastructure Needs to Be Secured

- While admittedly many SCADA issues are national in scope, there are undoubtedly SCADA control systems here in Oregon – perhaps even SCADA systems operated by people in this room today – which need review.
- Are those local SCADA systems secure?
- What about the networks they use?
- Do you see local port 502/tcp traffic on your enterprise backbone or transit links? Should it be there?
- Are you seeing probes targeting SCADA facilities from offsite? Are you reporting or blocking those probes?

Speaking of Probes...

- One familiar technique from enterprise network security is the “honeypot,” or a system that *looks* vulnerable/exploitable, but which is actually well instrumented and being run solely to capture evidence of miscreant misbehavior.
- There’s one SCADA honeypot project:
<http://scadahoneynet.sourceforge.net/>
but how many folks are actually deploying SCADA honeypots? Not very many, I suspect...
Maybe deploy one?

Update Intrusion Detection Systems

- Work has just recently begun on a DHS-funded research project focused on developing Snort signatures for MODBUS/TCP; see:
http://www.digitalbond.com/SCADA_Blog/2004_05_01_archive.html
- The excellent open source protocol analyzer Ethereal (www.ethereal.com) and a number of other common protocol analyzers also support Modbus protocols.

If You Do Security Training, Add SCADA Security to The Syllabus

- If you teach network security courses at your company, or as part of the training the cybercrime investigators receive, make sure SCADA security becomes part of that syllabus.
- Besides the topics covered already in this talk, some additional areas which may be worth consideration include...

Embedded Real Time Operating Systems (RTOS)

- We all know some version of Windows (or Unix), but quick check: how many of you are also familiar with embedded RTOS's like:
 - Integrity from <http://www.ghs.com/>
 - LynxOS or BlueCat from <http://www.lynuxworks.com/>
 - QNX Neutrino <http://www.qnx.com/>
 - RTOS-32 from <http://www.on-time.com/>
 - TinyOS from <http://www.tinyos.net/>
- What are their respective security strengths and weaknesses? SHOULD you know?

How About Hardware Topics, Such as Programmable Logic Controllers?

- Unless you're an electrical engineer, you probably never had a chance to learn about PLCs, even though there's excellent support for educational use of programmable microcontrollers such as Basic STAMPs from www.parallax.com or more traditional ladder-logic programming PLCs such as Toshiba's T1 (see <http://xtronics.com/toshiba/plcnf.htm> and http://xtronics.com/toshiba/Ladder_logic.htm)

