OFFICE OF INSPECTOR GENERAL

Catalyst for Improving the Environment

Briefing Report

EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Supervisory Control and Data Acquisition (SCADA) Vulnerabilities

Report No. 2005-P-00002

January 6, 2005

Report Contributors: Michael Loughnane
Ricardo Martinez
Erin Mastrangelo
Andrew McLaughlin

Abbreviations

EPA	Environmental Protection Agency
ORD	Office of Research and Development
OW	Office of Water
SCADA	Supervisory Control and Data Acquisition

U.S. Environmental Protection Agency
Office of Inspector General

2005-P-00002
January 6, 2005

At a Glance

Catalyst for Improving the Environment

Why We Did This Review

Federal Directives highlighted the need to secure cyberspace, including SCADA, from terrorists and other malicious actors, and stated that securing SCADA is a national priority. We learned from stakeholder contacts that utilities may require assistance in order to secure their SCADA system vulnerabilities.

Background

SCADA is a technology that allows a user to collect data from sensors and control equipment, such as pumps and valves, from a remote location. SCADA is commonly used in many industries, including water utility operations.

We suspended our SCADA project because EPA agreed to incorporate our concerns into an Agency SCADA project. At EPA's request, we briefed the Agency on our preliminary research and prepared this briefing report.

For further information, contact our Office of Congressional and Public Liaison at (202) 566-2391.

To view the full report, click on the following link:

www.epa.gov/oig/reports/2005/20050106-2005-P-00002.pdf

EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Supervisory Control and Data Acquisition (SCADA) Vulnerabilities

What We Found

SCADA networks were developed with little attention paid to security. As a result, many SCADA networks may be susceptible to attacks and misuses. Furthermore, studies indicated that some water utilities may have spent little time and money securing their SCADA systems.

Some areas and examples of possible SCADA vulnerabilities include operator errors and corruption, unsecured electronic communications, hardware and software limitations, physical security weaknesses, natural disasters, poorly written software, and poor security administration. Vulnerabilities may allow a person of malicious intent to cause significant harm. For example, in 2000, an engineer used radio telemetry to gain unauthorized access into an Australian waste management system and dump raw sewage into public areas. In another example, a contractor conducting a utility water assessment stated that he was able to access the utility's network from a remote location within minutes and could have caused significant harm.

Through preliminary research, we found several possible reasons why utilities have not successfully reduced or mitigated identified vulnerabilities. It is important to note that this list is not in any way expected to be exhaustive of what a full study may reveal. Specifically:

- Current technological limitations may impede implementing security measures.
- Companies may not be able to afford or justify the required investment.
- Utilities may not be able to conduct background checks on existing employees.
- Officials may not permit SCADA penetration testing.
- Technical engineers may have difficulty communicating security needs to management.

To better enable water systems to secure their SCADA systems, we suggest that EPA identify impediments preventing water systems from successfully reducing or mitigating SCADA vulnerabilities, and take steps to reduce those impediments. If EPA identifies a problem with no apparent solution, the Agency should communicate this problem to the Department of Homeland Security, Congress, and others as appropriate. We also suggest that EPA develop SCADA security measures to track the effectiveness of security efforts.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

OFFICE OF
INSPECTOR GENERAL

January 6, 2005

MEMORANDUM

SUBJECT: Final Briefing Report:
EPA Needs to Determine What Barriers Prevent Water
Systems from Securing Known Supervisory Control and Data
Acquisition (SCADA) Vulnerabilities

FROM: Jeffrey K. Harris /s/
Director for Program Evaluation, Cross-Media Issues

TO: Lek Kadeli
Acting Deputy Assistant Administrator for Management for Research and Development

Benjamin Grumbles
Assistant Administrator for Water

As part of our ongoing evaluation of the Environmental Protection Agency's (EPA's) activities to enhance the security of the Nation's water supply, we planned on conducting an evaluation of impediments to securing water Supervisory Control and Data Acquisition (SCADA) systems. Specifically, we planned to research what barriers, if any, impede water systems from securing SCADA weaknesses identified in their vulnerability assessments prepared under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188; June 12, 2002) or by other means. Understanding impediments may better enable EPA to appropriately consider and plan for water systems' SCADA security needs.

Many infrastructures and industries use computer-based systems to remotely control sensitive processes and physical functions previously controlled manually. These systems, commonly known as SCADA[1], allow a water utility to collect data from sensors and control equipment located at remote sites. Common water system sensors measure elements such as fluid level, temperature, pressure, water purity, water clarity, and pipeline flow rates. Common water system equipment includes valves, pumps, and mixers for mixing chemicals into the water supply.

[1] SCADA systems are also sometimes referred to as Digital Control Systems or Process Control Systems.

At EPA's request, we suspended our SCADA project because EPA has agreed to incorporate our questions into their planned work. On September 30, 2002, EPA awarded the Water Environment Research Foundation[2] a cooperative agreement to support their water security research efforts. The $2.1 million agreement partially funded various research projects, including $250,000 to partially fund research in Security Measures for Computerized and Automated Systems. On September 8, 2004, the Water Environment Research Foundation awarded EMA, Inc.[3], a $294,748 contract to conduct the SCADA research project titled "Security Measures for Computerized and Automated Systems." EPA participates on the project steering committee, and requested that we elaborate on our preliminary research[4] and share SCADA information and concerns that we observed. In response, on November 16, 2004, we convened a meeting with officials from the Office of Water and Office of Research and Development, and agreed to compile the attached briefing. The OIG presentation slides used for the meeting are included in Appendix A.

We planned the SCADA evaluation because, during our preliminary research, we learned that utilities may require assistance in order to secure their SCADA systems. We based our observations on information obtained from our interviews with water utility officials, contractors, other infrastructure SCADA security persons, the Department of Homeland Security, Sandia National Laboratories, and EPA representatives; attendance at stakeholder and national water conference meetings; and a review of vulnerability assessment tools, methodologies, and related documents. We conducted our work between May 24, 2004, and September 28, 2004, in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

Federal Directives Highlight Need to Secure SCADA

In recent years, various official sources have addressed the importance of securing cyberspace, including SCADA.

Presidential Directives: Presidential Decision Directive 62, issued in 1998, noted that the Nation's critical infrastructure relies heavily on the use of computers with cyber vulnerabilities that terrorists or criminals may use to commit attacks. Presidential Decision Directive 63, also issued in 1998, addressed the need to protect the Nation's critical infrastructures against criminal and terrorist attacks, and designated EPA the lead Federal agency for helping to secure water infrastructure. It also stated that advances in information technology and the necessity of improved efficiency have resulted in increasingly automated and interlinked infrastructures, and created new vulnerabilities to equipment failure, human error, weather and other natural causes,

[2] The Water Environment Research Foundation is a nonprofit corporation with its principal place of business located in Alexandria, VA.

[3] EMA, Inc., is a for profit organization with its principal place of business located in St. Paul, MN.

[4] The EPA Office of Inspector General conducted preliminary research evaluating water system security activities in support of the Agency's September 2002 Strategic Plan for Homeland Security. EPA's Homeland Security Strategy was subsequently updated on October 5, 2004.

and physical and cyber attacks. It challenged the Nation to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including specially our cyber systems." In December 2003, Homeland Security Presidential Directive 7 confirmed EPA's role as the lead agency for identifying, prioritizing, and coordinating the protection of critical infrastructure and key resources for drinking water and water treatment systems.

National Strategies: The White House's July 2002 National Strategy for Homeland Security noted that cyber attacks frequently occur on a local scale, and such attacks can occur on a more catastrophic national scale. The National Strategy further stated that our Nation's potential enemies have the intent, the tools of destruction are broadly available, our systems have well known vulnerabilities, and that a single act could inflict damage in multiple locations without the attacker ever physically entering the United States. The February 2003 National Strategy to Secure Cyberspace[5] included five priorities. The second priority, titled "A National Cyberspace Security Threat and Vulnerability Reduction Program," addressed SCADA security issues and stated that securing SCADA is a national priority.

The Bioterrorism Act: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188) requires utilities serving a population greater than 3,300 persons to conduct vulnerability assessments and to prepare emergency response plans. The Act required vulnerability assessments to include a review of automated systems. EPA awarded $51 million in grants to help large utilities prepare vulnerability assessments required under the Bioterrorism Act. EPA stores copies of these assessments in a secure area. Within six months of completing their assessments, water systems must certify to EPA that they completed their emergency response plans. However, the Act did not require utilities to submit copies of their plans to EPA.

SCADA Vulnerabilities Are Many

SCADA networks developed with little attention paid to security, making the security of these systems often weak. Studies have found that, while technological advancements introduced vulnerabilities, many water utilities have spent little time securing their SCADA networks. As a result, many SCADA networks may be susceptible to attacks and misuse.

Remote monitoring and supervisory control of processes begun to develop in the early 1960s, and adopted many technological advancements. The advent of minicomputers made it possible to automate a vast number of once manually-operated switches. Advancements in radio technology reduced the communication costs associated with installing and maintaining buried cable in remote areas. SCADA systems continued to adopt new communication methods including satellite and cellular. As the price of computers and communications dropped, it became economically feasible to distribute operations and to expand SCADA networks to include even smaller facilities.

Advances in information technology and the necessity of improved efficiency have resulted in increasingly automated and interlinked infrastructures, and created new vulnerabilities due to

[5] Cyberspace is composed of computer systems and their interconnections (source: The White House, "The National Strategy to Secure Cyberspace," 2003, executive summary, p. vii).

equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Some areas and examples of possible SCADA vulnerabilities include:

- **Human** - People can be tricked or corrupted, and may commit errors.
- **Communications** - Message can be fabricated, intercepted, changed, deleted, or blocked.
- **Hardware** - Security features are not easily adapted to small self-contained units with limited power supplies.
- **Physical** - Intruders can break into a facility to steal or damage SCADA equipment.
- **Natural** - Tornados, floods, earthquakes, and other natural disasters can damage equipment and connections.
- **Software** - Programs can be poorly written.

A study published May 1998 included a survey[6] that found that many water utilities were doing little to secure their SCADA network vulnerabilities. For example, many respondents reported that they had remote access, which can allow an unauthorized person to access the system without being physically present. More than 60 percent of the respondents believed that their systems were not safe from unauthorized access and use. Twenty percent of the respondents even reported known attempts, successful unauthorized access, or use of their system. Yet 22 of 43 respondents reported that they do not spend any time ensuring their network is safe and 18 of 43 respondents reported that they spend less than 10 percent ensuring network safety.

SCADA system computers and their connections are susceptible to different types of information system attacks and misuse such as system penetration and unauthorized access to information. The Computer Security Institute and Federal Bureau of Investigation conduct an annual Computer Crime and Security Survey[7]. The 2004 survey reported on 10 types of attacks or misuse, and reported that virus and denial of service had the greatest negative economic impact. The same study also found that 15 percent of the respondents reported abuse of wireless networks, which can be a SCADA component. On average, respondents from all sectors did not believe that their organization invested enough in security awareness. Utilities as a group reported a lower average computer security expenditure/investment per employee than many other sectors such as transportation, telecommunications, and financial.

Sandia National Laboratories' *Common Vulnerabilities in Critical Infrastructure Control Systems*[8] described some of the common problems it has identified in the following five categories:

[6] The survey was part of a thesis presented to the Faculty of the School of Engineering and Applied Science at the University of Virginia: Ezell, Captain Barry C., "Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply (May 1998)."

[7] Computer Crime Institute and Federal Bureau of Investigations, "Ninth Annual Computer Crime and Security Survey" (2004).

[8] Stamp, Jason et al., "Common Vulnerabilities in Critical Infrastructure Control Systems (2nd edition, 22 May 2003; revised 11 November 2003)," Sandia National Laboratories.

1. **System Data** -Important data attributes for security include availability, authenticity, integrity, and confidentiality. Data should be categorized according to its sensitivity, and ownership and responsibility must be assigned. However, SCADA data is often not classified at all, making it difficult to identify where security precautions are appropriate.
2. **Security Administration** -Vulnerabilities emerge because many systems lack a properly structured security policy, equipment and system implementation guides, configuration management, training, and enforcement and compliance auditing.
3. **Architecture** -Many common practices negatively affect SCADA security. For example, while it is convenient to use SCADA capabilities for other purposes such as fire and security systems, these practices create single points of failure. Also, the connection of SCADA networks to other automation systems and business networks introduces multiple entry points for potential adversaries.
4. **Network** (including communication links) - Legacy systems' hardware and software have very limited security capabilities, and the vulnerabilities of contemporary systems (based on modern information technology) are publicized. Wireless and shared links are susceptible to eavesdropping and data manipulation.
5. **Platforms** - Many platform vulnerabilities exist, including default configurations retained, poor password practices, shared accounts, inadequate protection for hardware, and nonexistent security monitoring controls. In most cases, important security patches are not installed, often due to concern about negatively impacting system operation; in some cases technicians are contractually forbidden from updating systems by their vendor agreements.

