

PROTECTION OF CONTROL SYSTEMS AT DRINKING WATER UTILITIES

John McNabb

john@infraseclabs.com

ICSJWG 2012 Spring Conference

May 9, 2012



John McNabb, about me:

RESEARCHER & IT PRO

- Infrastructure Security Labs (infraseclabs.com)
- South Shore PC Services
- Bowdoin College, B.A. Psychology

FORMER WATER COMMISSIONER

- 1997-2010, small Massachusetts town

FORMER LOBBYIST

- Mass. Dept. of Environmental Protection
- Clean Water Action

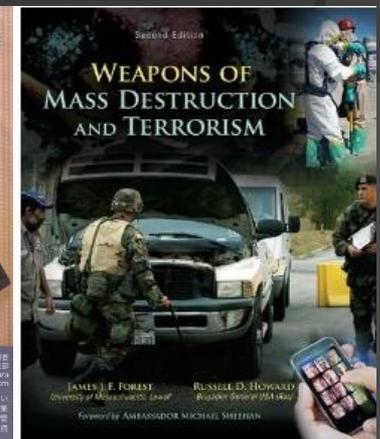
SPEAKER

- 2012 – Black Hat Summit @ DESIGN West, HOPE Number 9, ICSJWG, Notacon, Source Boston, Thotcon
- 2011 – Shmooccon, Black Hat USA+2011, DEFCON 19
- 2010 - The Next Hope, Phreaknic 14, DEFCON 18
- 2008 - American Water Works Association (AWWA)
- 2007 - 2009 - NE Water Works Association (NEWWA)

AUTHOR

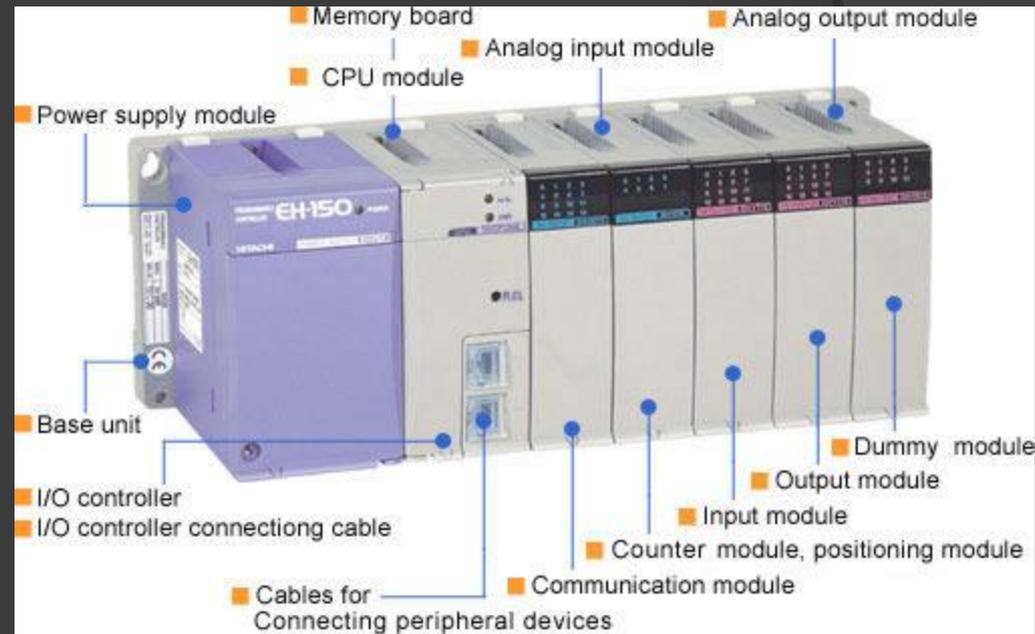
- Journal of the NEWWA – 3 articles on water infrastructure
- Book chapter: “*Chemical and Biological Threats Against Public Water Systems*” in Weapons of Mass Destruction and Terrorism, 2nd Ed. Howard & Forest (McGraw-Hill, 2012)

NOT A CONTROL SYSTEMS EXPERT!



Definitions & Acronyms

- ⦿ ICS – Industrial Control system
- ⦿ DCS – Distributed Control System
- ⦿ SCADA – Supervisory Control And Data Acquisition
- ⦿ PLC – Programmable Logic Controller



Why I Am Giving This Talk

- Drinking Water is a “**Critical Infrastructure**” - essential for life, commerce, existence of society
- But, the security of drinking water does not get enough attention
- PROBLEMS & ISSUES ARE SILO'D; WATER PROS, IT PTOS, SCADA PROS – IN SEPARATE SILOS
- The water sector lists “cyber attack” as a high priority to protect against – but is doing little to stop it!
- There are real threats and security issues -- but not enough resources or the will to fully address these threats!
- There is now an **explosion** of newly discovered vulnerabilities in control systems... including those in water utilities.
- But, the federal budget for water infrastructure security is declining.
- Water utilities and other critical infrastructure are now spending only about 10% of what is needed to repel 95% of cyber attacks
- This is not just about the hardware and software of a computer system, but the ecosystem it is in, and the unique security challenges and issues it therefore presents to society.

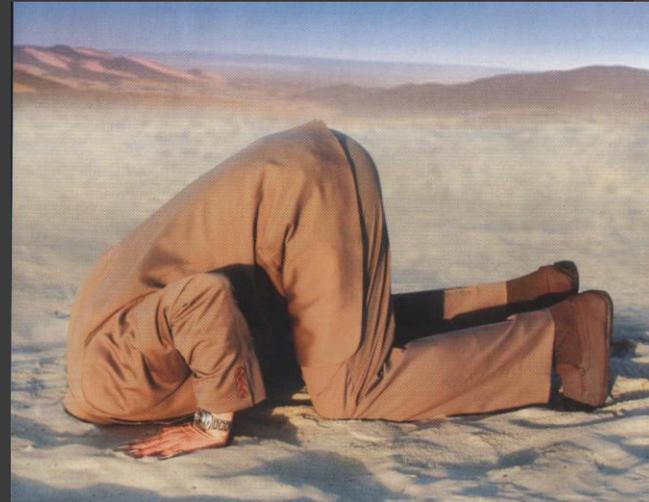
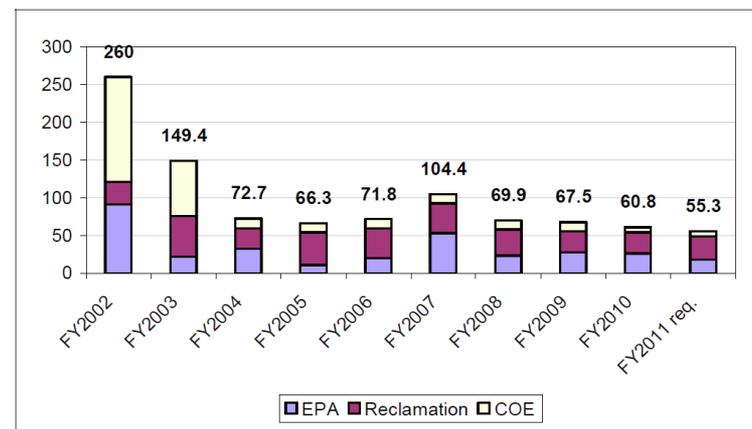


Figure 1. Water Infrastructure Security Appropriations

Millions of Dollars



Source: Compiled by CRS.

The Illinois 'Water Hack' That *Never Happened*

- In November, 2011 a pump at an Illinois drinking water utility burned out.
- The local Fusion Center in a draft 'not for public release' report, said that it was caused by an attack from a foreign hacker with a Russian IP address.
- Joe Weiss wrote about the report in his blog and read it to many news outlets, causing a firestorm of media reporting on 'the first hack of a water system' by foreign hackers.
- DHS and FBI immediately discounted the report and finally concluded that it was not caused by a foreign hacker.
- Wired Magazine reported that yes it was not a foreign hacker, the Russian IP address was there because a consultant for the utility vacationing in Russia had remoted into the system to check on it.
- Hacker named Pr0f, angry at DHS dismissal of the hack, posted his successful intrusion into a South Houston water system, to show how easy it is to hack into these systems.
- While the frantic reporting on this alleged hack did include calls for more to be done to secure drinking water systems, it does not appear that anything has been done to better secure them
- The internet news reports of the hack live on forever, and some more recent internet articles and blogs still report on the hack as if it had really happened.
- Even though it is clear now that the pump damage was not caused by a foreign hacker, the 'fact' that it 'did occur' lives on. This is the "*continued influence effect of misinformation*" effect.