**VII. What Are A Few Things
Critical Infrastructure Industries
Should Be Thinking About?
What Should They Be Fixing?**

The Potential List Is Long, And Parts Aren't Well Suited to Public Discussion

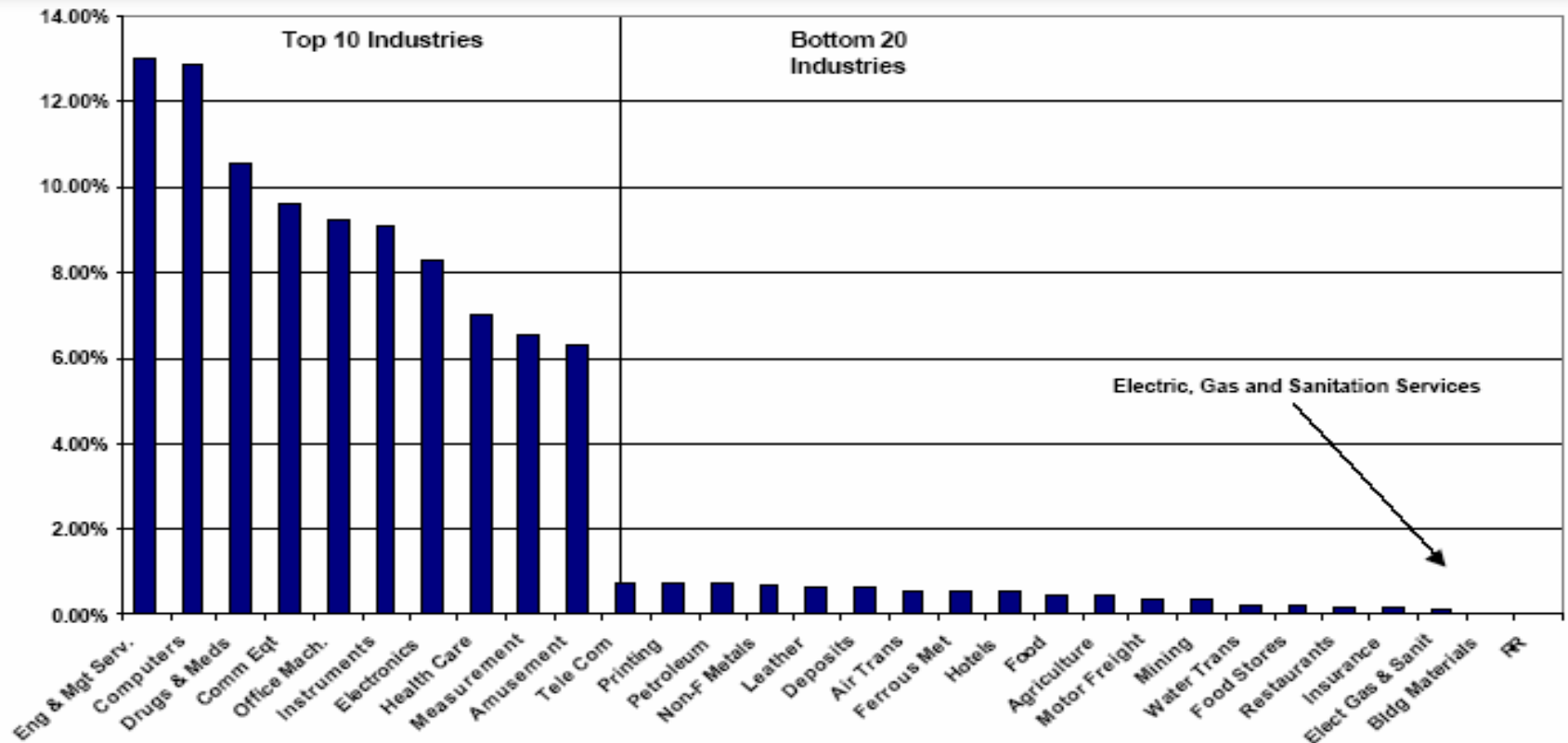
- What's required may vary from industry to industry
- It is hard to make concrete suggestions without identifying current vulnerabilities
- We'll offer just a few strategic observations, and then a few tactical suggestions...

Work With Government Agencies to Insure Security Priorities Have Been Set Appropriately

- If you were to compare security initiatives in the area of critical infrastructure (particularly in the electricity generation and distribution area, and the pipeline area) to security initiatives for commercial aviation or nuclear power, how would that balance look to you?
- “Congress Passes DHS Spending Bill”
<http://www.fcw.com/fcw/articles/2004/1011/web-dhs-10-11-04.asp>
-- \$32 **Billion** to DHS
-- \$67.4 **Million** for “cybersecurity”
[For context, one V-22 Osprey tilt-rotor aircraft costs \$100 million according to <http://www.washingtonpost.com/wp-dyn/articles/A25659-2004Oct11.html>]
- See also “Cybersecurity for the Homeland,” House Subcommittee on Cybersecurity, Science, and Research & Development (released yesterday)
<http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf>

Increase Industry Spending On R&D (Including Security R&D)...