The following two incidents help to illustrate some of the risks associated with SCADA vulnerabilities.

- In 2000, an engineer used radio telemetry to gain unauthorized access into an Australian waste management system and dump raw sewage into public waterways and the grounds of a hotel. The perpetrator had worked for the contractor that supplied the remote control and telemetry equipment to the waste management system. This incident highlights many SCADA vulnerabilities. It illustrates the human factor of how people may be corrupted, and that the risk extends beyond current employees to outsiders who gain working knowledge system operations. Additionally, it illustrates that an outsider can exploit communications vulnerabilities to hack into a system.

- During the course of conducting a vulnerability assessment, a contractor stated that personnel from his company penetrated the information system of a utility within minutes. Contractor personnel drove to a remote substation and noticed a wireless network antenna. Without leaving their vehicle, they plugged in their wireless radios and connected to the network within 5 minutes. Within 20 minutes they had mapped the network, including SCADA equipment, and accessed the business network and data. This illustrates what a cyber security advisor from Sandia National Laboratories specializing in SCADA stated, that utilities are moving to wireless communication without understanding the added risks.

EPA Needs to Determine What Barriers Prevent Water Systems from Securing Known Vulnerabilities

EPA agreed to incorporate our SCADA research question into their planned work, and requested that we elaborate on the SCADA security issues we would like covered. Our research question was “What barriers, if any, prevent water systems from securing known SCADA vulnerabilities?” More specifically, our research goals were as follows.

The first goal was to identify specific SCADA vulnerabilities uncovered by water system vulnerability assessments and by other means. Vulnerability assessments stored at EPA may identify a wide array of vulnerabilities, as may other or subsequent assessments maintained by the utilities. Other possible sources of vulnerabilities information include water and SCADA experts from other infrastructures, National Laboratories, the Department of Homeland Security, academia, and contractors. Identified vulnerabilities can be listed, grouped, and analyzed to determine which are the most critical and most common vulnerabilities identified at water systems.

The second goal was to determine if vulnerability assessments are being successfully addressed. Completing vulnerability assessments and emergency response plans may not by themselves make water systems safer. Water systems must respond with proper security measures. Conversations with SCADA water system personnel and contractors may reveal whether water systems have implemented adequate security measures. For example, a contractor stated that utility operators may continue using default passwords due to a false sense of security. Utility representatives, system integrators, and manufacturers of hardware, software, and firmware may reveal whether utilities include security specifications in their procurement requirements. It is also important to determine what steps water systems take to validate the degree to which their remedies mitigated the vulnerability.

The third goal was to determine the reasons behind those instances where utilities cannot successfully reduce or mitigate identified vulnerabilities. Securing SCADA has inherent obstacles, and water systems may be unable or unwilling to take necessary security measures. The February 2003 National Strategy to Secure Cyberspace stated that securing SCADA is complicated because companies cannot afford or justify the required investment in systems and research and development; current technological limitations impede implementing security measures. This and other obstacles or barriers may impede water systems from successfully securing their water systems, leaving water systems at risk. For example, some utilities stated that they cannot conduct background checks on existing employees. Another utility representative stated that a city manager did not permit SCADA penetration testing. A Sandia National Laboratories representative and a contractor both stated that technical SCADA engineers have difficulty communicating security needs to management in a way that will get the projects funded. Another factor may be that water systems with significant investment in SCADA equipment and training may hesitate to undertake protection methods that require major replacement. What we found to date is based on preliminary research and is not in any way expected to be exhaustive of what a full study may reveal. EPA may find additional SCADA security constraints and may wish to pay particular attention to those that affect the most critical or common vulnerabilities.

The fourth goal was to determine what actions EPA can take to help remove impediments to water SCADA security. Possible EPA responses might include technical papers, manuals, a toolbox, new research, investment in new technologies, standards, and alerting other stakeholders. By identifying the most significant barriers impeding water systems from securing their SCADA systems, EPA will be better equipped to plan for and address key problems. EPA will be in a better position to address those problems that delay or preclude water SCADA security. This may allow EPA and others to focus limited resources into the areas that will have the greatest water SCADA security impact. Where EPA identifies a problem with no viable, likely, or apparent solution, the Agency should communicate this problem to the Department of Homeland Security, Congress, water industry groups, or others as appropriate.

We Encourage EPA to Develop SCADA Security Measures

We encourage EPA to look for ways to measure the extent to which water system efforts and EPA contributions increase SCADA security. This would entail developing program measures and ways to systematically collect information. EPA may be able to learn from the practices of others. For example, the Computer Security Institute joined forces with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad and developed an annual computer crime and security survey. The survey asks participants to respond anonymously to a series of security-related questions, and establishes trends based on the responses. Possible sources of information include water systems, SCADA system integrators, security component manufacturers, intrusion assessment contractors, etc. Proper measures will allow EPA to better ensure that resources are allocated appropriately and efficiently, and that the program is accomplishing its goals. It will also help EPA to comply with the Government Performance and Results Act of 1993 and the President's Management Agenda, which require EPA to measure the effectiveness of its programs.

Suggestions

To better enable water systems to secure their SCADA systems, we suggest that

1. EPA identify impediments preventing water systems from successfully reducing or mitigating SCADA vulnerabilities, and take steps to reduce those impediments.

2. EPA develop SCADA security measures to track the effectiveness of security efforts.

Agency Response

The EPA Office of Research and Development chose not to provide a formal written response. Similarly the EPA Office of Water chose not to provide written comments, but noted that their current activities are addressing the OIG suggestions. We are closing this report upon issuance since it does not contain recommendations.

OIG/ORD/OW SCADA Meeting

Ricardo Martinez, Office of Program Evaluation

Michael Loughnane, Computer Crimes Directorate

November 16, 2004

Agenda

1. What is SCADA
2. SCADA Vulnerabilities
3. Federal Directives
4. Current Status

Agenda

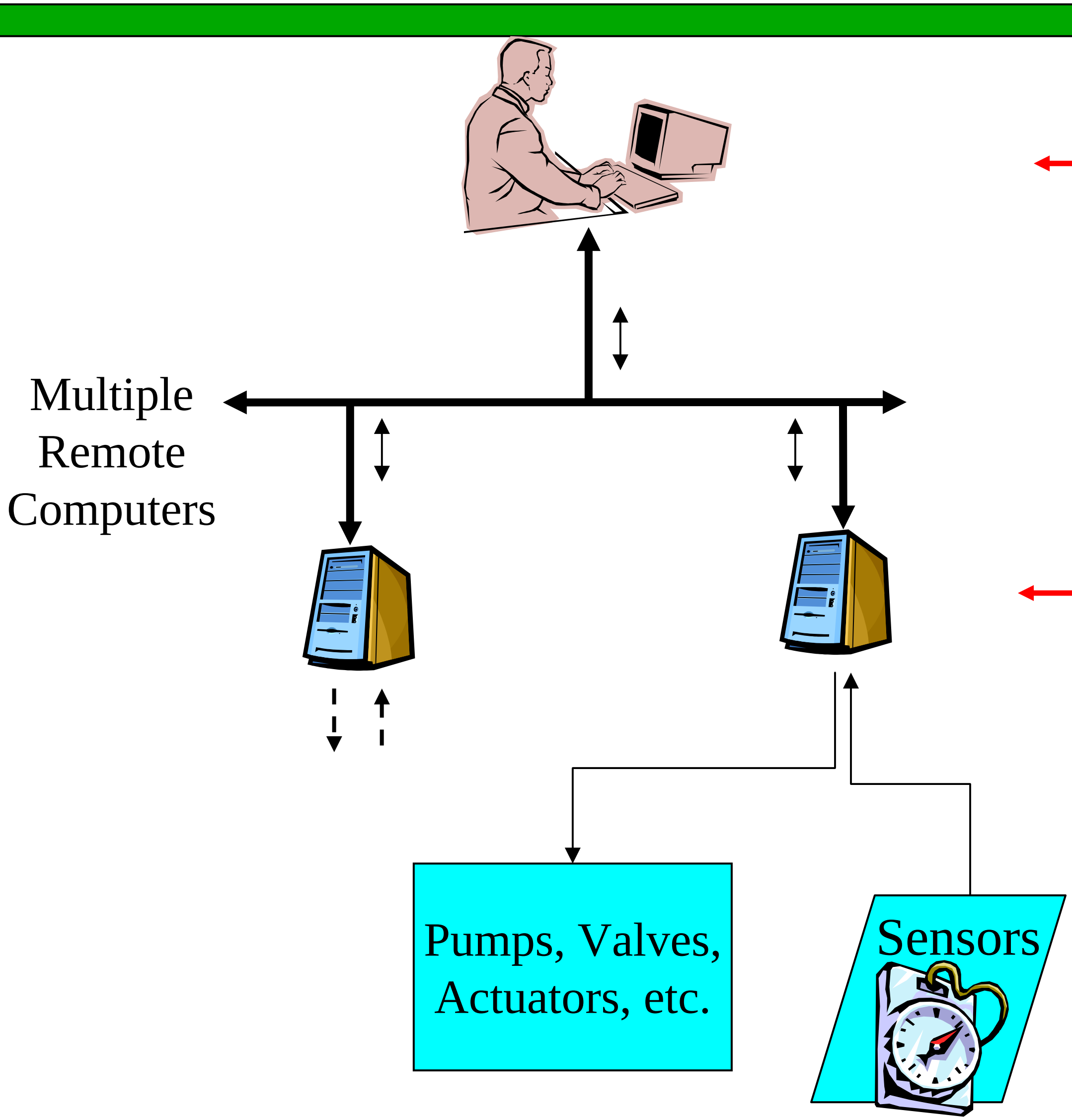
1. **What is SCADA**
2. SCADA Vulnerabilities
3. Federal Directives
4. Current Status

What is SCADA?

Computer-based system that remotely controls processes previously controlled manually.

Allows a water utility to

- Collect data from sensors
- Control equipment at remote sites



Multiple Remote Computers

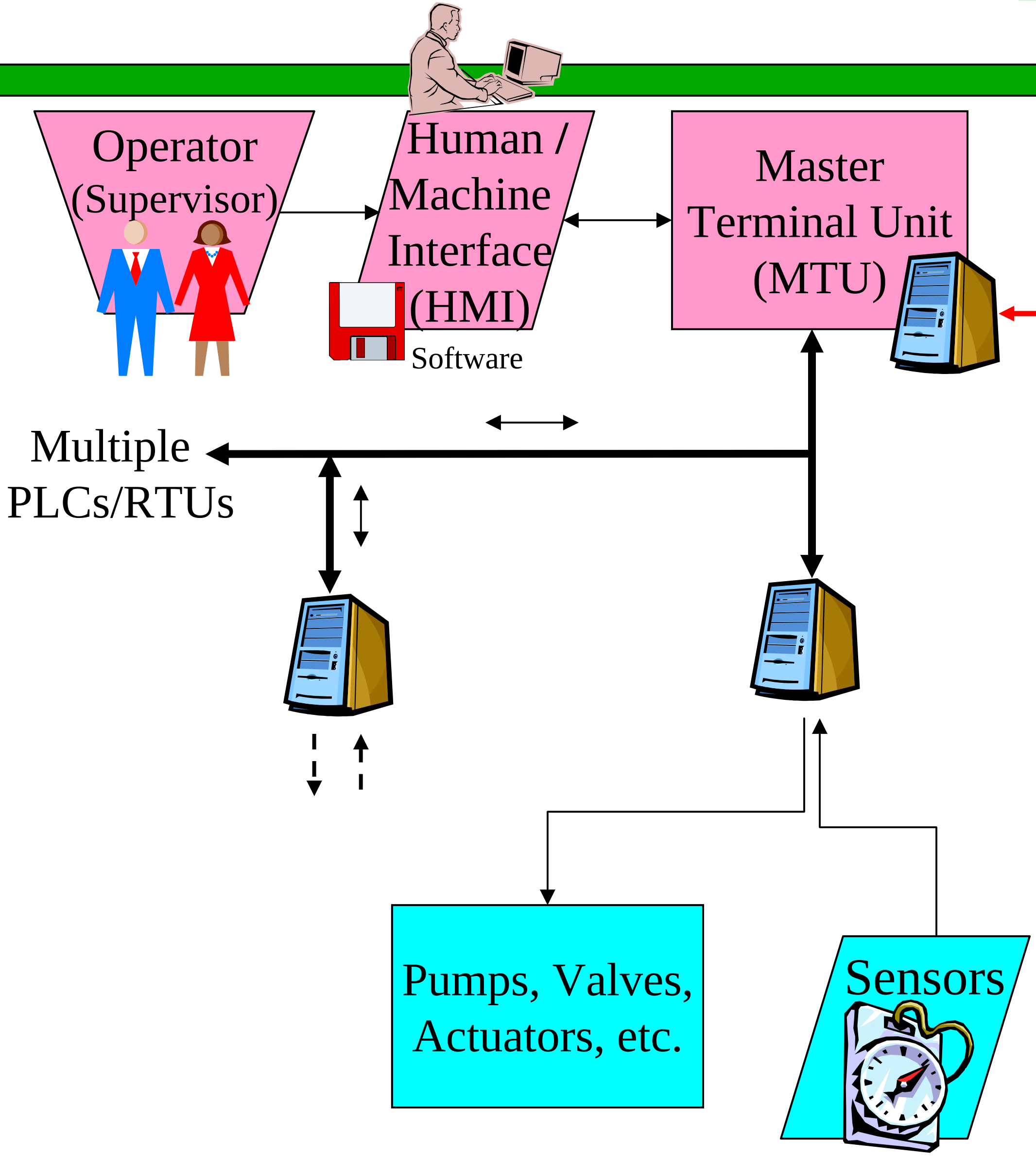
Pumps, Valves, Actuators, etc.