***Does this mean we are
safe?***

“US energy and water utilities are under daily cyber attack”

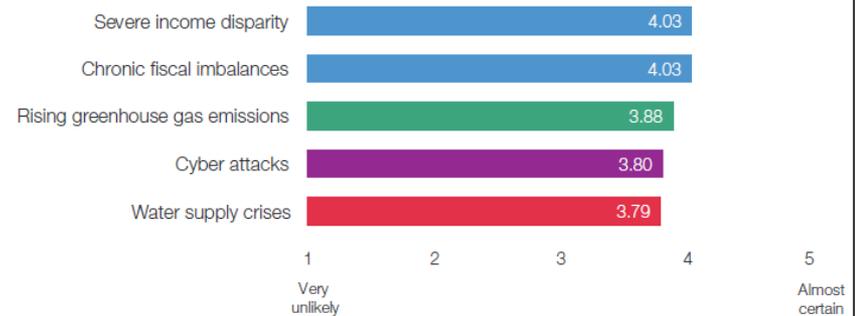
- Spear phishing attacks on water utilities
- Social engineering attempts on water utilities
- Occasional reports of people doing recon of water utilities across US
- And ‘suspicious’ activity
- Insider hack of Key Largo wastewater plant computer system
- Intruders break into water treatment plant
- Team Cymru 2008 ‘heatmaps’ of scans of SCADA systems
- So, is there some potential attack or attacks in the works? Or are these all non-connected activity?



How Important is Water?

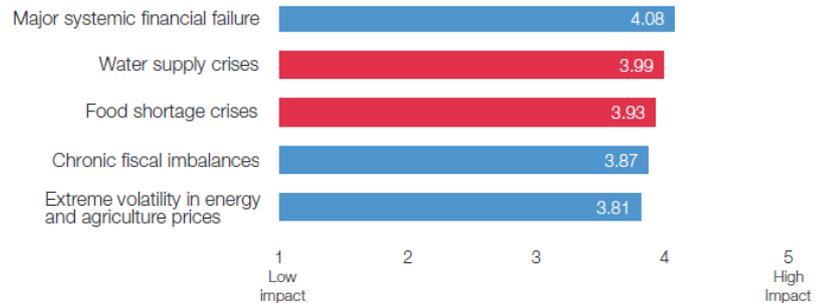
- Critical Infrastructure; can't live, cook, or work without it – for long.
- Source of wars and conflicts, target of terrorists, since the beginning of civilization
- Global Risks 2012 Report ranks “water supply crisis” in top 5 for Likelihood and Impact

Figure 4: Top 5 in terms of Likelihood



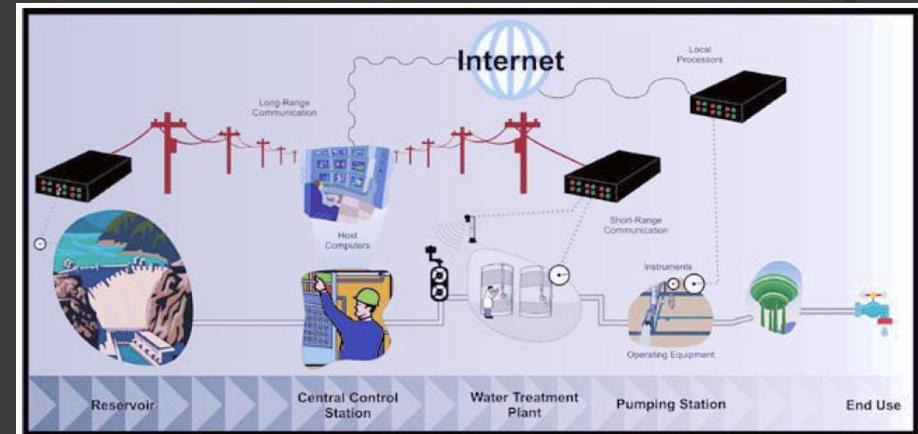
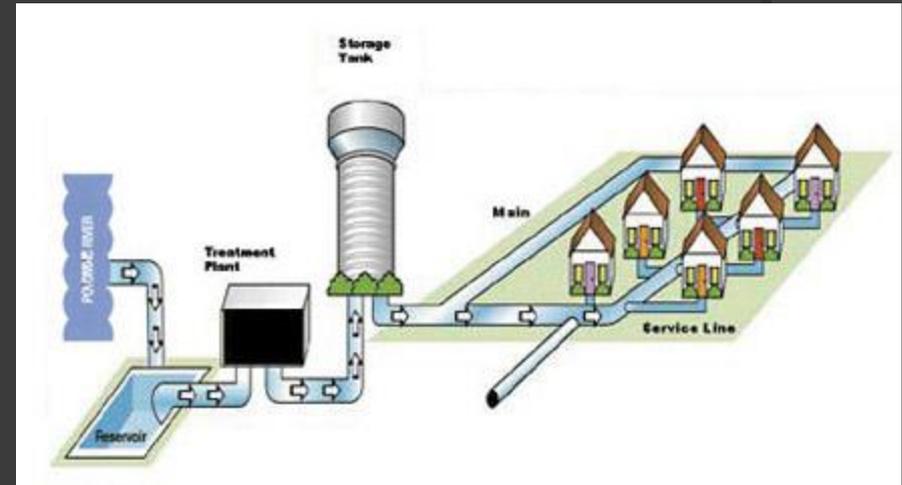
Source: World Economic Forum

Figure 5: Top 5 in terms of Impact



How Does A Water Utility Work?

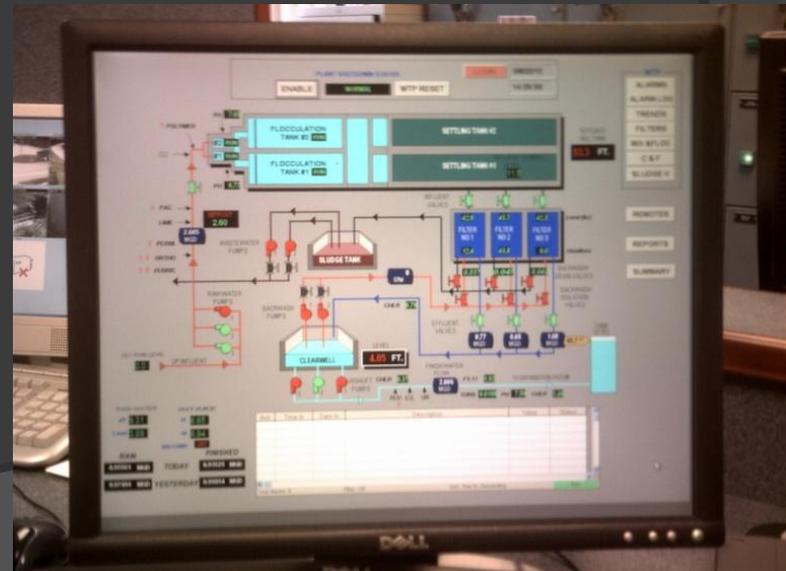
- Source (surface, ground)
- Dams
- Treatment (process control)
- Finished Water Storage
- Pump Stations
- Distribution (pipes, valves, hydrants, blowoffs)
- PSA requirements: **P**ressure, **S**afe, & **A**vailability of water
- Operators must: keep water flowing, meet regulatory standards, maintain pipes & capital infrastructure, issue bills & collect revenue



Source: GAO (07-1036)

Control Systems 101

- ICS Control Loop consists of:
- Process sensors to transmit measurement variables transmitted to controller, and
- Controller (PLC) interprets signals & generates control signals to process actuators, and
- Process changes result in new sensor signals, etc., and
- Human Machine Interface (HMI) allows human operator to configure set points, control algorithms, and operating parameters, and provides status info and alarms
- Different from conventional IT