Context: R&D Expenditures*



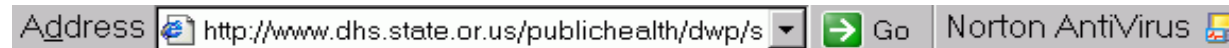
*R&D expenditures as % of net sales

EPRI

[chart from Massoud Amin's "R&D challenges in R&D challenges in Security of the Electricity Infrastructure", Feb 2004]

Do Vulnerability Assessment/Security Auditing/Penetration Testing of SCADA Systems

- Some named industries are already required to do this sort of thing...



Federal Regulations

The Bioterrorism Act of 2002 requires all Community Water Systems over 3,300 population to complete Security Vulnerability Assessments and submit them directly to the Environmental Protection Agency (EPA). Do not submit them to DHS-DWP or the counties. Within six months of the federal deadlines, these water systems must also develop or revise an existing ERP and incorporate the results of their vulnerability assessments. See table below for the submittal schedule:

Population Served	Vulnerability	ERP
	Assessment Due Date	Due Date
3,301-49,999	June 30, 2004	Dec. 31, 2004
50,000-99,999	Dec. 31, 2003	June 30, 2004
100,000+	Mar. 31, 2003	Sept. 30, 2003

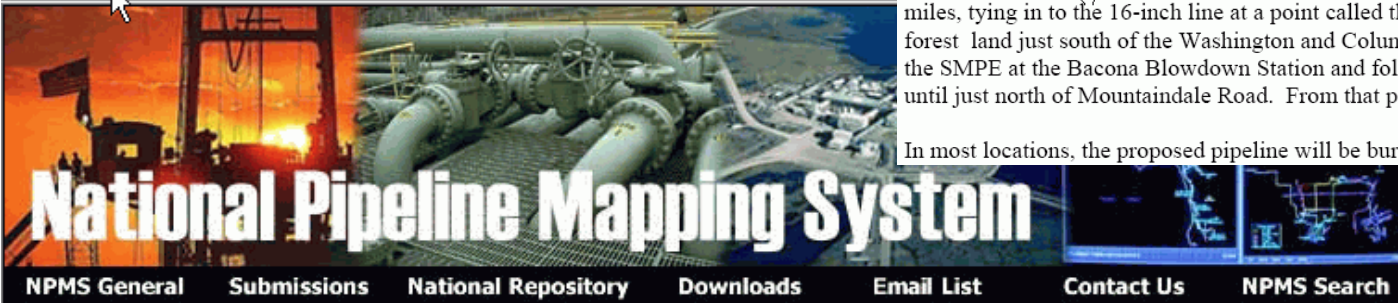
Instructions for complying with and submitting a vulnerability assessment are available on EPA's website at www.epa.gov/safewater/security. On this website you will also find a Vulnerability Assessment factsheet that summarizes the key points that an assessment must address along with guidance tools. Some of the Vulnerability Assessment guidance documents recognized by EPA to be

Be Sure Any Security Exercises Are Realistic

- Don't do it the NRC way...
GAO: "NRC: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened" (September 2003)
<http://www.gao.gov/new.items/d03752.pdf>
-- "The [security] exercises were conducted infrequently, against plant security that was enhanced by additional guards and/or security barriers, by simulated terrorists who were not trained to operate like terrorists, and with unrealistic weapons. In addition, the exercises did not test the maximum limits of the design basis threat..."
-- "According to NRC officials, they provided the licensee with up to 12 months' advance notice of OSRE [force-on-force] exercises so that it could assemble a second team of security guards to protect the plant while the exercise was being conducted. However, the advanced notification also allowed licensees to enhance security prior to the OSRE exercises, and they were not required to notify NRC of any enhancements to their security plan. As a result, according to NRC officials, during the exercises, many plants increased the number of guards that would respond to an attack; added security barriers, such as additional fencing; and/or added defensive positions that they did not previously have..."