Sensors

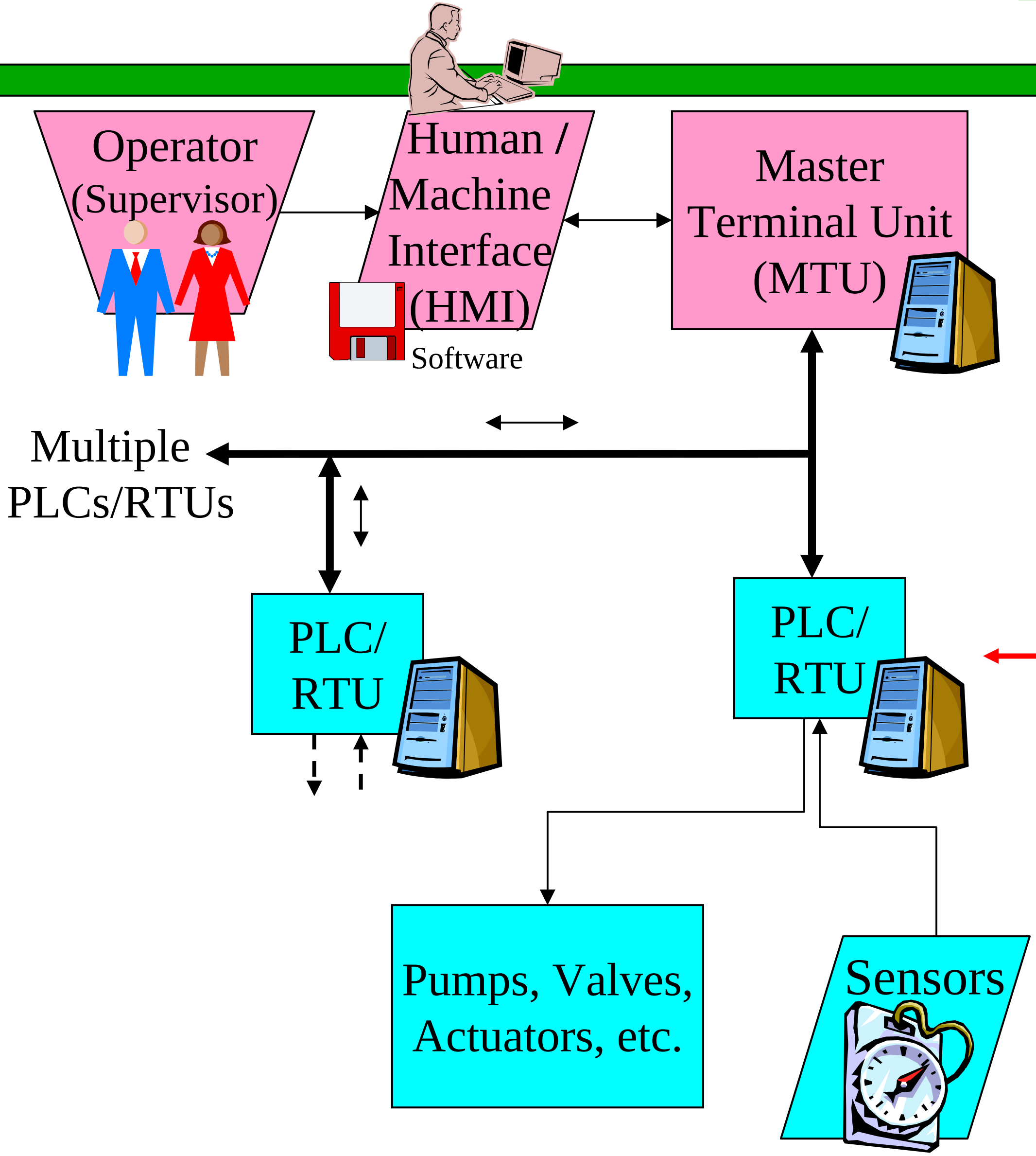
SCADA allows an Operator using a central computer to supervise (control and monitor) multiple networked computers at remote locations.

Each remote computer can control mechanical processes (pumps, valves, etc.) and collect data from sensors at its remote location.

Thus the Phrase: Supervisory Control and Data Acquisition, or **SCADA**.



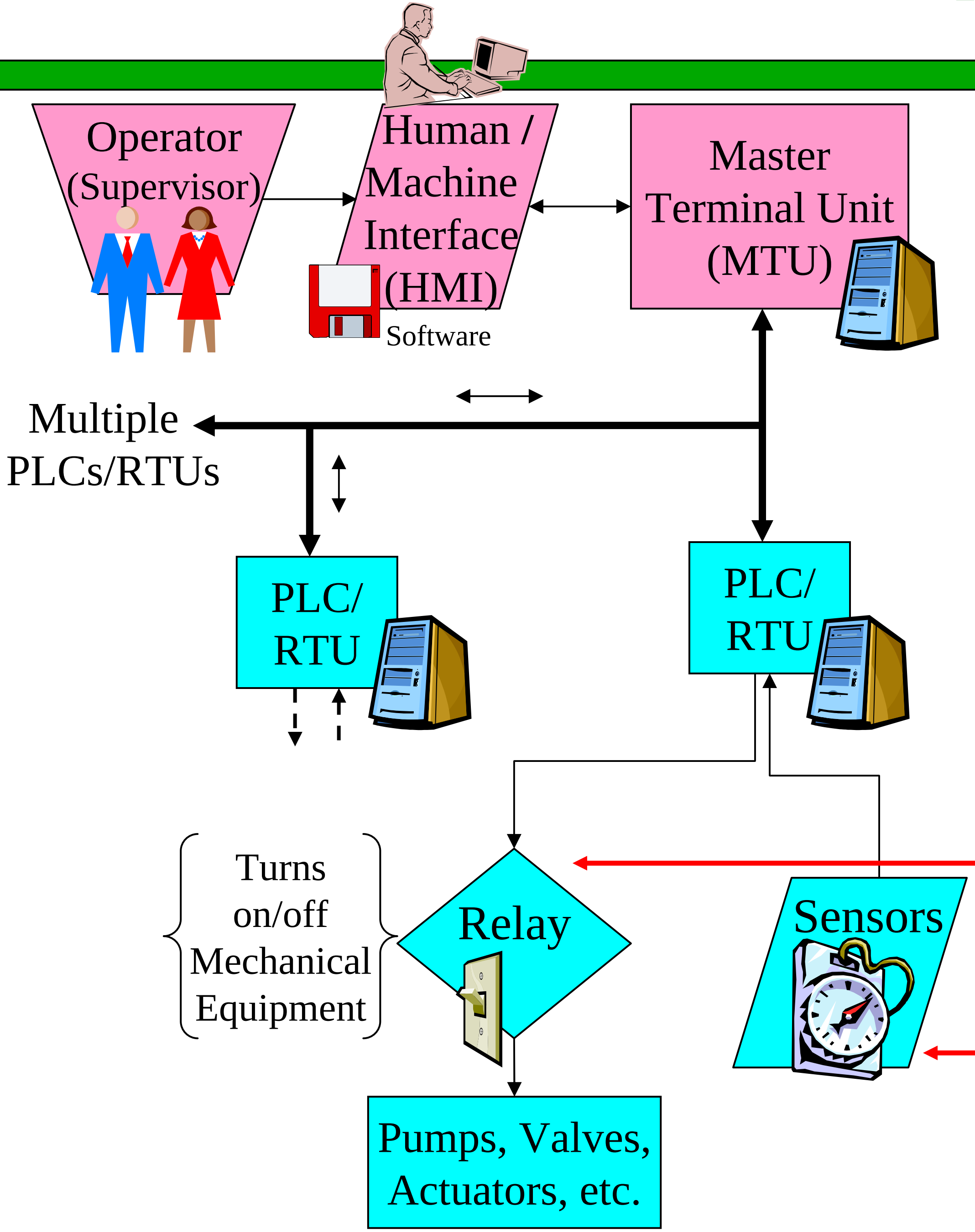
The central computer is called the Master Terminal Unit, or MTU. The Operator interfaces with the MTU using a software called Human Machine Interface, or HMI.



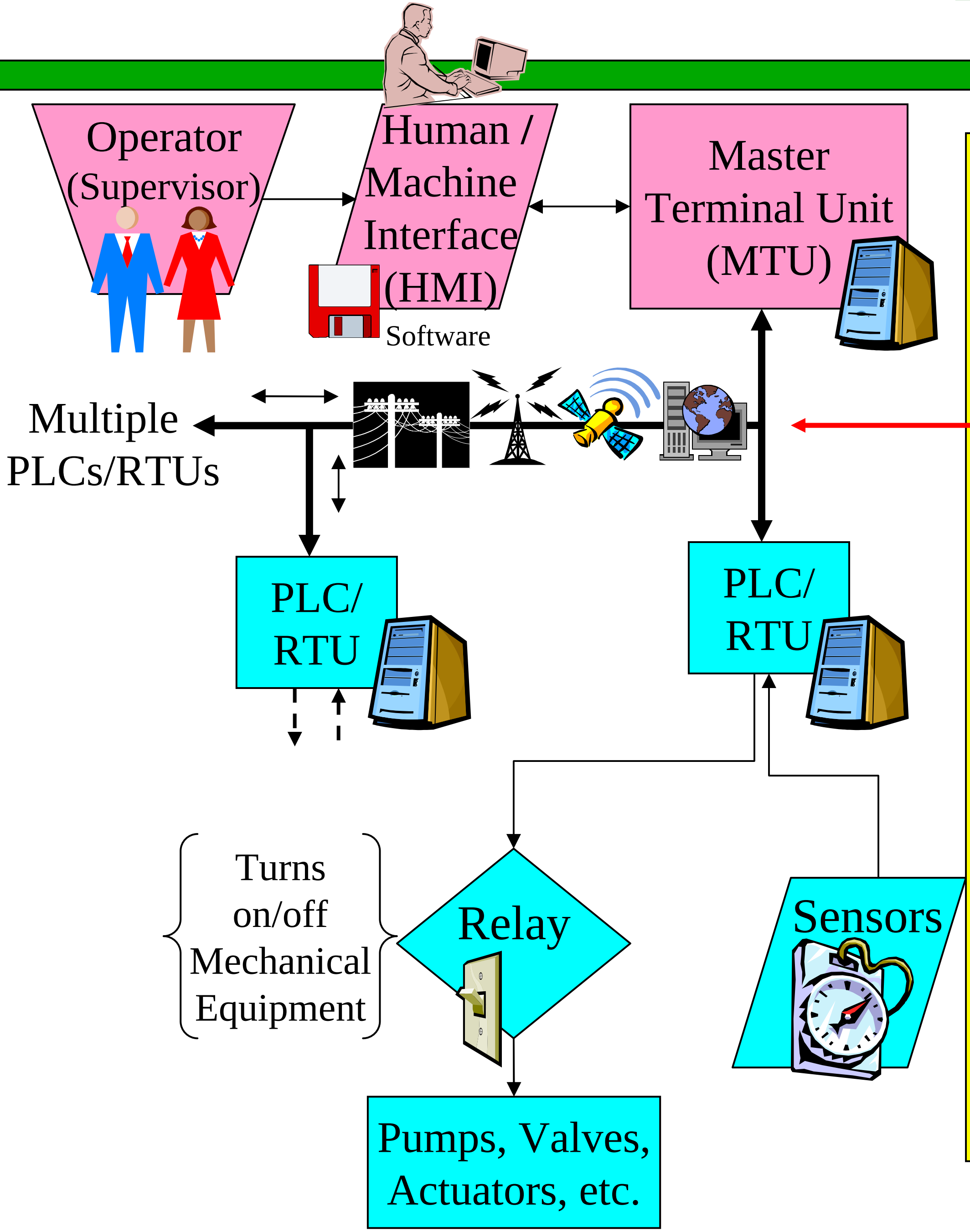
The remote computer is called Program Logic Controller (PLC) or Remote Terminal Unit (RTU)*

*There are differences between a PLC and RTU.