Industrial Control System - Process

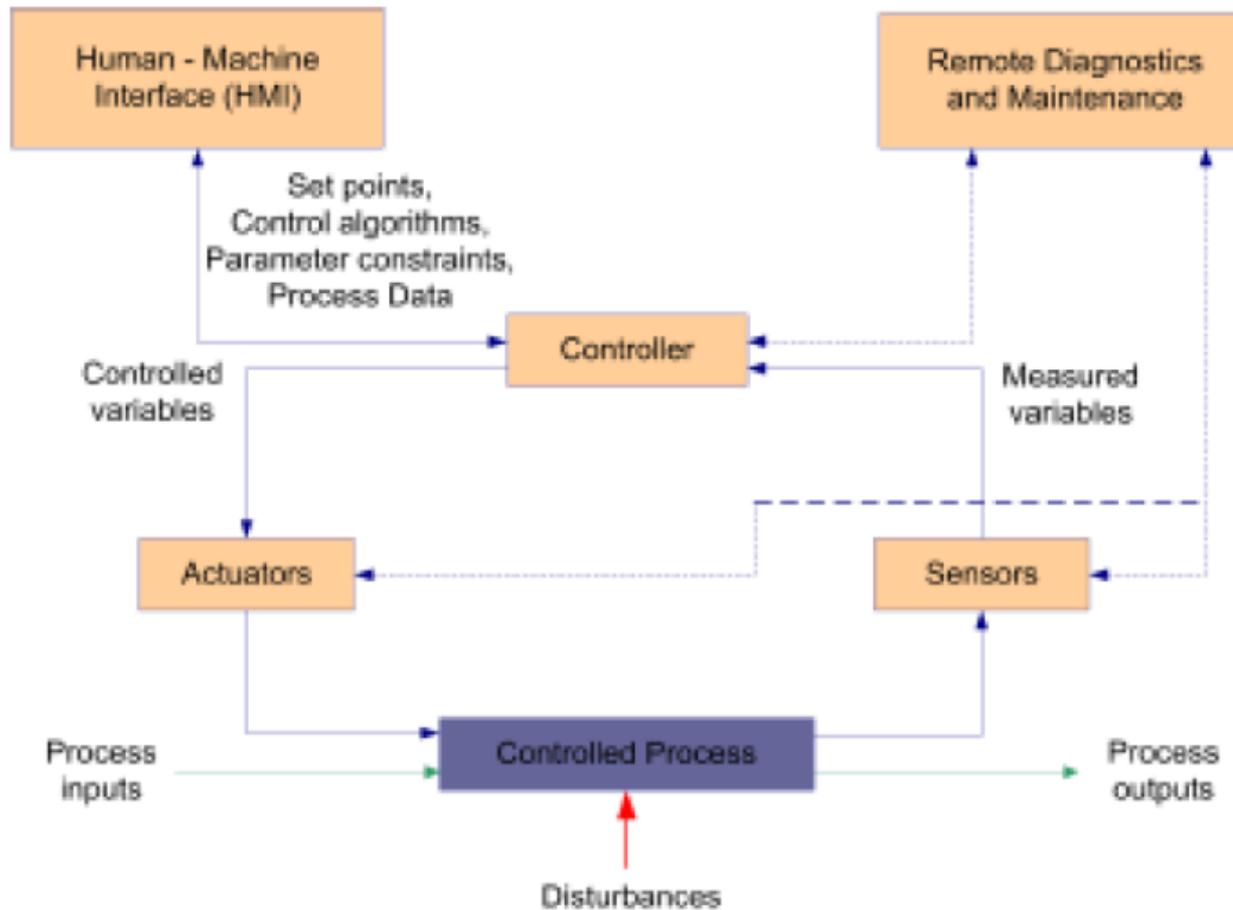
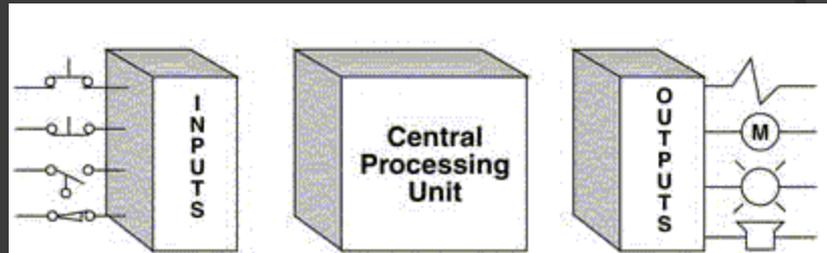


Figure 1 Key Control Components

Control System Hardware - PLC



What is a PLC input/output?

INPUT

Sensing Devices
Switches and Pushbuttons
Proximity Sensors
Limit Switches
Pressure Switches

OUTPUT

Valves
Solenoids
Motor
Actuators
Pumps

PLC Operations consist of four steps

1. Input Scan: Scans the state of the Inputs
2. Program Scan: Executes the program logic
3. Output Scan: Energize/de-energize the outputs
4. Housekeeping

ICS Different than IT:

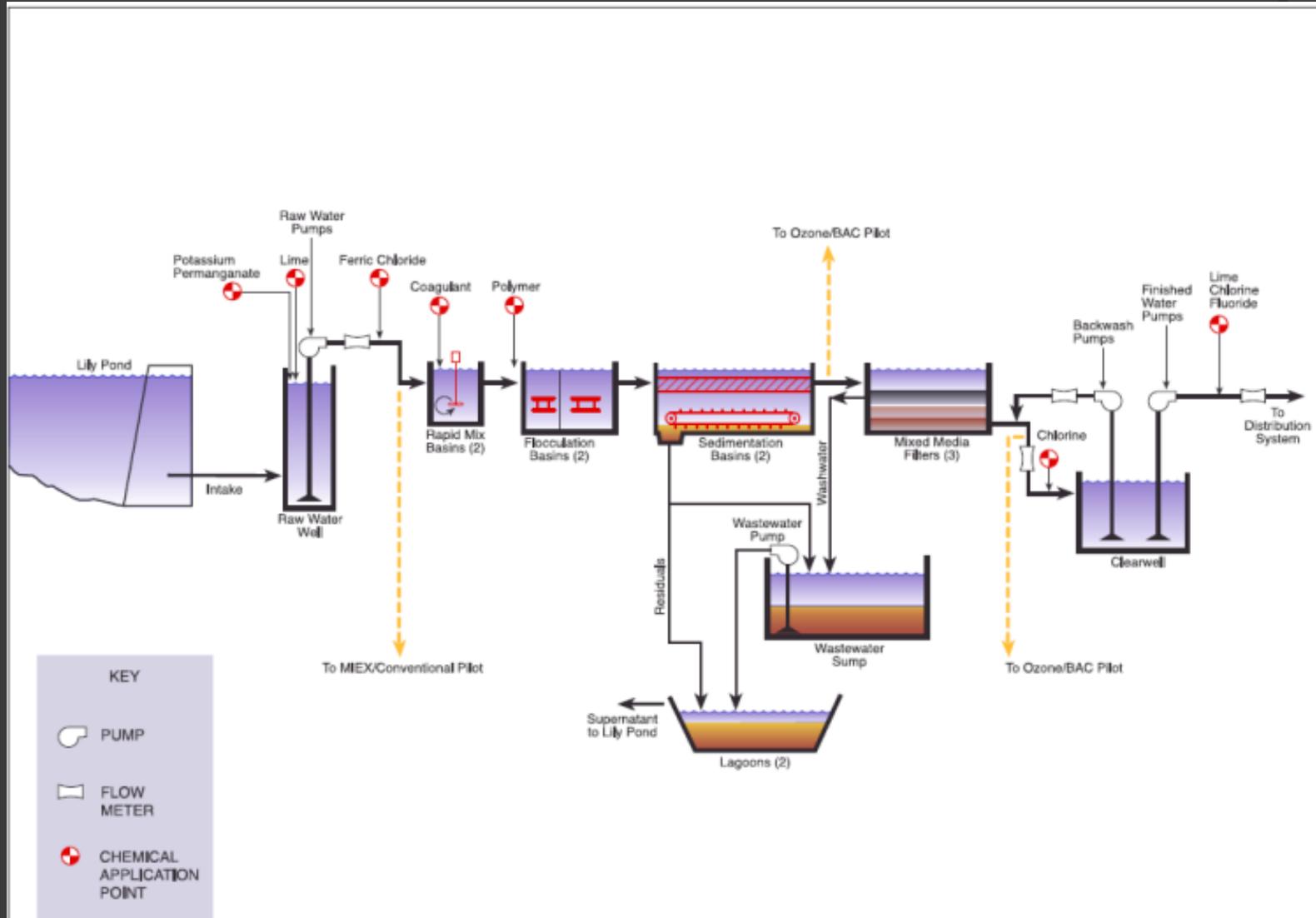
Control Systems

- Focus
 - Safety
 - 100% Availability
 - Electro-mechanical
 - No updating, Aged equipment
- The Language
 - RTUs, PLCs, IEDs
 - DNP, Modbus
 - Low Bandwidth
 - Analog & Digital
- The Vendors
 - Allen Bradley(AB)/Rockwell, Honeywell, Siemens, Johnson Controls