Think About Information Management and Target Intelligence Collection

Address http://www.npms.rspa.dot.gov/data/dot_data_pipeline.htm



Data
Dissemination

DOT - OPS DATA

The Office of Pipeline Safety (OPS) has discontinued providing open access to the National Pipeline Mapping System. Recent events have focused additional security concerns on critical infrastructure systems. Due to these concerns, OPS no longer provides unlimited access to the Internet mapping application, pipeline data, and drinking water Unusually Sensitive Area data. OPS is committed to provide pipeline related data to pipeline operators complying with integrity management programs and to community officials.



Miller station, USA

Customer Northwest Natural Gas (NW Natural)
Product 501-KC5
Location Mist, Oregon - 50 miles (80km) northwest of Portland

Project Description

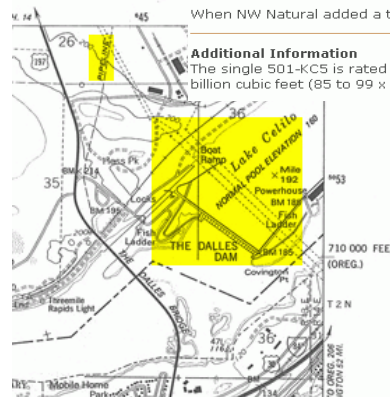
Following the discovery of Oregon's first commercial reserves of natural gas, NW Natural began operation of Miller station in 1979.

After extraction of all the gas, NW Natural converted the depleted wells into storage reservoirs for gas bought in off-peak months.

When NW Natural added a third reservoir to cope with demand, extra compression was needed for which a 501-KC5 was selected.

Additional Information

The single 501-KC5 is rated at 5,500 hp (4.1 MW) and helps fill the Flora, Bruer and Calvin Creek 1 reservoirs at Miller Station with 3 to 3.5 billion cubic feet (85 to 99 x 106 cubic metres) of working gas.



Reconsider The Extent To Which Buried == “Inaccessible and Safe”



[home](#) | [pay](#) | [register](#) | [sign in](#) | [services](#) | [site map](#)

[Buy](#) [Sell](#) [My eBay](#) [Community](#) [Help](#)

💡 Giving this as a gift? Print a [Gift Preview](#) to show it's on the way!

[Back to list of items](#)

Listed in category: [Business & Industrial](#) > [Construction](#) >
Also listed in: [Business & Industrial](#) > [Construction](#) >

CASE 680 C LOADER BACKHOE

Bidder or seller of this item? [Sign in](#) for your status



[Larger Picture](#)

Current bid: **US \$3,150.01**

[Place Bid >](#)

Time left: **3 days 20 hours**
7-day listing
Ends Dec-10-04 07:46:25 PST

Start time: Dec-03-04 07:46:25 PST

History: [2 bids](#) (US \$3,000.00 starting bid)

High bidder: [419richards](#) (0) 🌟

<http://ljworld.com/section/agriculture/story/115960>

For nearly three years, Shultz said, he has been trying to get Williams Pipeline Co. to bury an exposed 3-foot section of gasoline pipeline that runs through the field.

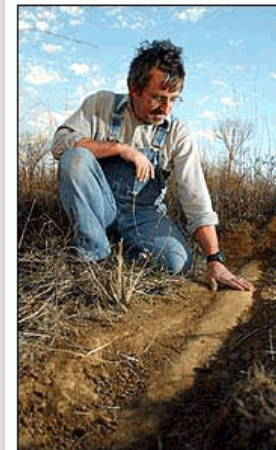
"They've done nothing but give me lip service," Shultz said.

His anger and concern intensified last week after more than 8,000 gallons of gasoline from a pipeline belonging to Williams spilled into a field north of Lawrence. A farmer ruptured the shallow pipeline while plowing. No one was injured in that accident.

Shultz is worried he may not be so lucky.

Leo Haynos, chief of pipeline safety for the Kansas Corporation Commission, said Shultz's worry was justified.

"He has something to be concerned about," Haynos said, adding that if gasoline from last week's rupture had spewed a different direction and contacted a hot surface on the tractor, an explosion would have been almost certain.