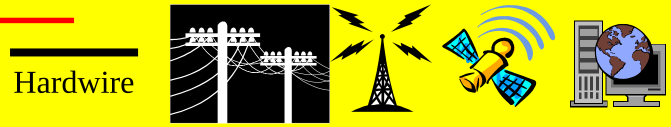
SCADA



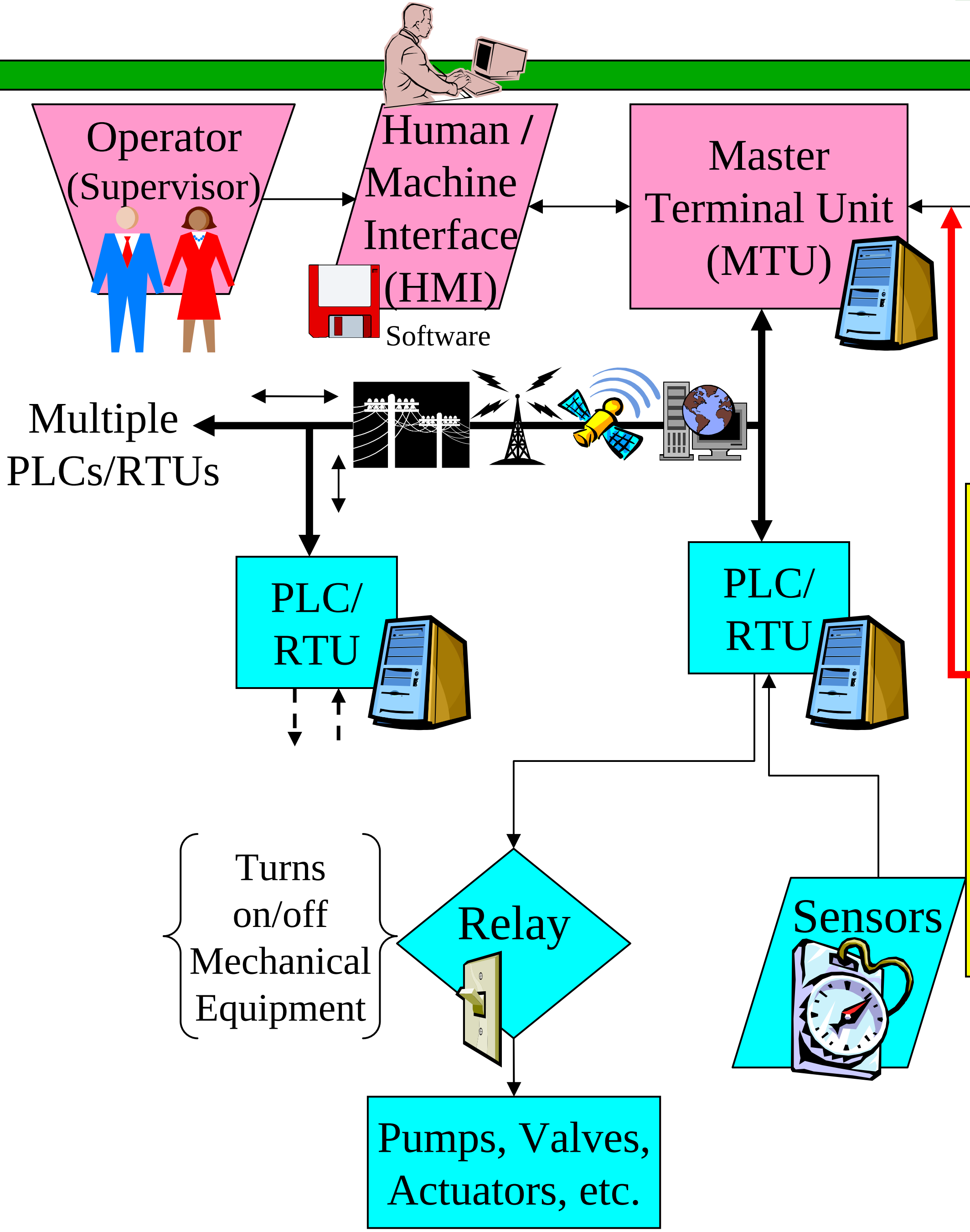
The RTU activates a relay (or switch) that turns mechanical equipment "on" and "off." The RTU also collects data from sensors.


Operator (Supervisor)
Human / Machine Interface (HMI)
Software
Master Terminal Unit (MTU)
Multiple PLCs/RTUs
PLC/ RTU
PLC/ RTU
Turns on/off Mechanical Equipment
Relay
Sensors
Pumps, Valves, Actuators, etc.

In the early stages utilities ran wires, also known as hardwire or land lines, from the central computer (MTU) to the remote computers (RTUs).

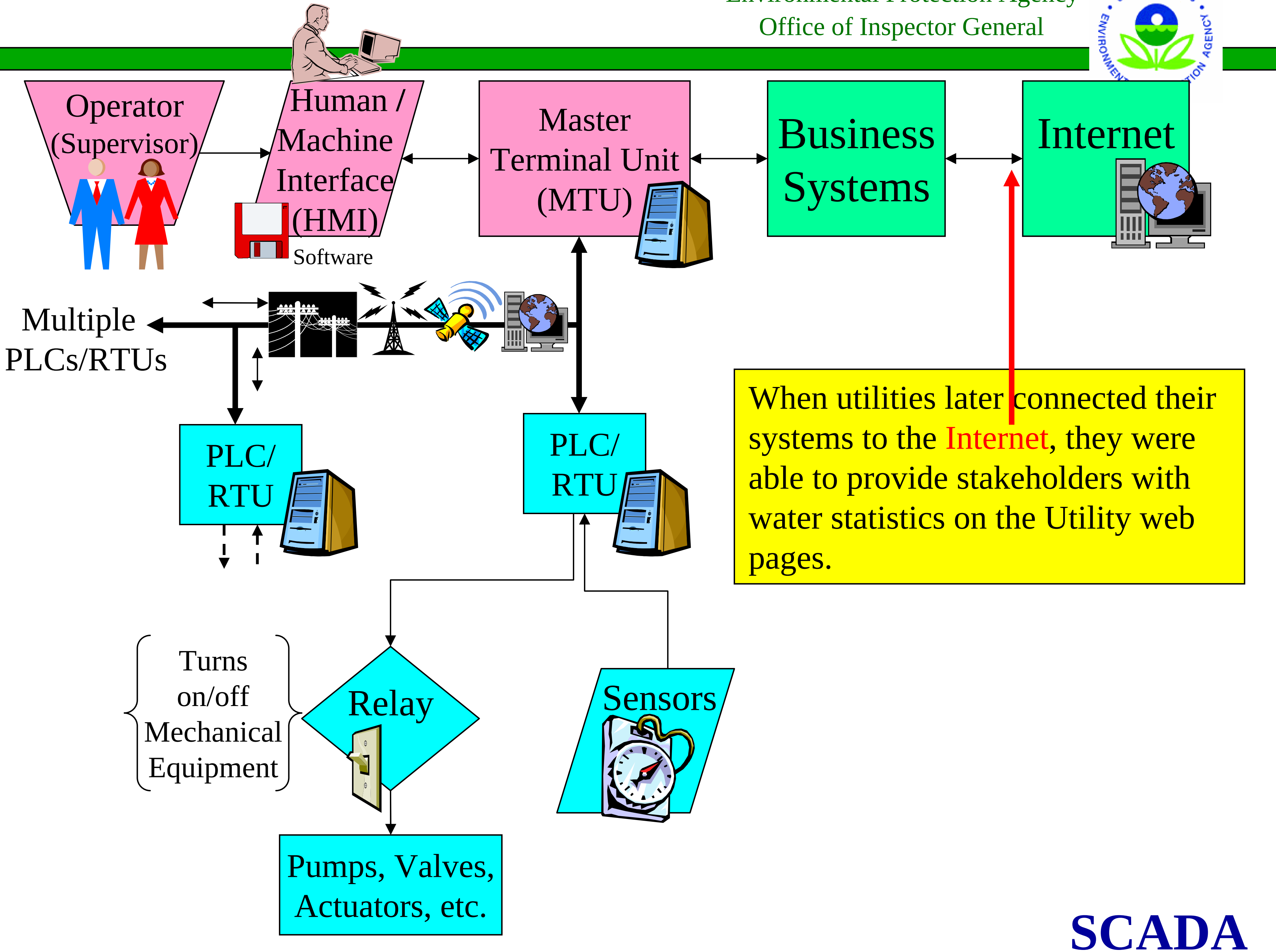


Since remote locations can be located hundreds of miles from the central location, utilities begun to use public phone lines and modems, leased telephone company lines, and radio & microwave communication. More recently, they have also begun to use satellite links, Internet, & newly developed wireless technologies.



Since the SCADA systems' Sensors provided valuable information, many utilities established "connections" between their SCADA systems and their business system. This allowed Utility management and other staff access to valuable statistics, such as water usage.

SCADA



Operator (Supervisor)

Human / Machine Interface (HMI)

Software

Master Terminal Unit (MTU)