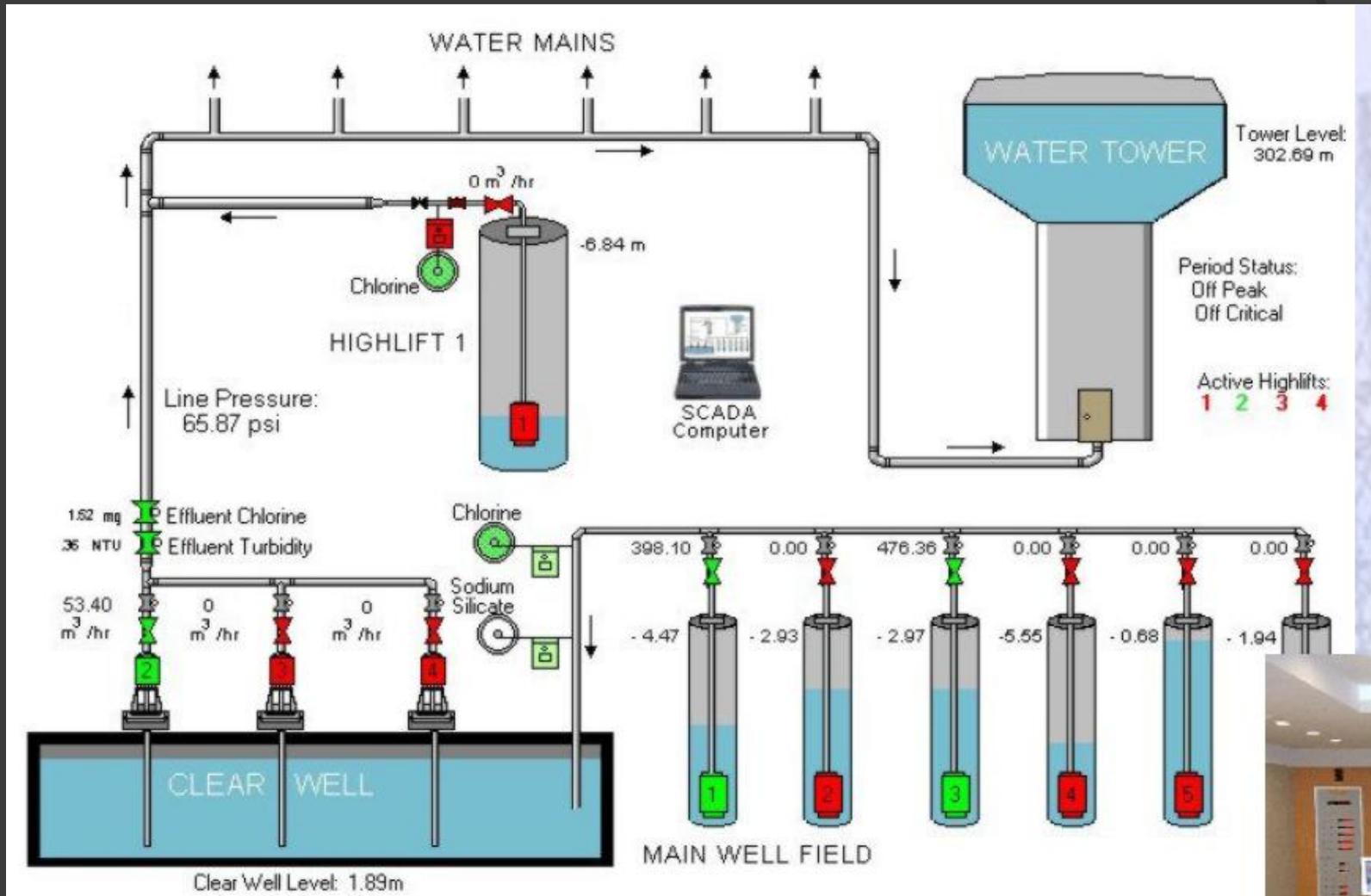
Computers

- Focus
 - Security
 - 99.5% Availability
 - Electronic
 - Continuous Updating, New
- The Language
 - Routers, Switches, Servers
 - IP, Ethernet
 - High Bandwidth
 - All Digital
- The Vendors
 - IBM, Microsoft, CISCO, Dell

Water DCS – Treatment Process



Water SCADA – Supply/Distribution



Potential Effects of a Cyber Attack?

- Interfere with the operation of water treatment equipment, which can cause chemical over or under-dosing
- Make unauthorized changes to programmed instruction in local processors to take control of water distribution systems, resulting in disabled service, or reduced pressure flows of water into fire hydrants
- Modify the control systems software, producing unpredictable results
- Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions
- Change alarm thresholds or disable them
- Prevent access to account information, or steal account information
- Although many facilities have manual backup procedures in place, failures of multiple systems may overtax staff resources—even if each failure is manageable in itself
- Be used as ransomware



Real Water Computer

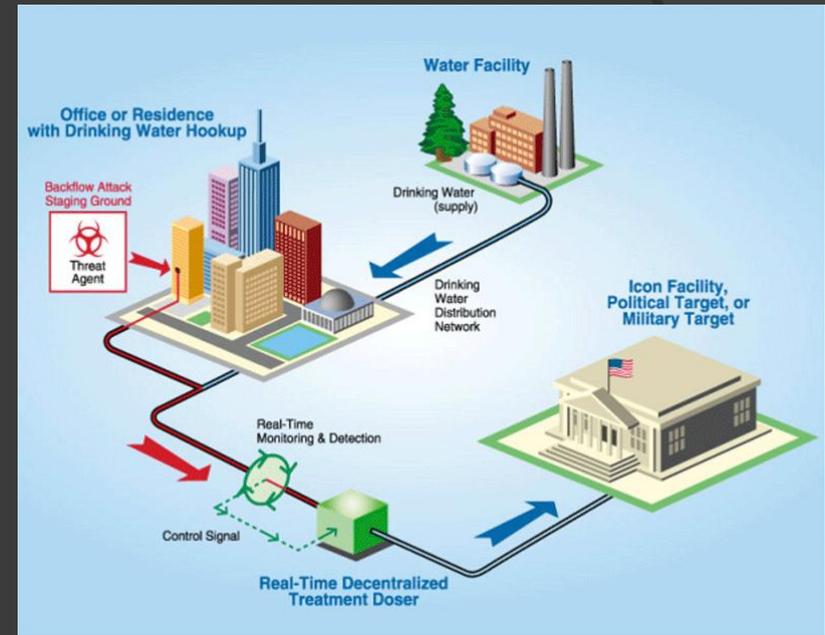
‘Glitches’

- ⦿ Prevented water tank from being filled, boil water order. Watertown, NY, 2009
- ⦿ Caused water tank to overflow, Howard, Michigan
- ⦿ Water production stopped cold, Lake Chelan, Washington
- ⦿ False low pressure reading turned on pumps that blew seven water mains. Jersey Heights, NJ, 2009
- ⦿ Prevented reverse 911 calls to alert people about water main break. Contra Costa, CA 2012
- ⦿ Very high, erroneous water bills. Davie, 2012
- ⦿ Erroneous shutoff notices. Detroit MI 2011
- ⦿ Chlorination shut off, making water undrinkable, Lewiston, ME



Poisoning of Water Scenario

- Cyber poisoning of water is possible, but is not the optimal way to do so
- Could alter treatment plant to:
 - Eliminate chlorination
 - Increase chlorination
 - Change other chemicals
- BUT --Most effective water poisoning method is localized injection of poison from a hydrant or a building directed at a single building with a high value target
- Best countermeasure is real time contaminant monitoring in the distribution system, and in all such buildings with high value targets



Are sensitive US Government Buildings protecting the flow of water from the outside distribution system into the building?

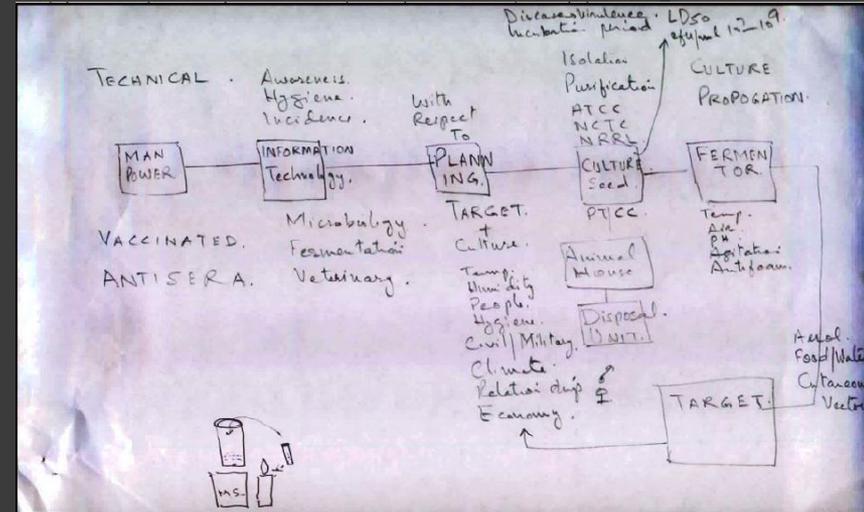
Potential Attackers?

- **Vandals** – defacement of water tank or web page
- **Hacktavists** – deface web page
- **Criminals** – theft of money or materials (copper)
- **Competitors** – no; utilities are monopolies
- **Nation-State Actors** – attack US thru infrastructure
- **Terrorists** – have threatened to poison US drinking water
- **Insiders** – personal reasons, assist outsiders to attach utility



Terrorists – Cyberterrorism?