Thad Allender/Journal-World Photo
After a nearby farmer

Though there are parts of the country with more buried pipelines, Haynos said there were a considerable number in the Lawrence area because many lines converge at terminals in Kansas City.

"If you look at a pipeline map, as you get closer (to Kansas City), you'd see more," he said.

Shultz said the exposed pipeline was on a hillside and the soil that covers it has washed away. It is in the area of North 1802 and East 1700 roads west of U.S. Highway 40 near the Douglas-Leavenworth County line. He has been farming the land several years.

Three times since he noticed the exposed pipeline, Shultz said, he has called Williams. Three times the same representative has been sent to examine it.

"The first time he said he didn't think it was anything to worry about," Shultz said. "He keeps saying he'll

Increase/Improve ROW Surveillance

Nat'l Academies Press, Making the Nation Safer: (20

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://www.nap.edu/openbook/0309084814/html/207.html>

Advanced Intrusion Detection Systems

Improved surveillance techniques for the extended rights-of-way of pipeline systems are needed. The present method of monitoring thousands of miles of pipeline right-of-way—through visual inspection in an overflight—is inadequate. Pipeline operators need new surveillance techniques capable of highly reliable detection of unwanted activity. Surveillance technologies developed for defense and intelligence agencies may be useful in defense against terrorist attacks, as well as against simple right-of-way encroachments, on widely distributed oil and gas assets. These technologies could include remotely operated drone aircraft, satellite surveillance systems, intelligent-software-based analysis of surveillance images to detect unwanted activity, change-detecting sensors, and intrusion-detection cameras designed to sense unusual vibrations or noises (see Recommendation 6). Intrusion detection technology R&D could be managed through the existing DOD and DOE programs. Its application to the oil and gas industries could be coordinated by industry groups such as the National Petroleum Council.

CHAPTER SELECTOR:

6. Energy Systems, pp. 177-209

GO TO PAGE:

GO

[TABLE OF CONTENTS](#)

PAGE
207

[PRINTABLE PDF PAGE](#)

CHAPTER



PAGE



GO

Usually, some of the best places to hunt are on utility right of ways (electric and telephone), and pipeline right of ways. The utility companies have crews that work around the year cutting all trees and brush away from the power lines and telephone lines.

There are thousands of oil and gas wells located in East Texas, and hundreds of miles of oil and gas pipelines, buried underground. The oil and gas pipeline companies do not allow any trees to grow on the pipeline right of way. They do this by bush hogging (mowing) all of the right of ways several times during the year.

Because the underbrush is so thick in places, deer and other wildlife use these pipelines to travel at times, when moving between feeding grounds and bedding areas. This makes an ideal place to build deer stands and to hunt, if you like to walk and hunt. Because you can sometimes see several hundred yards down a pipeline or power line right of way, you may see several deer cross at 200 or 300 yards. Sometimes these pipelines will curve and the deer seem to want to cross at the curves or where they feel they have less chance of being seen. You can find out where to set up your stand by finding deer trails between the bedding and feeding area.

These pipelines and right of ways also make excellent areas to plant food plots such as oats, rye, wheat and other foods for the times when there are no acorns for the deer to find. By planting several different plots, you will make a feeding area that will attract deer from all over the area.

Deer stands on these pipelines and right of ways should be well hidden, and placed in the hunting area several months before the season. Even if deer are using a trail, if you put in a deer stand or blind, the deer will alter

70

[emphasis added]

Improve Remote Monitoring of Key Sites

- If you have fiber to remote facilities, you have sufficient bandwidth to allow for extensive video and audio instrumentation of that facility, and for reports from sophisticated intrusion detection systems. Those systems should be tied into SCADA systems, and system responses should be recalibrated in response to identification of active or potential threats.
- Alternatively, aren't key remote facilities (many of which cost millions to build, and which are virtually irreplaceable) important enough to justify round-the-clock on-site technical and security personnel?