Business Systems

Internet

Multiple PLCs/RTUs

PLC/ RTU

PLC/ RTU

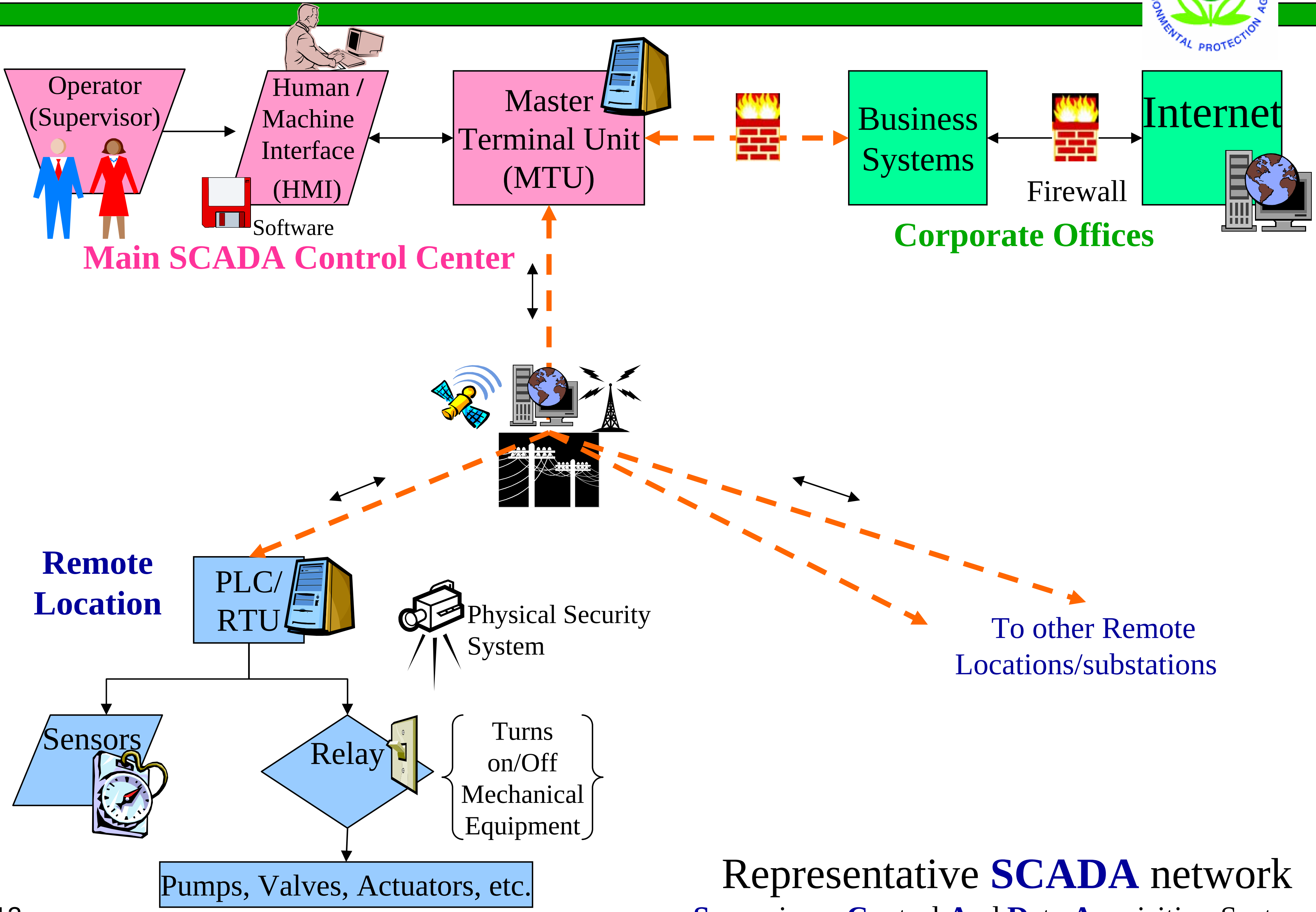
Turns on/off Mechanical Equipment

Relay

Sensors

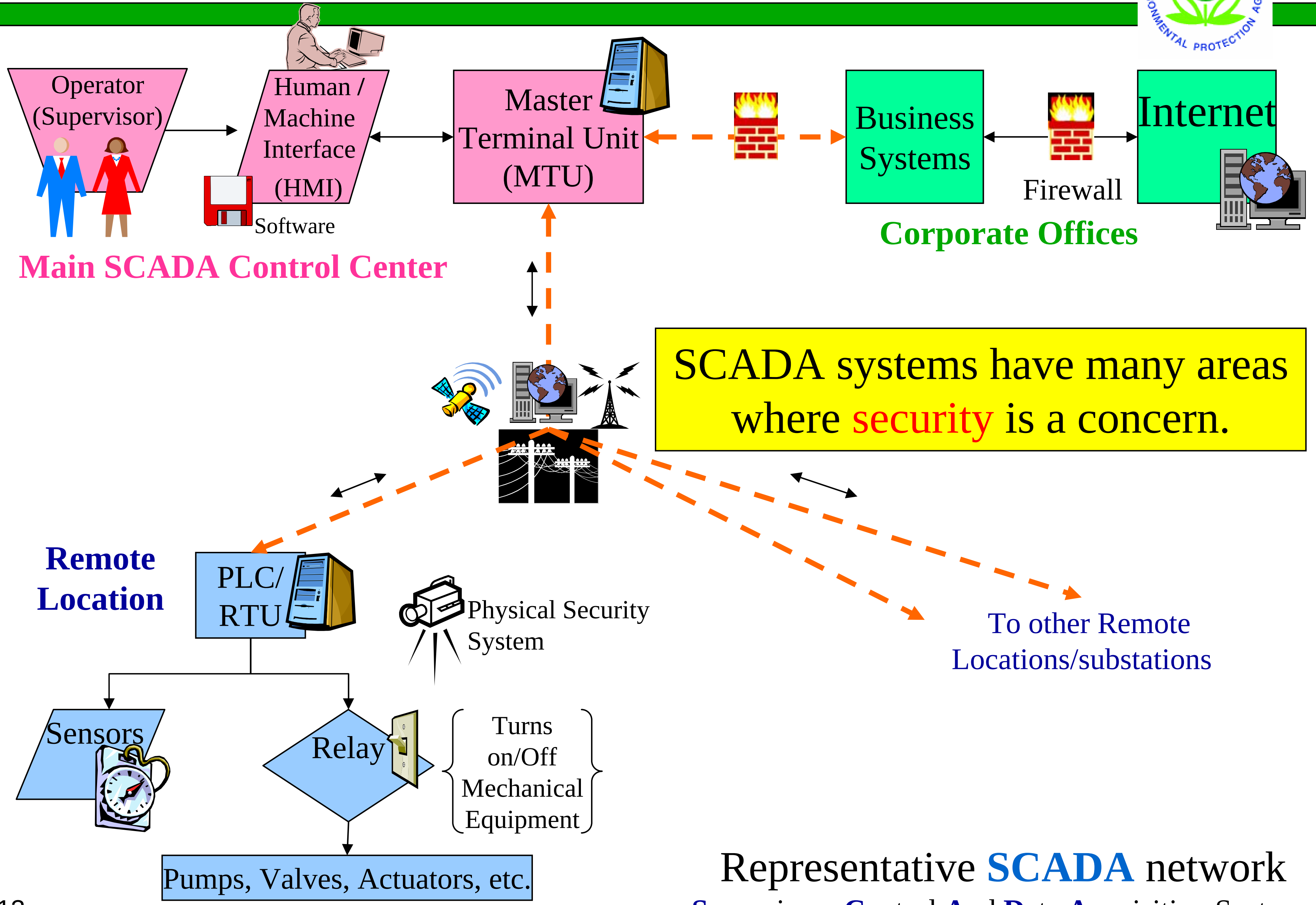
Pumps, Valves, Actuators, etc.

When utilities later connected their systems to the Internet, they were able to provide stakeholders with water statistics on the Utility web pages.


Operator (Supervisor)
Human / Machine Interface (HMI)
Software
Master Terminal Unit (MTU)
Business Systems
Firewall
Internet
Corporate Offices
Main SCADA Control Center
Remote Location
PLC/ RTU
Physical Security System
To other Remote Locations/substations
Sensors
Relay
Turns on/Off Mechanical Equipment
Pumps, Valves, Actuators, etc.

Representative **SCADA** network

Supervisory **C**ontrol **A**nd **D**ata **A**cquisition System



SCADA systems have many areas where security is a concern.

Representative **SCADA** network

Supervisory **C**ontrol **A**nd **D**ata **A**cquisition System

Agenda

1. What is SCADA
2. **SCADA Vulnerabilities**
3. Federal Directives
4. Current Status

Vulnerabilities

- Physical

  Example-Intruders can break into your facilities to steal or damage SCADA equipment.

- Natural

  Example-Tornados, floods, earthquakes, and other natural disasters can damage equipment or connections.

- Hardware

  Example-Security features are not easily adapted to small self-contained units with limited power supplies.

- Software

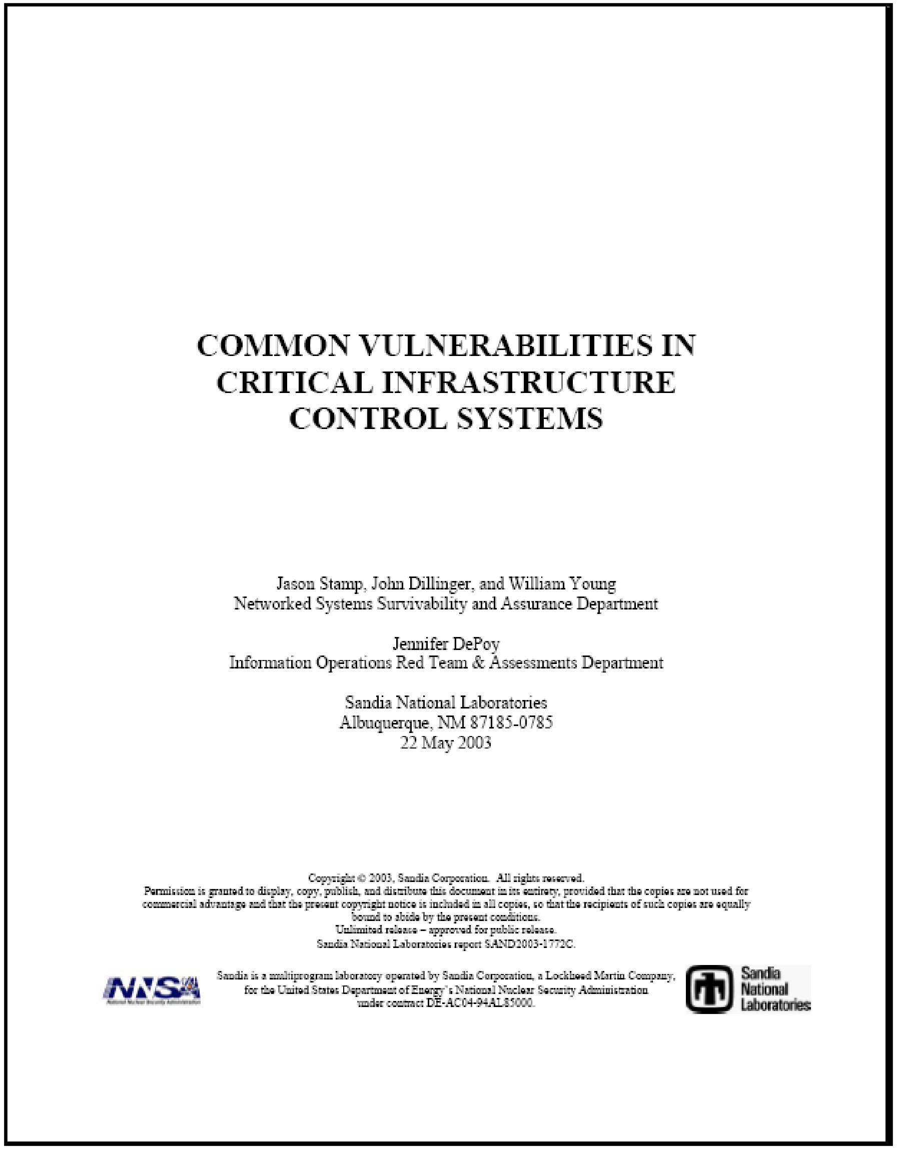
  Example-Programs can be poorly written.

- Communications

  Example-Message can be fabricated, intercepted, changed, or deleted/blocked.

- Human

  Example-People can be tricked or corrupted, and may commit errors.



COMMON VULNERABILITIES IN
CRITICAL INFRASTRUCTURE
CONTROL SYSTEMS

Jason Stamp, John Dillinger, and William Young
Networked Systems Survivability and Assurance Department

Jennifer DePoy
Information Operations Red Team & Assessments Department

Sandia National Laboratories
Albuquerque, NM 87185-0785
22 May 2003

Copyright © 2003, Sandia Corporation. All rights reserved.
Permission is granted to display, copy, publish, and distribute this document in its entirety, provided that the copies are not used for commercial advantage and that the present copyright notice is included in all copies, so that the recipients of such copies are equally bound to abide by the present conditions.
Unlimited release – approved for public release.
Sandia National Laboratories report SAND2003-1772C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Described common problems identified in 5 categories:

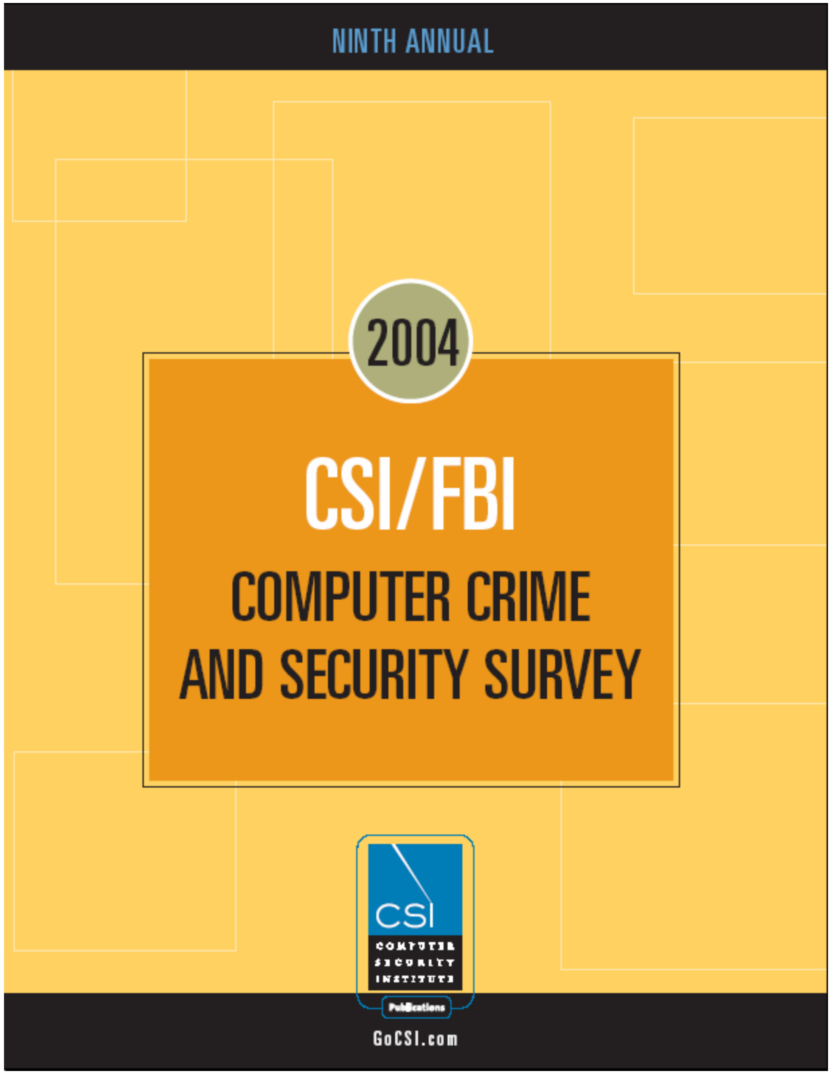
1. Data
2. Security Administration
3. Architecture
4. Network
5. Platforms

Pre-9/11 Baseline Condition

per a study published 1998, approximately:

- 60% reported their SCADA system could be remotely accessed and controlled.
- 60% reported their systems not safe from unauthorized access or use.
- 20% reported known attempts.
- 50% reported not spending any time ensuring their network is safe.
- 40% reported they spend less than 10% of their time ensuring network safety.