- Despite death of Osama bin Laden and other successes in crippling Al Quada, Rand says its going to be around another 10-15 years
- Al Quada has repeatedly threatened to 'poison' US drinking water. **They have MOTIVE.**
- Al Quada. Docs recovered at Tarnak Farms, Afghanistan, show their research on poisoning drinking water with biotoxins.
- On the other hand, it is argued that this would be a "sub optimal" target, very unlikely, for terrorists who prefer planes & bombs. *Poisoning drinking water also more effective thru physical than cyber.*
- Hezbollah may also have an interest in attacking within the US
- Also threat of local 'lone wolves' and home grown terrorists & history of local groups attacking water
- Terrorists don't seem to have the ability to attack infrastructure via cyber, but Stuxnet may be changing that equation. **They may now have MEANS.**
- However, so far the Stuxnet attack on the nuclear facilities in Iran is the only documents instance of actual cyberterrorism that damaged physical assets



Media depiction of a hacker

Nation-State Actors

- Nations are more likely than others to have capability to launch major cyber attack
- **China** - interested in espionage & industrial espionage; but also cyber attacks in US
- **Iran** – working on nukes, but the Cyber-Hezbollah act as proxies for them.
- **North Korea** – has launched cyber attacks on South Korea
- **Russia** – hotbed of cyber criminals; but nation still practicing industrial espionage against the West



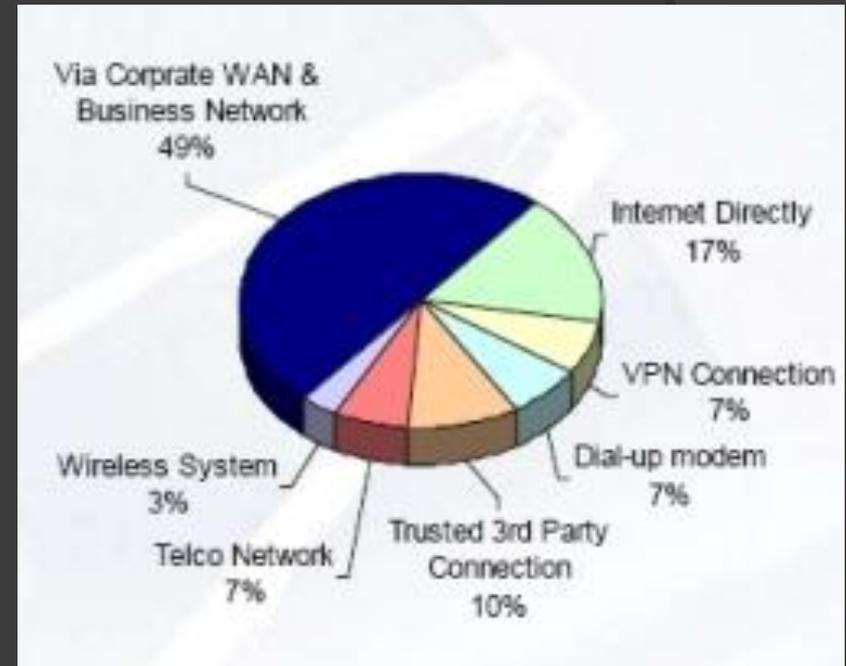
Insiders

- Disgruntled present or former employees are usually greatest risk
- Insider threat can be:
 - Physical sabotage
 - Cyber attacks
 - Provide inside information
 - Violent extremists with an inside position
- Maroochy good example
- Recent Key Largo insider hacking
- Reported that Al Qaeda has attempted to recruit insiders at water facilities
- Protective measures: screening new employees, limiting access to security areas, controlling access to control systems, employee training



Potential Attack Vectors?

- USB, other Removable Media
- Laptops, tablets
- Connections to the system's business network
 - Computers
 - Printers
 - Uninterruptible Power Supplies
- Modems (many still have) - War Dialing
- Other legacy systems; serial, etc.
- Wireless Network - War Driving
- Wireless Water Meters
- Remote Users
- External connections for contractors, support
- Sensors, PLCs, etc on outlying tanks, pump stations, dam gates, etc.
- VPN
- Mobile Phones
- Internet
- And there may be others.....



Internet Access

- Eireann P. Leverett - discovered 10,000 SCADA systems online via Shodan, June 2011 Masters Thesis (see table)
- Shodan provides access, but also so does Google, Yahoo, etc.
- Other researchers have easily accessed water system ICS via Shodan or Google
- Because - Many water SCADA systems are on the internet
- Easier and cheaper to connect using Ethernet and the internet rather than run new wires
- Many with simple or default passwords
- Just first step in an intrusion, obviously a big step; would still need some local knowledge, get passwords, learn how to affect SCADA through the HMI on the Windows box

Shodan Query	Connections	Category	Note
A850+Telemetry+Gateway	3	Telemetry	
ABB+Webmodule	3	Embedded Webserver	
Allen-Bradley	23	PAC	
/BroadWeb/	148	HMI	Known Vulnerabilities
Cimetrics+Eplus+Web+Server	6	Embedded Web Server	
CIMPLICITY	90	HMI	Zero Config Web View
CitectSCADA	3	PCS	
EIG+Embedded+Web+Server	104	Embedded Web Server	
eiPortal	1	Historian	
EnergyICT	585	RTU	Primarily Energy
HMS+AnyBus-S+WebServer	40	Embedded Web Server	
i.LON	1342	BMS	Primarily for energy
ioLogik	36	PLC	Small Vendor
Modbus+Bridge	12	Protocol Bridge	IP to Modbus
ModbusGW	11	Protocol Bridge	
Modicon+M340+CPU	3	Protocol Bridge	
Niagara+Web+Server	2794	HAN/BMS	Web server for EMS/BMS
NovaTech+HTTPD	1	Embedded Web Server	Substation Automation
Powerlink	257	BMS/HAN	
Reliance+4+Control+Server	10	SCADA	
RTS+Scada	15	SCADA	Runs on FreeBSD
RTU560	2	RTU	Web Interface
Simatic+HMI	9	HMI	Affected by Stuxnet
SIMATIC+NET	13	HMI	Affected by Stuxnet
Simatic+S7	13	PLC	Affected by Stuxnet
SoftPLC	80	PAC	Eastern Europe
TAC/Xenta	1880	BMS	Self Certs for HTTPS
WAGO	2	Telemetry	
webSCADA-Modbus	3	HAN	
Total	7489		

Table 2.1: Number of connections per query

Thumb Drives – Stuxnet!

- The “air gap” is not reliable protection
- Stuxnet got thru the “air gap” presumably via thumb drives used by Siemens engineers who supported the system
- Buckshot Yankee – in 2008 thumb drives got through DOD “air gap” to infect classified network
- Other removable media – CD, DVD, can also be used
- As long as the Windows boxes hosting the SCADA HMI have working USB and optical drive ports, they are not secure



Remote Access

- Marc Maiffret's pen test, unnames Calif. Water utility, got thru to SCADA via employees remote access
- The security of the SCADA is only as strong as the security on the employee with the weakest security on his home PC
- One successful phishing or spear-phishing attack is all one may need
- External access for contractors: the "Russian IP address" in the Illinois water hack that never happened
- VPN has known vulnerabilities
- Microsoft RDP vulnerability ups the ante; exploit already out there, lots of exposed systems
- Mobile phone apps also being used for remote access to SCADA; another security hole to exploit



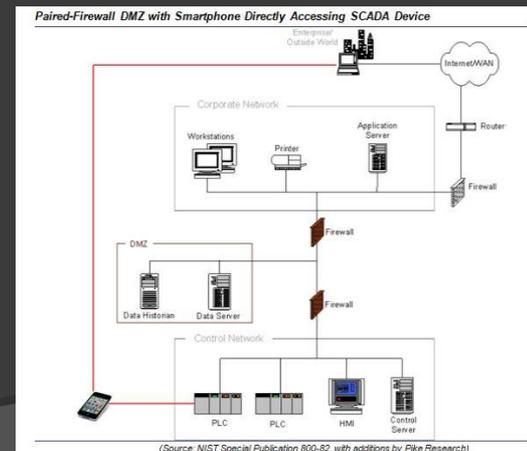
```
C:\WINDOWS\system32\cmd.exe
C:\>netstat -an > netstat-check.txt
C:\>netstat-check.txt
C:\> netstat-check.txt - Notepad
File Edit Format View Help

Active connections

Proto Local Address
TCP 0.0.0.0:135
TCP 0.0.0.0:445
TCP 0.0.0.0:902
TCP 0.0.0.0:912
TCP 0.0.0.0:1028
TCP 0.0.0.0:3389
TCP 0.0.0.0:11876
TCP 0.0.0.0:34800
TCP 0.0.0.0:44140
TCP 127.0.0.1:1031
TCP 127.0.0.1:1035
TCP 127.0.0.1:1117
```