Assume Technical Staff May Need Security Support at The Site of Incidents

- If you assume the severity of an incident is proportional (in part) to its duration, it would be reasonable to assume that terrorists might actively attempt to prevent crews from accessing and repairing a damaged facility. Assuming this is true, technical staff may need security staff to protect them from attack or to help them avoid IEDs/booby traps while restoring a damaged facility. [Protection of technical staff should be a very high priority given that there may be a limited number of qualified and knowledgeable individuals available.]

When a SCADA Incident Occurs, LE & Company Staff On Site Routinely Use VHF/UHF Radios for Communications; People May Be Listening, Even With Digital Trunking

Digital Trunking Handheld Scanner - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://www.radioshack.com/product.asp?cookie%5Ftest=1&catalog%5Fname=CTLG&category%5Fname=CTLG%5F>

Digital Cameras & Imaging
Parts, Tools & Wire
Phones & Radio Communications
School & Office
Security & Home Automation
Toys & Gaming
TV, Satellite & Video
Unique Gadgets & Gifts

FREE SHIPPING
on orders over \$25. Order in time for the holidays! [Details](#)

SIGN UP AND SAVE.
Get special offers and news.
[Sign up now](#)

NEED HELP DECIDING?
1.800.THE.SHACK (1.800.843.7422)

SITE TOOLS

- BATTERY FINDER
- CELLULAR/PCS ACCESSORIES FINDER
- CREDIT CARD SERVICES
- HOME THEATER HOOKUP GUIDE
- iGo SOLUTIONS
- REBATE CENTER

Digital Trunking Handheld Scanner

\$499.99 Brand: **RadioShack**
Catalog #: **20-526** Model: **PRO-96**

(Pricing and Availability may vary outside the contiguous 48 United States.)

Where to Buy

On-line	In Stock
1-800-THE-SHACK (1-800-843-7422)	In Stock

Check your local store for availability: Zip code [Go](#)

[Owner's Manual](#) [Click here](#) [Search for Support Documents](#) [Click here](#)

This handheld scanner has an abundant memory capacity, able to store frequencies in 5500 memory channels. Plus, you can store up to 16,500 ID codes in one "working" 500 channel, 1500 ID code scanner with 11 "virtual" scanner pages of memory! This scanner follows APCO 25 digital and virtually all analog Motorola® and GE/Ericsson EDACS trunked systems. More and more cities are using these trunked systems, allowing city services to share the same set of scanner frequencies. Conversations on these systems start on one frequency, then shift to a different one with each transmission. This scanner can follow these systems. Patent Pending.

Need Related Products?
Check the products that you would like added to the cart and then click the **Add to Cart** or **Update Cart** button.

- ☐ 800MHz Scanner Antenna 20-283 **\$15.49**
- ☐ 9V/300mA AC-to-DC Power Adapter 273-1767 **\$13.99**
- ☐ Adaptaplug B 273-1705 **\$4.99**
- ☐ 4-Pack "AA" Energizer®

North American railroad frequencies - Microsoft

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address <http://zippy.cso.uiuc.edu/~roma/r-freqs/>

Union Pacific

161.310 -- [AAR channel 80] -- car department (Portland)
161.340 -- [AAR channel 82] -- car department (various locations)
160.410 -- [AAR channel 20] -- channel 1 (ex-MP road)
160.470 -- [AAR channel 24] -- channel 2 (ex-MP road)
160.515 -- [AAR channel 27] -- channel 3 (ex-UP road)
160.740 -- [AAR channel 42] -- channel 4 (ex-UP road)
160.590 -- [AAR channel 32] -- channel 5 (ex-MKT road)
160.290 -- [AAR channel 12] -- executive mobile telephone
160.605 -- [AAR channel 33] -- MOW mobile telephone (various locations)
160.950 -- [AAR channel 56] -- UP motor freight (Seattle)
161.145 -- [AAR channel 69] -- yard (Chicago)
160.830 -- [AAR channel 48] -- yard (Milpitas, Warm Springs)
160.115 -- yard (San Jose, Milpitas, Stockton)
160.680 -- [AAR channel 38] -- yard (various locations)