Current Survey



NINTH ANNUAL

2004

CSI/FBI

COMPUTER CRIME AND SECURITY SURVEY

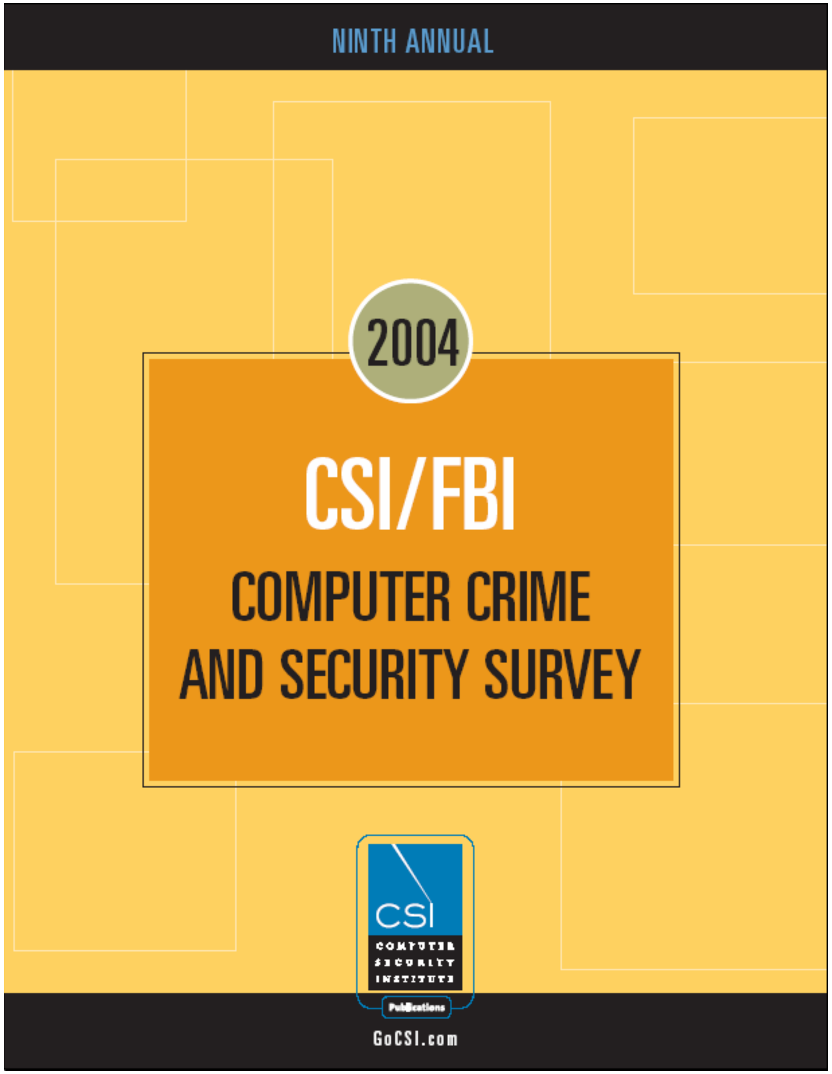
CSI
COMPUTER SECURITY INSTITUTE
Publications

GoCSI.com

On average, respondents from all sectors did not believe that their organization invested enough in security awareness.

Utilities as a group reported a lower average computer security expenditure/investment per employee than many other sectors such as transportation, telecommunications, and financial.

Current Survey



The survey also found:

- Of 10 types of attacks or misuse, virus and denial of service had the greatest negative economic impact

- 15% reported abuse of wireless networks

Two SCADA Risk Illustrations

- Australian waste management system

  Engineer used unauthorized access to dump raw sewage.

- Utility vulnerability assessment

  Contractor penetrated a utility information system from a remote substation within minutes.

Agenda

1. What is SCADA
2. SCADA Vulnerabilities
3. **Federal Directives**
4. Current Status

Federal Directives

- **PDD 62,** issued May 1998
- **PDD 63,** issued May 1998
- **The National Strategy for Homeland Security**, July 2002
- **The National Strategy to Secure Cyberspace**, Feb 2003

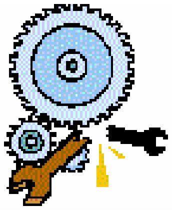
PDD 62, issued May 1998, noted that,

the Nation's critical infrastructure
relies heavily on the use of computers
with cyber vulnerabilities
that terrorists may exploit
to commit attacks.

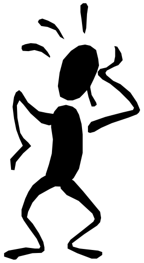
PDD 63, issued May 1998, noted that,

Information technology advances have:

- Improved efficiency
- Increasingly automated and interlinked infrastructures
- Created new vulnerabilities

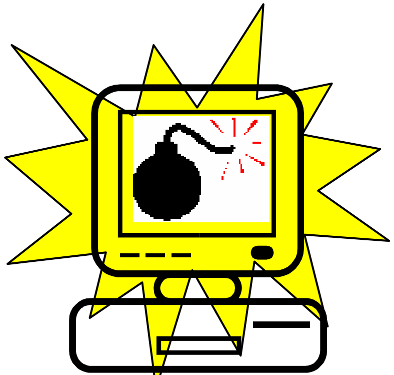


Equipment Failure



Human Error

Natural causes



Physical or
Cyber attacks

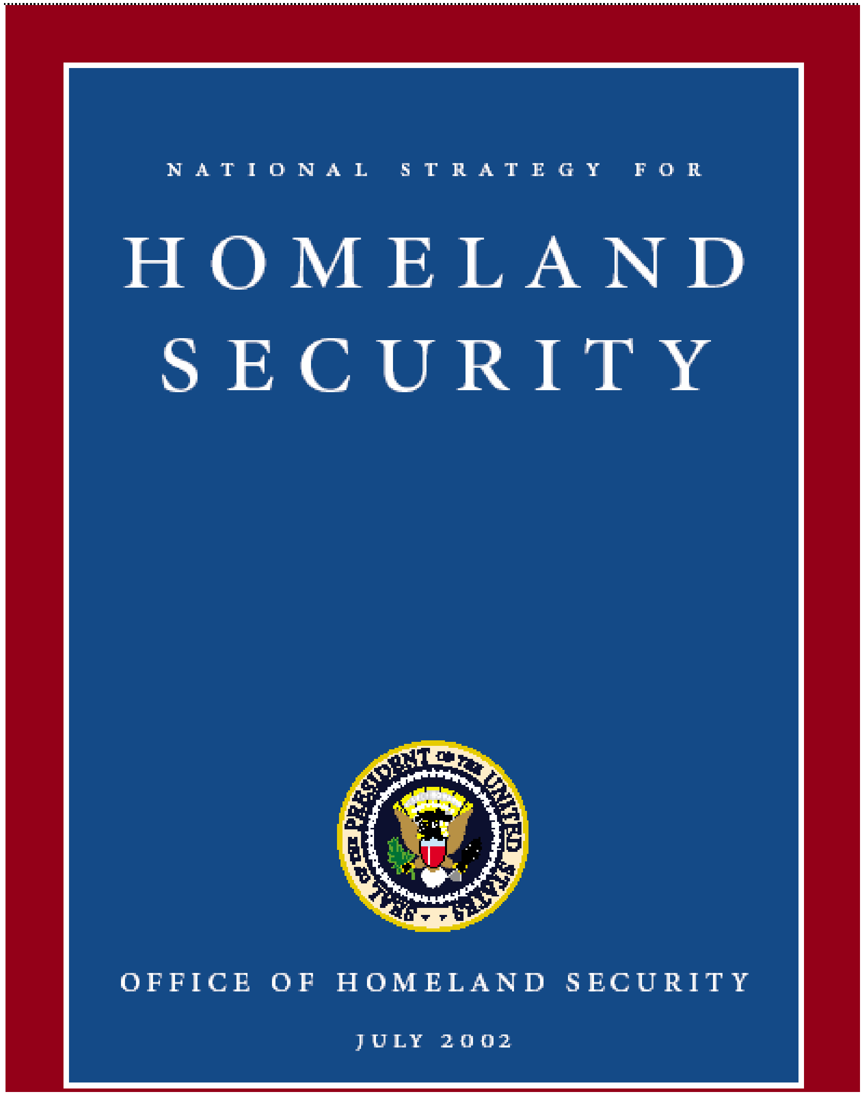
PDD 63, issued May 1998,

Named EPA as the water infrastructure lead tasked with forming a private-public partnership to:

- swiftly eliminate significant vulnerabilities, “including **specially our cyber systems**.” (See Section II)

- encourage utilities to provide maximum feasible infrastructure security & information so the government can assist them.

The National Strategy for Homeland Security stated, (p.34)



- **Cyber attacks** are happening frequently on a local scale

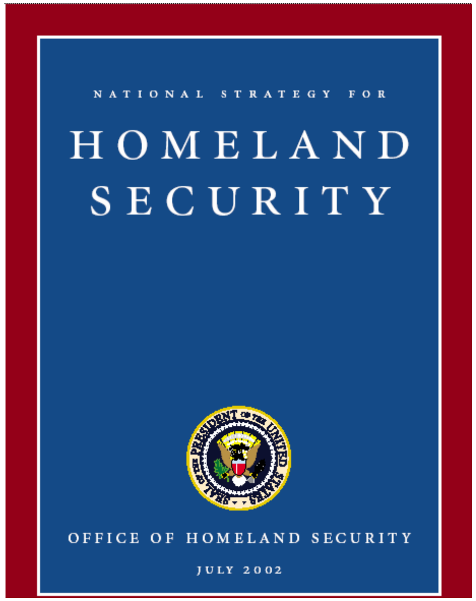
- It can occur on a broader or even national scale (catastrophic)

- Our potential enemies have the intent

- the tools of destruction are broadly available

- Our systems have many well-known vulnerabilities

- a single act can inflict damage in multiple locations simultaneously without the attacker ever having physically entered the United States



NATIONAL STRATEGY FOR

HOMELAND SECURITY

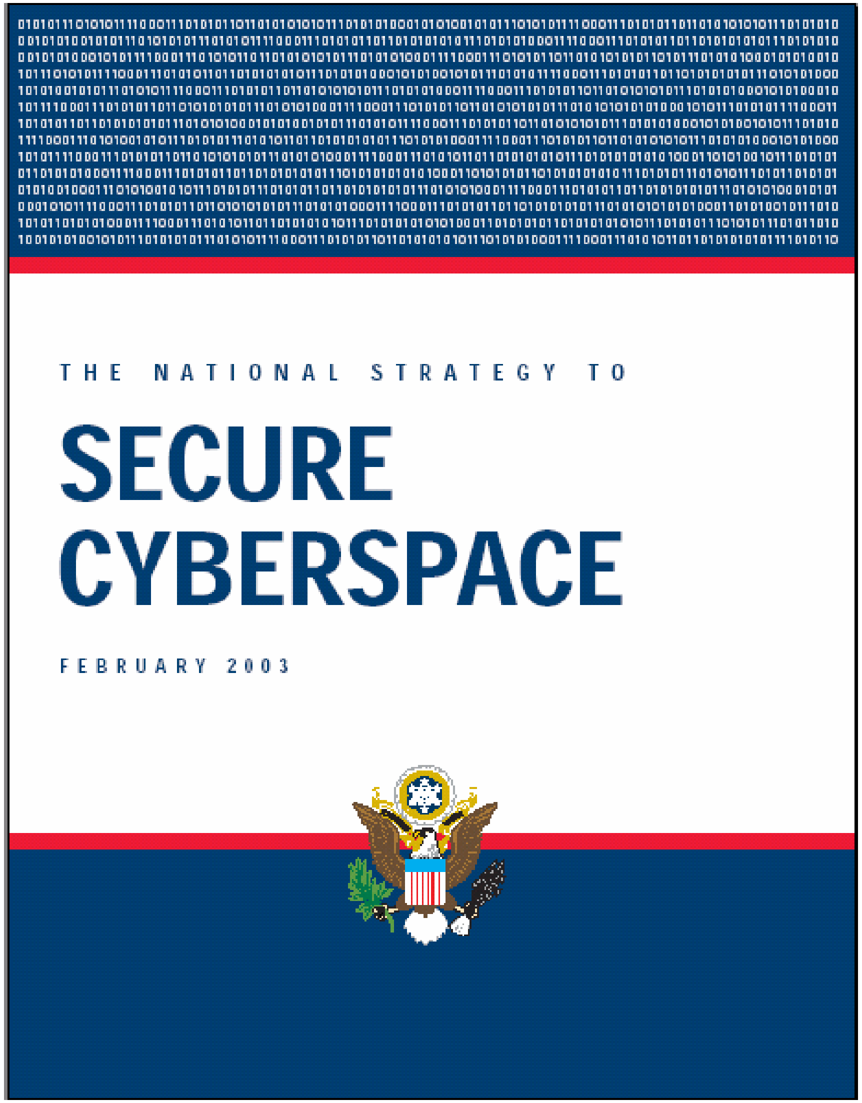
OFFICE OF HOMELAND SECURITY

JULY 2002

EPA’s role is crucial in making sure that the water sector’s security challenges are not overlooked.