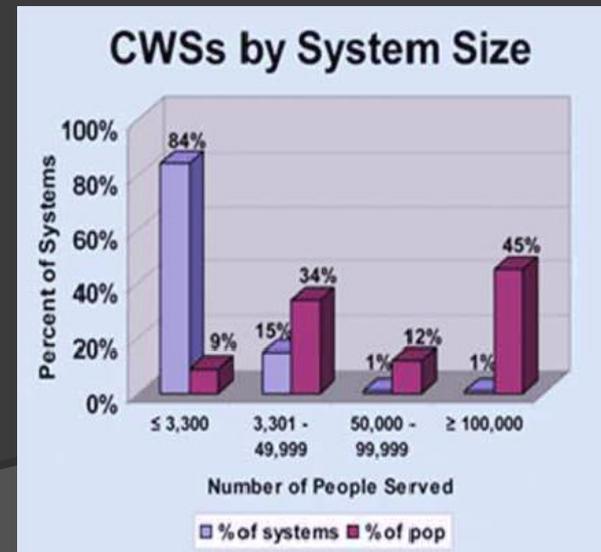
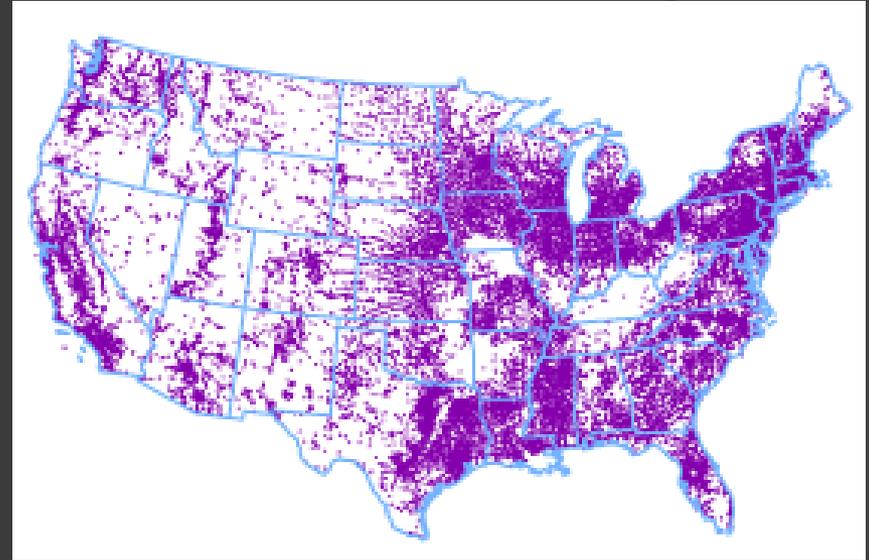
Mobile Phones & Tablets

- Mobile apps being used now to access and change settings in SCADA systems
- The new frontier
- What could go wrong?
- Very convenient
- Some have SSL type protection, like VPN
- Could be used to bypass all SCADA security
- Of course, mobile malware is increasing and innumerable security holes continually being discovered
- The SCADA security is thus only as strong as the mobile phone with remote access with the weakest security
- One phish or spear phish away from being pwned



National Water Infrastructure

- Critical Infrastructure; essential for public health, economy, business
- Fragmented difficult to attack all at once
- There are 155,693 public water systems, serving 286 million Americans.
- About 14% are privately owned
- The systems are varied, heterogeneous, run by variety of small-large local governments or private companies
- 8% of U.S. water systems (12,445) provide water to 82% of the U.S. population
- 0.2% of US water systems (404) are large systems that serve 46% of the population
- Can't take the whole infrastructure down at once, unlike the 3 national electric grids -- which can be taken down by attacks on 1-2 individual nodes
- Only common vector for water infrastructure appears to be treatment chemicals, especially chlorine (90%).



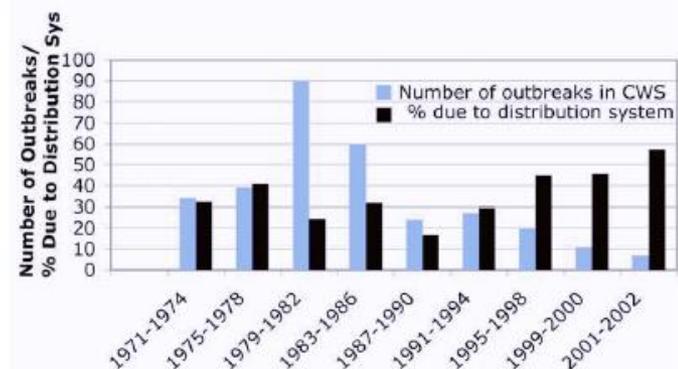
\$1 Trillion to Fix Infrastructure

- 24,000 water main breaks a year!
- Leak 7 billion gallons of water a year!
- Causes dozens of waterborne disease outbreaks a year!
- The national drinking water infrastructure is decaying
- Lots of 'noise' which makes it hard for a cyber attack to break through the clutter*
- \$1 Trillion needed to fix infrastructure ("Buried No Longer")
- One of the Strategic Bombing Survey's conclusions was that "The German experience showed that, whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary." Also cite WMD Resiliency Report
- Maybe the water infrastructure is in too bad shape for a cyber attack to even be noticed! (The Onion)

Al-Qaeda Claims U.S. Mass Transportation Infrastructure Must Drastically Improve Before Any Terrorist Attacks

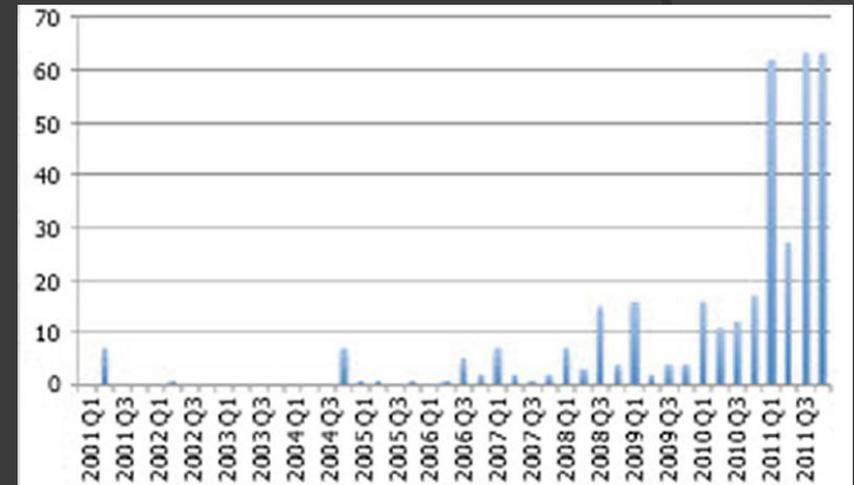


"We want to turn your bridges into rubble, but if we claimed credit for making them collapse, nobody would ever believe us."



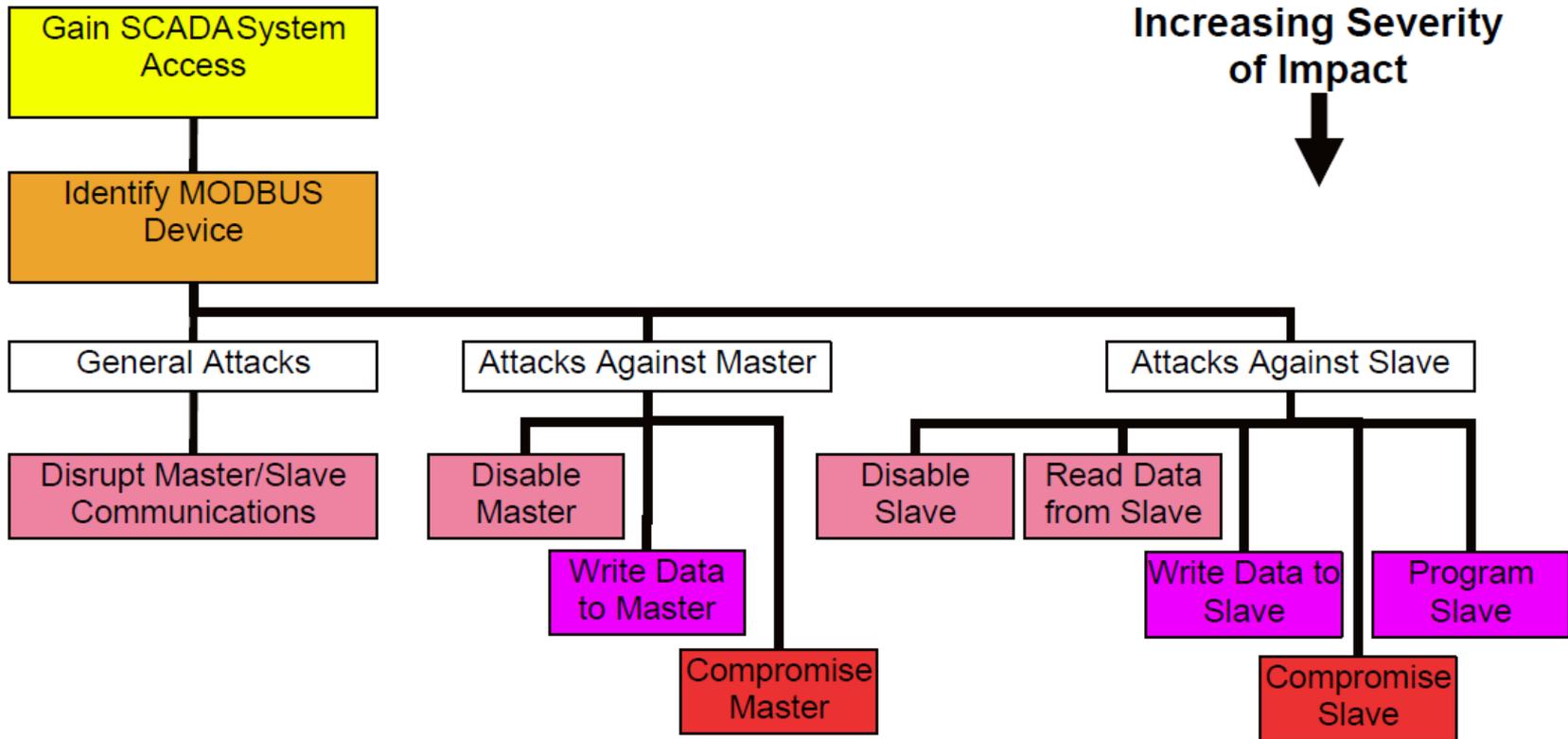
SCADA Vulnerabilities

- Originally isolated systems, not built with security in mind.
- ICS-specific vulnerabilities are increasingly being discovered
- Digital Bond – Project Basecamp documented many SCADA vulns, trying to end ‘decade of inaction’ over insecure SCADA systems
- McBride in S4 presentation said ICS specific disclosed vulnerabilities doubled in 2010 from 2009
- ICS specific disclosed vulnerabilities in 2011 were twice as much as all previously disclosed vulnerabilities
- ICS-CERT stated 60% of the ICS patches did not fix the problem
- Also Derbycon talk; Rios, McCorkle; 1,000+ vulns in 100 days
- Luigi Aureimello found numerous SCADA vulns
- Many are not being patched, called “Forever day” bugs or iDay bugs!