Virginia Southern

161.310 -- [AAR channel 80] -- all operations

When Upgrading Communication Systems, Retain Those Moldy-Oldie Communication Systems For Potential Backup SCADA Use

BONNEVILLE'S INTERNAL NEEDS

TECHNICAL AND OPERATIONAL

Bonneville requires each of its communication systems to have a reliability of 99.986%. Bonneville is moving from an analog microwave radio system to a digital system. The agency's digital options were fiber-optic cable, microwave radio, and satellite. Satellite was rejected due to long time delays, low bandwidth, and high cost. Therefore, Bonneville is installing a primarily fiber-optic system, supplemented by a digital microwave system. Reliability will remain Bonneville's paramount reason for ensuring high-quality communications.

- Fiber-optics allows the agency to reduce its dependence on Federal radio frequencies. Frequency diversity, which is the mainstay of Bonneville's analog system, is no longer acceptable for radio systems; acquiring new frequencies near metro areas and along the Canadian border is very difficult. Bonneville's options are becoming limited because the Federal Communications Commission (FCC), on behalf of the Federal Treasury, is continuing to auction off government frequencies.
- In locations where Bonneville has passive reflectors and long paths, digital radios cannot be used as a replacement.

Improve Vetting of Key Staff; Review Personnel Policies

- Insider threats will always remain a serious potential issue; insiders have specialized knowledge and tools, trusted access, etc.
- Are you thoroughly screening your staff? (You can see what the federal government requests for their sensitive positions at “Questionnaire for Public Trust Positions” at http://www.opm.gov/forms/pdf_fill/SF85P.pdf)
- Have you visited with your personnel office about the potential impact of labor actions on staffing requirements and staff access to critical systems? (labor issues were involved, for example, in the water facility sabotage that reportedly occurred on Plum Island, as described in the report at <http://www.gao.gov/new.items/d03847.pdf>)

Provide An Appropriate Mechanism By Which Staff Can Share Crucial Security Issues :-)

<http://tsa-screeners.com/start/modules.php?op=modload&name=News&file=article&sid=3465>



We are deeply troubled by the "April Fool's Day Incident 2004" where all of the CTX X ray machines at PDX were up and operating but we were ordered to let the machines operate without a TSA screener at the controls. This would permit improvised explosive devices, hazardous materials and the like to be placed onto passenger aircraft if the X ray machine over looked something that a fully trained screener would see. Nearly every screener in baggage inspection wrote an urgent missive to management that aviation security had been severely compromised and that all CTX machines must have an actual, trained, experienced screener operating the million dollar machine.

One concerned screener printed out a copy of what the X ray machine had revealed in a previous search; a hand grenade replica that the CTX machine had cleared but which a trained experienced screener identified on the X ray screen for further investigation. Next to the picture of the hand grenade in the luggage, he drew a box with the caption "Put a picture of your little girl here on this airplane." or words to that effect.

Years ago, an actual improvised explosive device (IED) was placed in luggage at PDX. The CTX X Ray machine failed to "alarm" on the threat but an alert screener, looking at the X Ray screen saw the components and stopped the luggage from being placed onto an airplane. Therefore, during the nearly 24 hour April Fool's Day Incident, an IED could have easily been placed on a passenger aircraft at PDX.

After nearly 24 hours of this bizarre and potentially disastrous procedure, trained and experienced screeners were once again permitted by TSA management to operate the six, million dollar CTX X Ray machines the American tax payers purchased for our use to enhance their safety.

[excerpt from a petition reportedly sent on 8/23/04 to DHS Secretary Tom Ridge, TSA Director David M. Stone, US federal inspector general, the TSA Inspector General, the Oregon and State of Washington Congressional Delegations, and the Oregon and Washington Governors]

Questions?

- Thanks for the chance to talk today!