The National Strategy for Homeland security stated,

- DHS depends on federal agencies to address a sector’s unique infrastructure challenges. (p31d)
- Government must help enable the private sector’s ability to carry out its protection responsibilities. (p33b)



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

The National Strategy to Secure Cyberspace

Feb. 2003

Under Priority #2 - A National Cyberspace security Threat and Vulnerability Reduction Program:

Page 32

Securing SCADA is a national Priority but complicated because:

- It requires investment in systems and R&D that companies cannot afford or justify on their own.
- Current technological limitations could impede the implementation of security measures.

e.g.-Security features may not be easily adapted, and could also impact the systems' performance/synchronization.

Page ix

A **government role** is warranted:

- When high transaction costs or legal barriers lead to significant coordination problems.
- When there is an absence of private sector forces.
- When incentive problems lead to under provisioning of critical shared resources;
- In raising awareness.

Agenda

1. What is SCADA?
2. SCADA Vulnerabilities
3. Federal Directives
4. **Current Status**

Current Status

- Utility VA's completed/due (copies in EPA vault.)
- Large & mid-sized utility ERP's complete/due, small size due at year end.
- DHS begun SCADA focus in May 2004. (Seeking ideas on how to best approach SCADA)
- EPA beginning SCADA work through WERF et al.
- OIG handing-off SCADA project to EPA

Current Status

- **Utility VA's completed/due (copies in EPA vault.)**
- **Large & mid-sized utility ERP's complete/due, small size due at year end.**
- DHS begun SCADA focus in May 2004. (Seeking ideas on how to best approach SCADA)
- EPA beginning SCADA work through WERF et al.
- OIG handing-off SCADA project to EPA

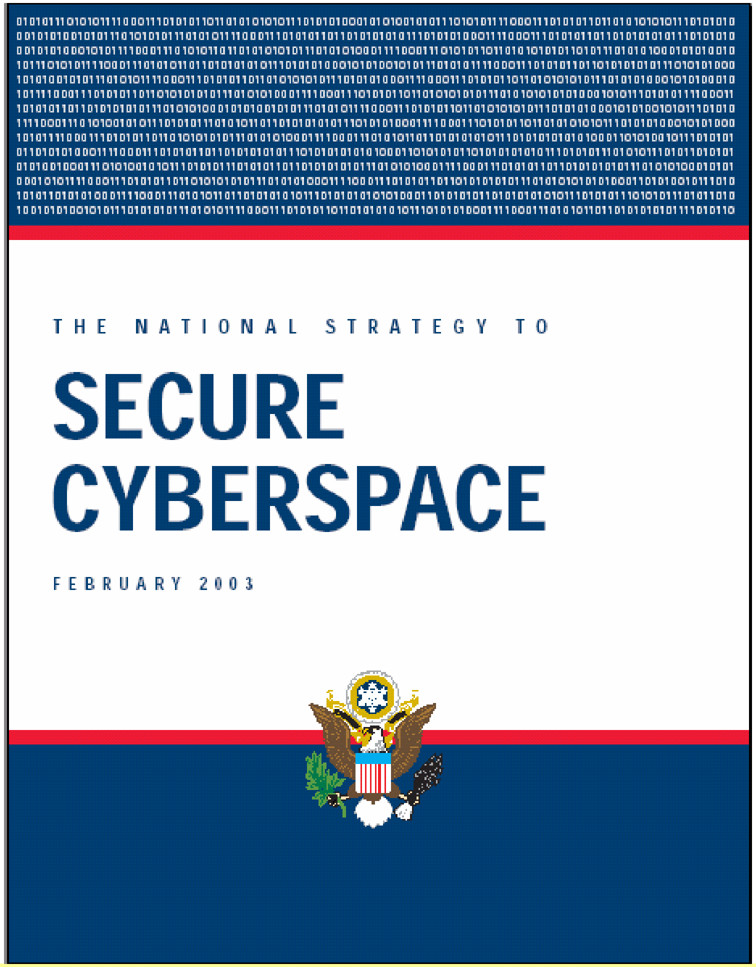
Water Utility **VAs and ERPs are either completed or almost due.**

Schedule under the Bioterrorism Act

Systems serving population of:	Certify and submit **Vulnerability Assessment** by:	Certify **Emergency Response Plan** within 6 months of VA but no later than:
100,000 or greater	March 31, 2003	September 30, 2003
50,000 - 99,999	December 31, 2003	June 30, 2004
3,301 – 49,999	June 30, 2004	December 31, 2004

Current Status

- Utility VA’s completed/due (copies in EPA vault.)
- Large & mid-sized utility ERP’s complete/due, small size due at year end.
- **DHS begun SCADA focus in May 2004. (Seeking ideas on how to best approach SCADA)**
- EPA beginning SCADA work through WERF et al.
- OIG handing-off SCADA project to EPA



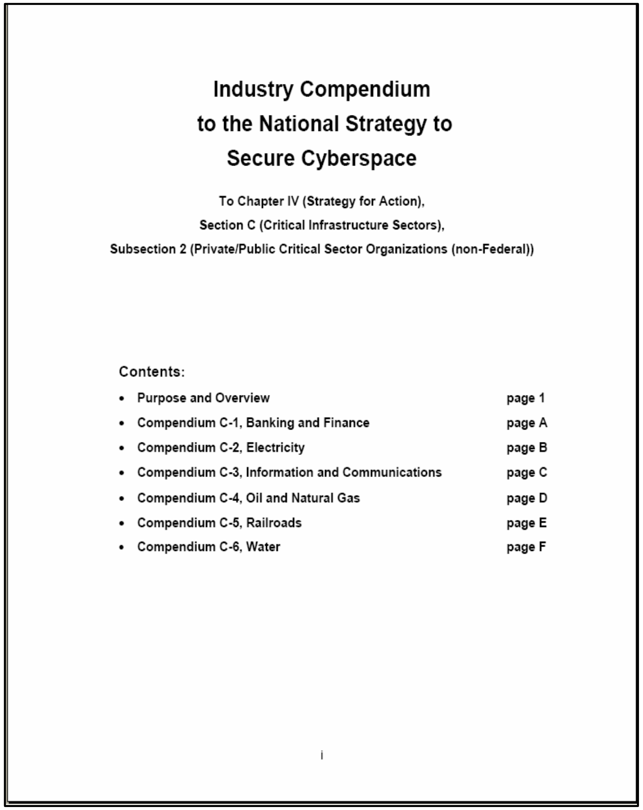
THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

DHS, **in coordination with** the Department of Energy and other **concerned agencies**, will work in partnership with private industry to ensure that there is broad awareness among industry vendors and users, both regulated and unregulated, of the vulnerabilities in DCS/SCADA systems, and the consequences of exploitation of those vulnerabilities.

On May 2004, DHS formed a team to address cyber security concerns, including individuals focusing on SCADA.

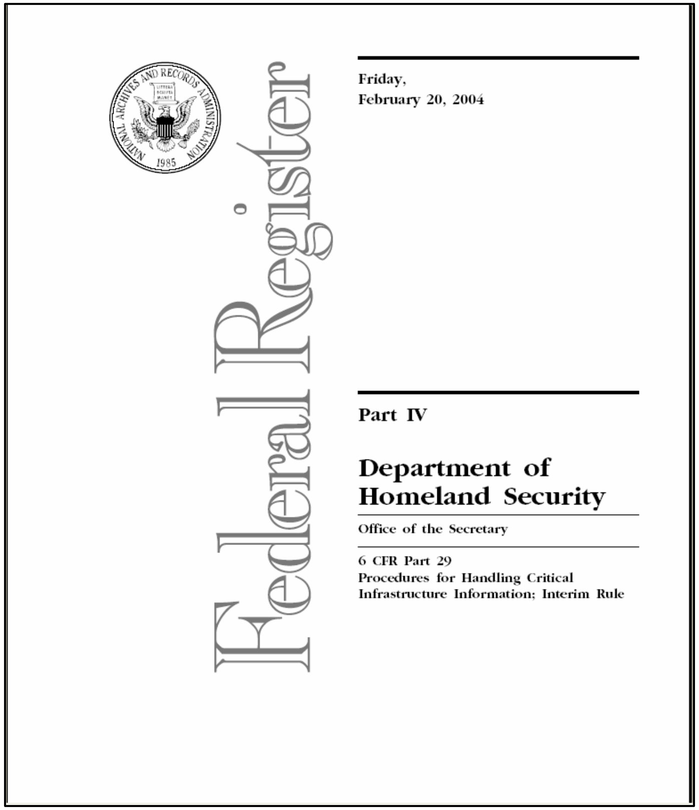


**Industry Compendium
to the National Strategy to
Secure Cyberspace**

To Chapter IV (Strategy for Action),
Section C (Critical Infrastructure Sectors),
Subsection 2 (Private/Public Critical Sector Organizations (non-Federal))

Contents:

i



Federal Register

Friday,
February 20, 2004

Part IV

Department of Homeland Security

Office of the Secretary

6 CFR Part 29
Procedures for Handling Critical Infrastructure Information; Interim Rule

“FOIA, antitrust & liability laws represent barriers to public-private cooperation.”(p.2)

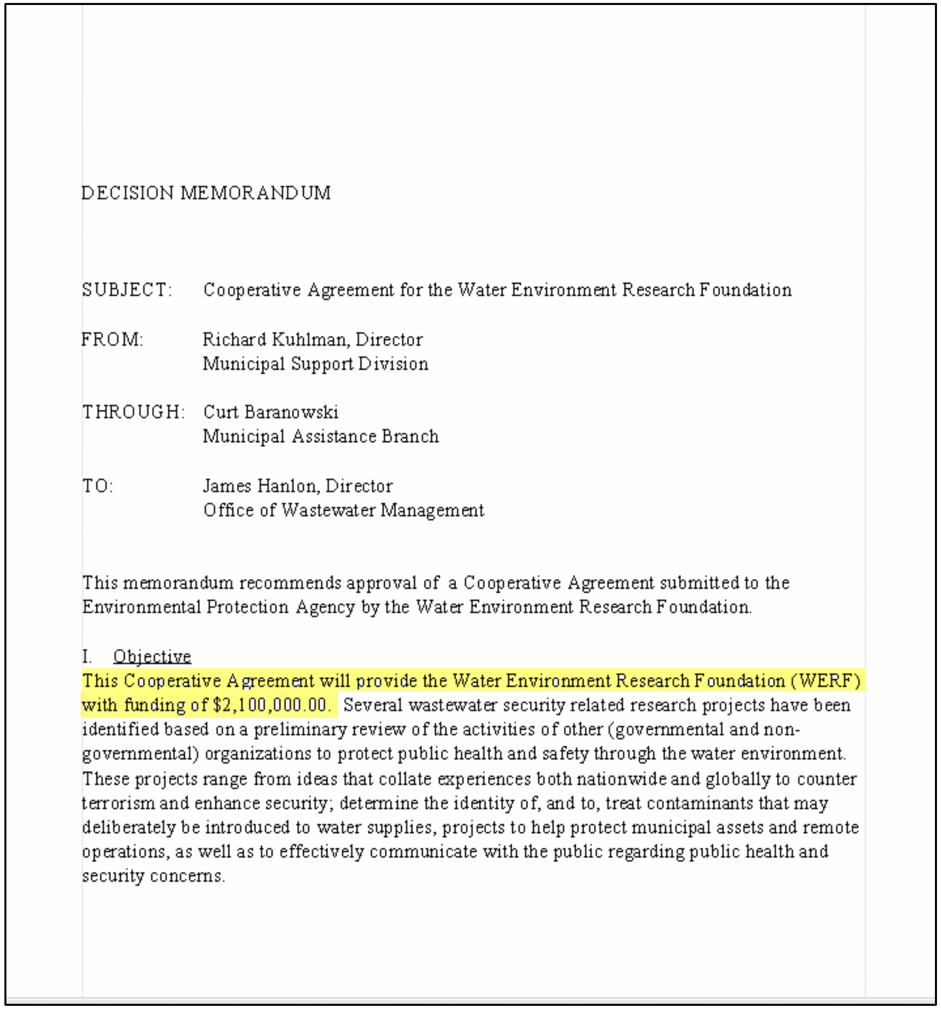
“Protected Critical Infrastructure Information (PCII) protection.”(p.2)

Current Status

- Utility VA's completed/due (copies in EPA vault.)
- Large & mid-sized utility ERP's complete/due, small size due at year end.
- DHS begun SCADA focus in May 2004. (Seeking ideas on how to best approach SCADA)
- **EPA beginning SCADA work through WERF et al.**
- OIG handing-off SCADA project to EPA

EPA awarded $2.1 million to WERF, including $250k for SCADA research.

WERF awarded almost $300,000 to EMA, Inc. to conduct the SCADA research.