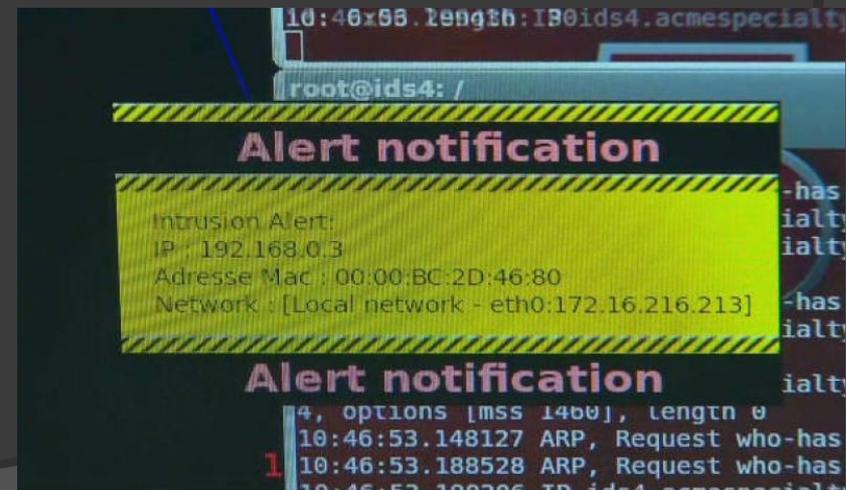
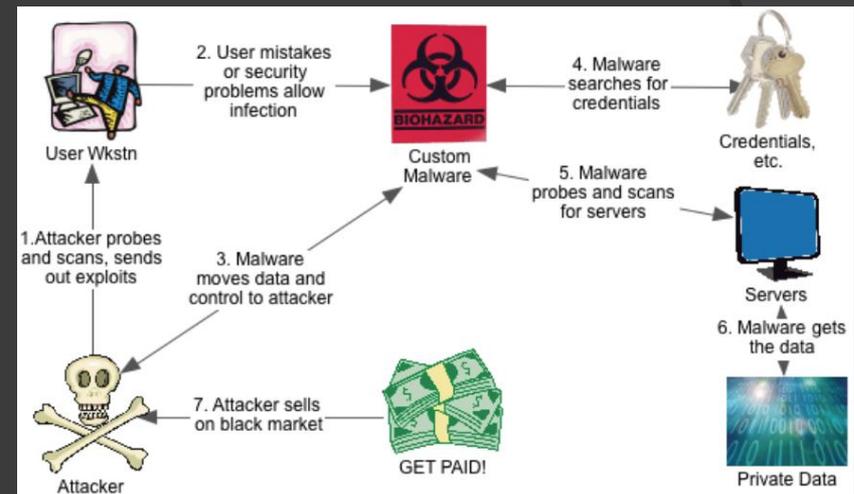
	AB BRALITY	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc Features	!	✗	✗	!	!

SCADA Attack Scenarios



Likely Attack Scenarios?

- Just getting access does NOT guarantee success
- Also need local knowledge, recon, to identify which assets have been compromised
- Need to identify what hardware there, the treatment process used, etc.
- Best case (for attacker) would be access to the HMI system with passwords and info on the plant; water flow, chemicals used, etc.
- Which is very possible...

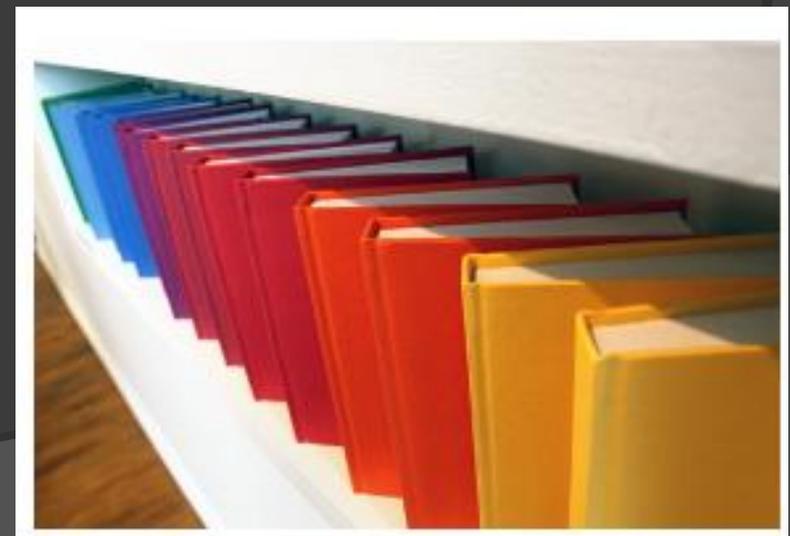


Water SCADA Security Weak

- Idaho National Lab 2005 report compares water ICS cyber security standards to baseline
- AWWA Security Guidance has cyber security standards for water sector
- Water standards WEAK!
- Out of 51 specific standards, AWWA fails 34, meets 15 partially, matches only 2 standards! – need to avoid power failures, and need for employee training

	Security Management				
	Management of Security Functions Behavior	Management of Security Attributes	Management of Security Function Data	Access Revocation	Time-limited Authorization
Chemical	○	○	○	●	○
Natural Gas	○	○	○	○	○
Petroleum & Oil	●	●	○	●	●
Transportation – Rail	○	○	○	○	○
Cross-Sector ISA TR99-01	○	○	○	○	○
Cross-Sector ISA TR99-02	○	○	○	○	○
Electrical Power	●	●	○	○	○
Telecommunications	●	○	○	○	○
Water	○	○	○	○	○

“o” = Gap; doesn’t meet NIST standards



AWWA ICS Security Standards

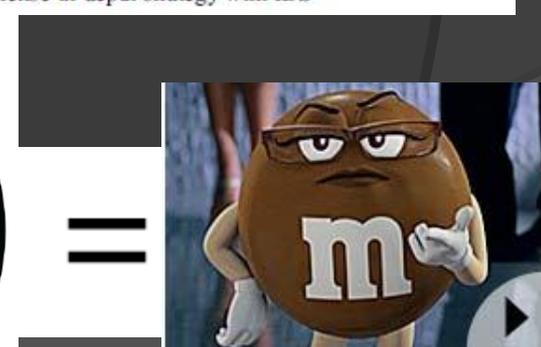
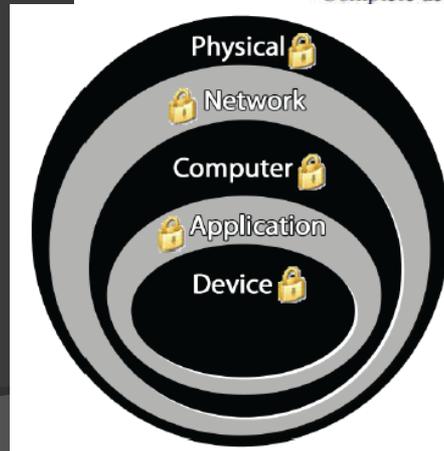
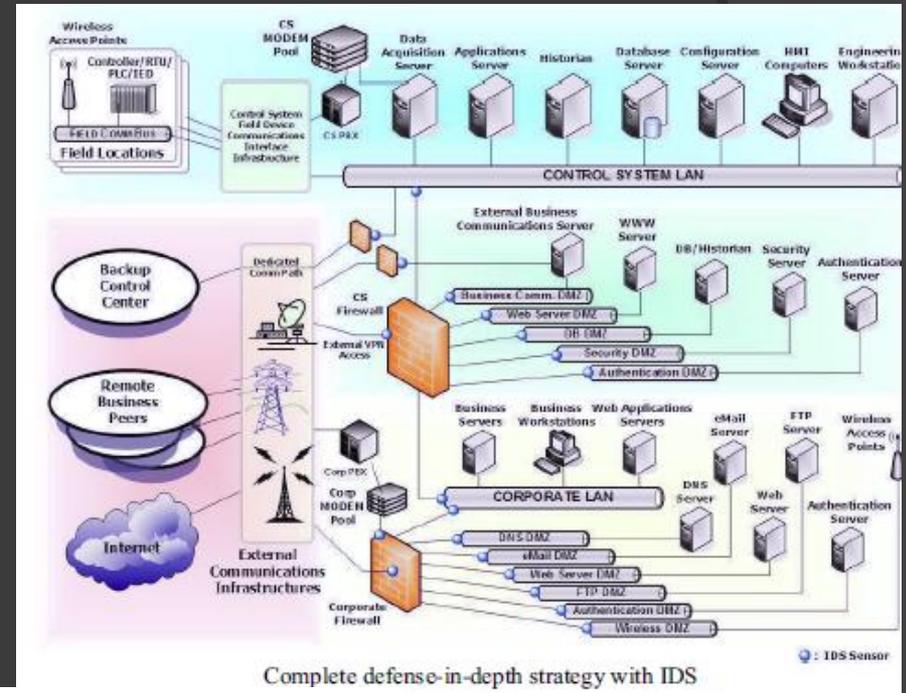
Recommended Standard

Does AWWA Meet?

- | | |
|---|-------------|
| ○ Security Alarms | ○ NO |
| ○ Cryptographic Key Management | ○ NO |
| ○ Data Authentication | ○ NO |
| ○ Authentication Failure Handling | ○ NO |
| ○ Time Limited Authorization | ○ NO |
| ○ Confidentiality During Transmiss | ○ NO |
| ○ Replay Detection | ○ NO |
| ○ Limited Priority of Service | ○ NO |
| ○ Session Establishment (Denial) | ○ NO |
| ○ Mutual Trusted
Acknowledgement | ○ NO |

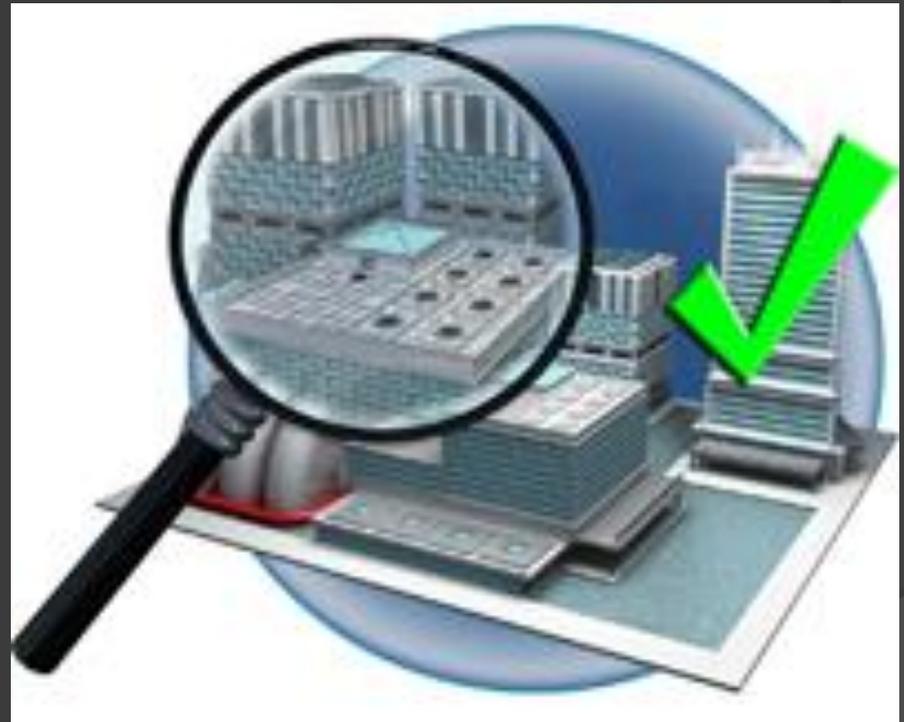
Technical Fixes Needed

- Technical fixes are well known
- Take SCADA off internet
- Fully update and patch HMI platforms
- Lock down remote access, modems, etc.
- Use only ISA (International Society of Automation) standards Secured SCADA systems
- There are many security standards and procedures, maybe too many.



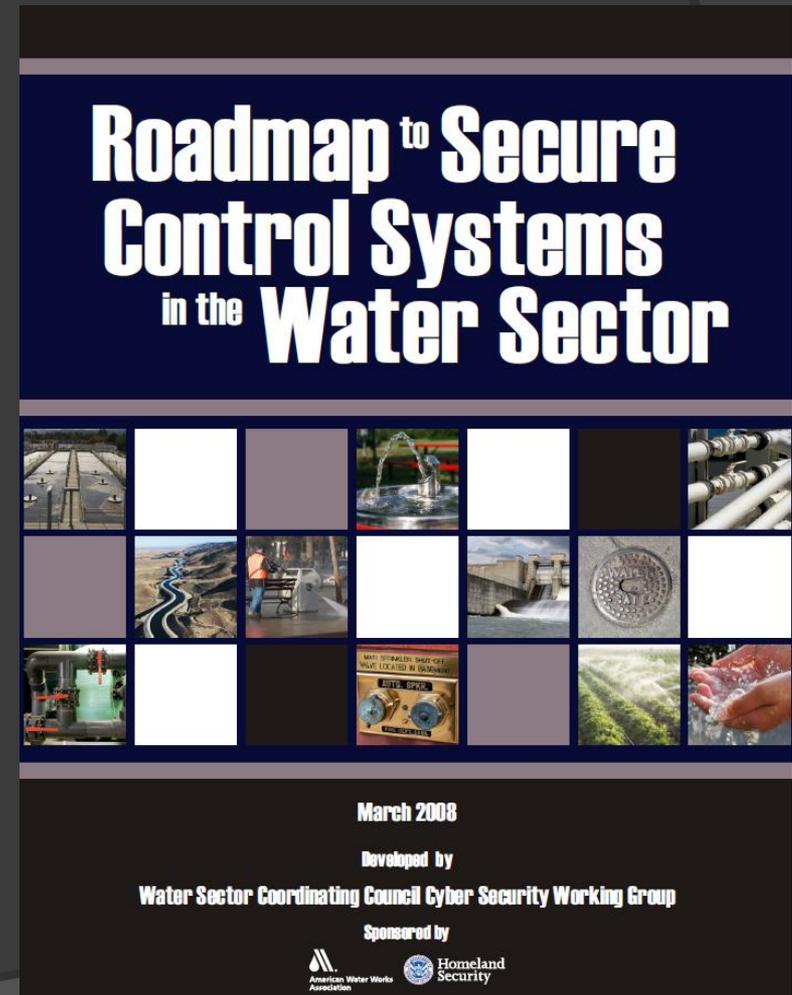
What Are Security Requirements for the Water Sector?

- Vulnerability Assessments 2003-2005
- No ICS questions
- No enforcement
- No repeatability; just one shot
- No money.
- Estimated \$1.6 billion to implement, the most basic measures



Roadmap to Control System Security in the Water Sector

- ONLY security req for water were the one-off vuln analysis 2002-2005 – voluntary, no ICS
- March 2008
- Major problem noted: “*business case has not been made*” for security
- Document had OK goals but no actual plan
- Needs a more thorough plan to actually accomplish goals.
- While energy sector ICS security is regulated by NERC, no one is regulating the water sector ICS security.



No progress, so far

Milestones

2008

Near-Term (2008-2009)

- 80% of water sector executives recognize that ICS security is critical to fulfilling their mission
- IT staff and ICS engineers and operators coordinate the development and implementation of ICS security efforts
- Integrate ICS security as a key goal in every project plan
- Develop a recommended practices ICS security template for widespread use in the water sector
- Integrate and elevate ICS security requirements with vendor contracts
- Isolate ICS from public-switched networks, including cable modems, direct-dial modems, open T1s, and internet access
- Integrate Roadmap to Secure Control Systems in the Water Sector with Water Sector Specific Plan

Mid-Term (2009-2011)

- Conduct sector-wide training on recommended practices ICS security template
- Integrate ICS security awareness, education, and outreach programs into water sector operations

Long-Term (2011-2018)

- Sustain roadmap activities in accordance with the Water Sector Specific Plan

End State (2018)

2018

- The water sector will have ICS security programs that reflect changes in technologies, operations, standards, regulations, and threat environments

- ⦿ Any progress on milestones? **NO**
- ⦿ Any plan for implementation? **NO**
- ⦿ Anyone in charge of implementing? **NO**

Conclusions

- ⦿ There are real threats to US drinking water infrastructure.
- ⦿ “Business case not been made” – biggest problem
- ⦿ “*Roadmap*” going nowhere
- ⦿ No requirements
- ⦿ No oversight
- ⦿ No funding
- ⦿ Water Systems need to:
 - Be REQUIRED to fix it
 - Be given \$\$\$ to do it
 - Be EVALUATED
 - Do it over regularly



John McNabb
john@infraseclabs.com
@Number0006
Infraseclabs.com