DECISION MEMORANDUM

SUBJECT: Cooperative Agreement for the Water Environment Research Foundation

FROM: Richard Kuhlman, Director
Municipal Support Division

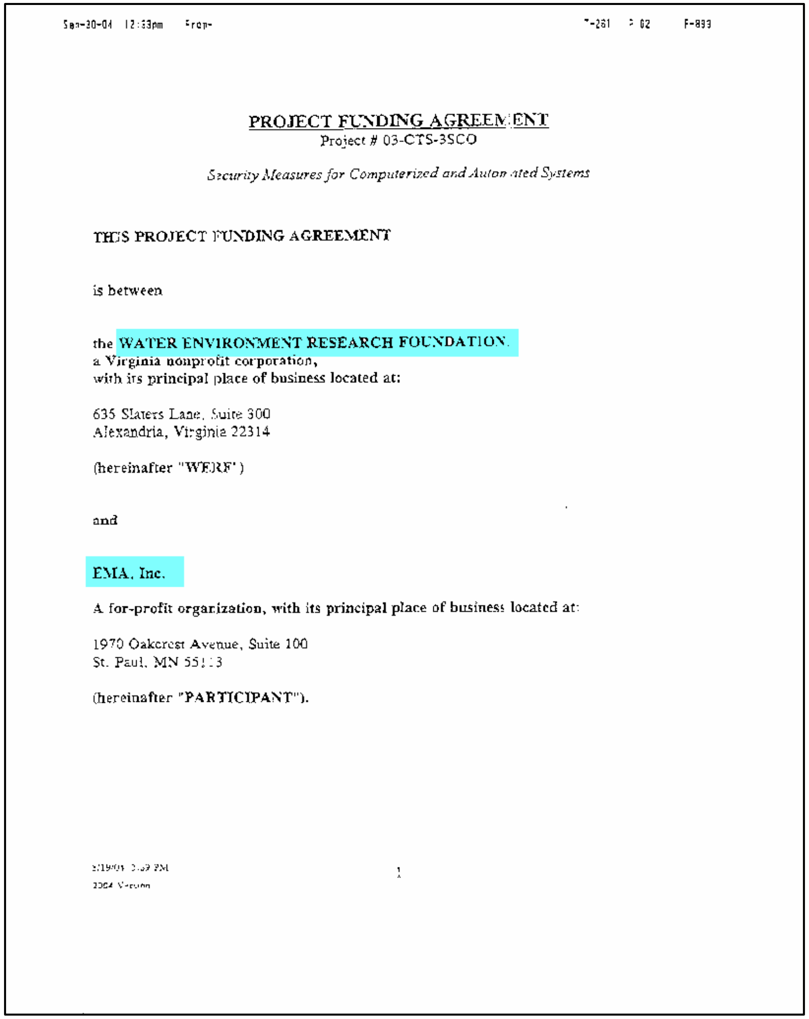
THROUGH: Curt Baranowski
Municipal Assistance Branch

TO: James Hanlon, Director
Office of Wastewater Management

This memorandum recommends approval of a Cooperative Agreement submitted to the Environmental Protection Agency by the Water Environment Research Foundation.

I. Objective

This Cooperative Agreement will provide the Water Environment Research Foundation (WERF) with funding of $2,100,000.00. Several wastewater security related research projects have been identified based on a preliminary review of the activities of other (governmental and non-governmental) organizations to protect public health and safety through the water environment. These projects range from ideas that collate experiences both nationwide and globally to counter terrorism and enhance security; determine the identity of, and to, treat contaminants that may deliberately be introduced to water supplies, projects to help protect municipal assets and remote operations, as well as to effectively communicate with the public regarding public health and security concerns.



Sep-30-04 12:33pm From- T-261 P 02 F-893

PROJECT FUNDING AGREEMENT
Project # 03-CTS-3SCO

Security Measures for Computerized and Automated Systems

THIS PROJECT FUNDING AGREEMENT

is between

the WATER ENVIRONMENT RESEARCH FOUNDATION,
a Virginia nonprofit corporation,
with its principal place of business located at:

635 Slaters Lane, Suite 300
Alexandria, Virginia 22314

(hereinafter "WERF")

and

EMA, Inc.

A for-profit organization, with its principal place of business located at:

1970 Oakcrest Avenue, Suite 100
St. Paul, MN 55113

(hereinafter "PARTICIPANT").

2/19/04 3:59 PM
2004 Version
1

Current Status

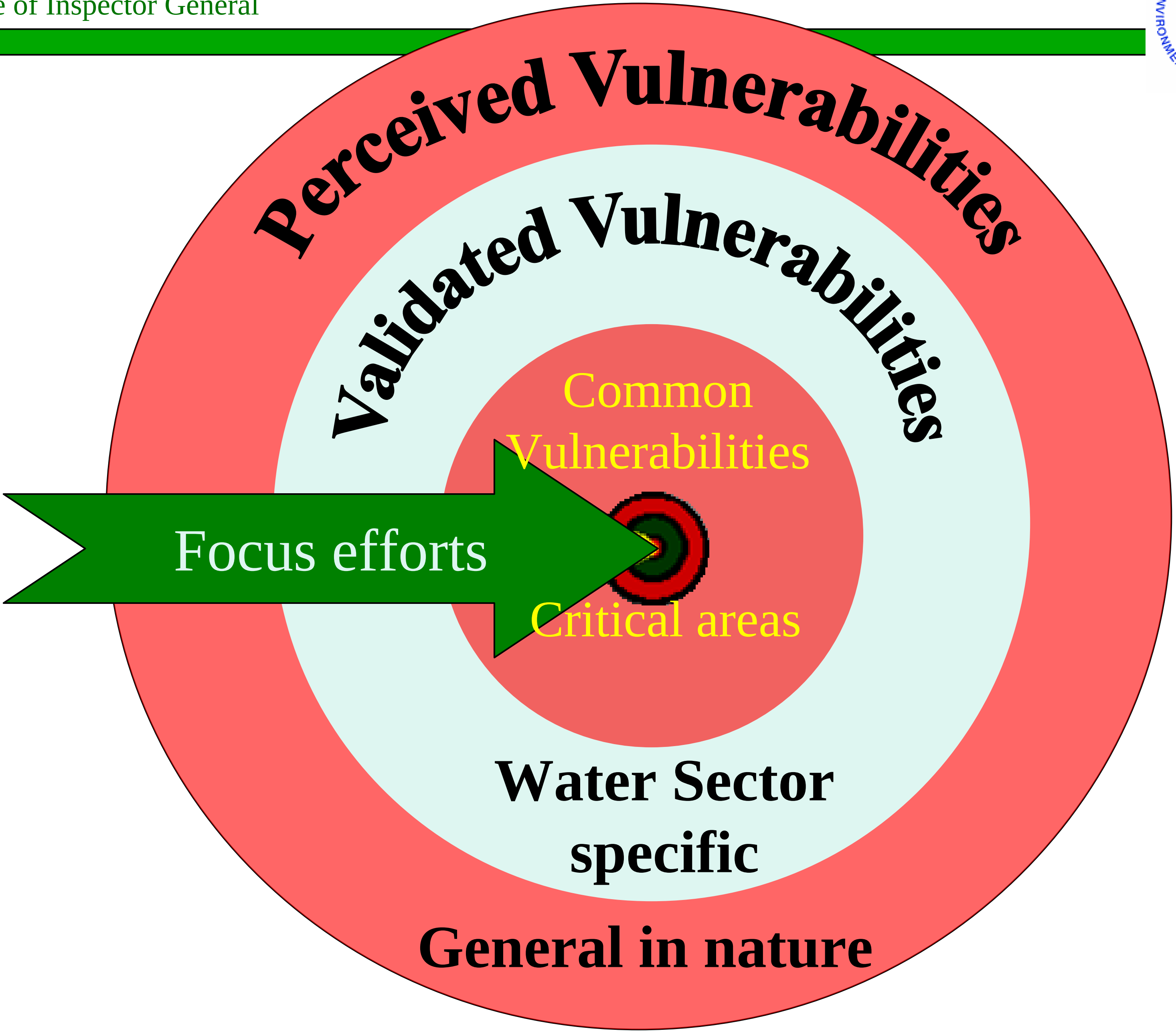
- Utility VA's completed/due (copies in EPA vault.)
- Large & mid-sized utility ERP's complete/due, small size due at year end.
- DHS begun SCADA focus in May 2004. (Seeking ideas on how to best approach SCADA)
- EPA beginning SCADA work through WERF et al.
- **OIG handing-off SCADA project to EPA**

What barriers, if any, prevent water systems from successfully securing known SCADA vulnerabilities?

- Determine specific SCADA vulnerabilities identified by water systems and others.
- Determine if identified vulnerabilities are being adequately addressed.
- Determine the reasons behind impediments where water systems cannot successfully reduce or mitigate identified vulnerabilities.
- Determine actions EPA can take to remove impediments.

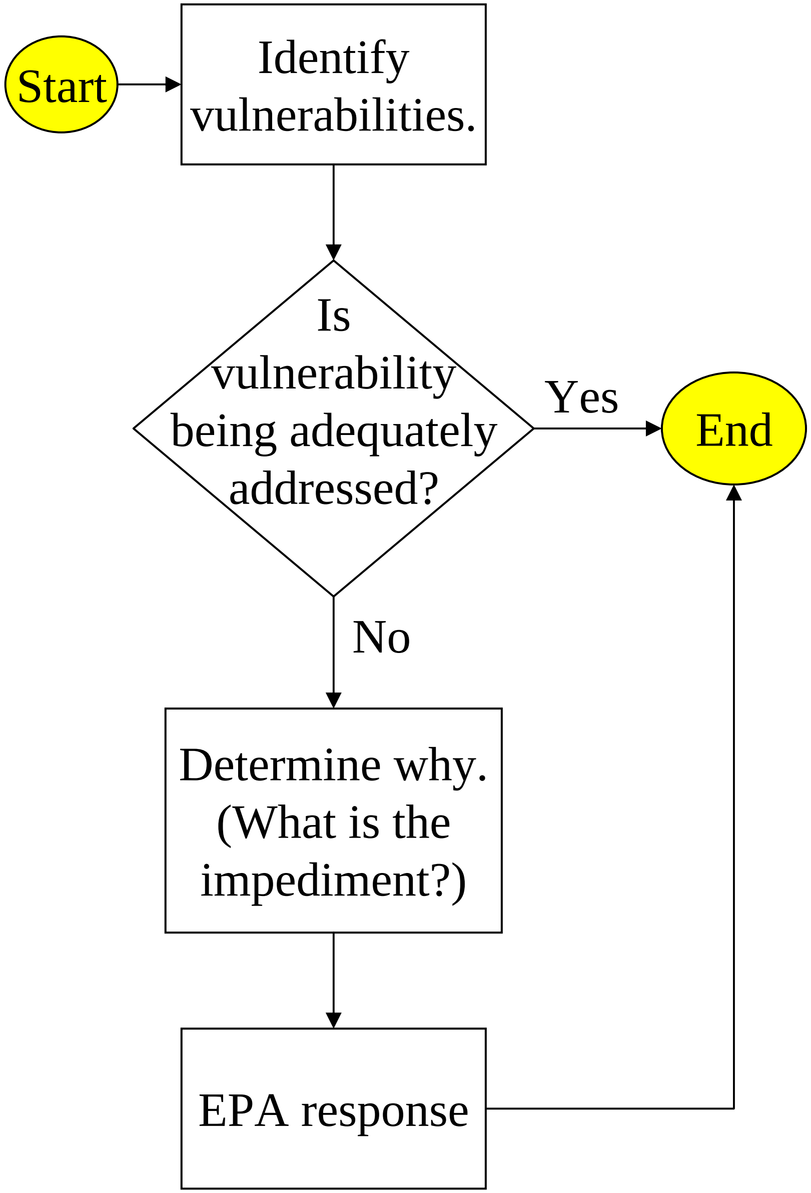
What barriers, if any, prevent water systems from successfully securing known SCADA vulnerabilities?

Goal 1 Identify Vulnerabilities			
Critical #1			
Critical #2			
Common #1			
Common #2			


Perceived Vulnerabilities
Validated Vulnerabilities
Common Vulnerabilities
Focus efforts
Critical areas
Water Sector specific
General in nature

What barriers, if any, prevent water systems from successfully securing known SCADA vulnerabilities?

Goal 1 Identify Vulnerabilities	**Goal 2** Adequately Addressed?	**Goal 3** Why not?	**Goal 4** EPA Response
Critical #1	No	Reason 1 Reason 2	Response 1 Response 2
Critical #2	Yes	N/A	N/A
Common #1	Yes	N/A	N/A
Common #2	No	Reason 1 Reason 2 Reason 3	Response 3 Response 4 Alert DHS/other


Start
Identify vulnerabilities.
Is vulnerability being adequately addressed?
Yes
End
No
Determine why. (What is the impediment?)
EPA response

Goal 1

Determine Specific SCADA vulnerabilities identified by water systems and others.

Goal 2

Determine if identified vulnerabilities are being adequately addressed.

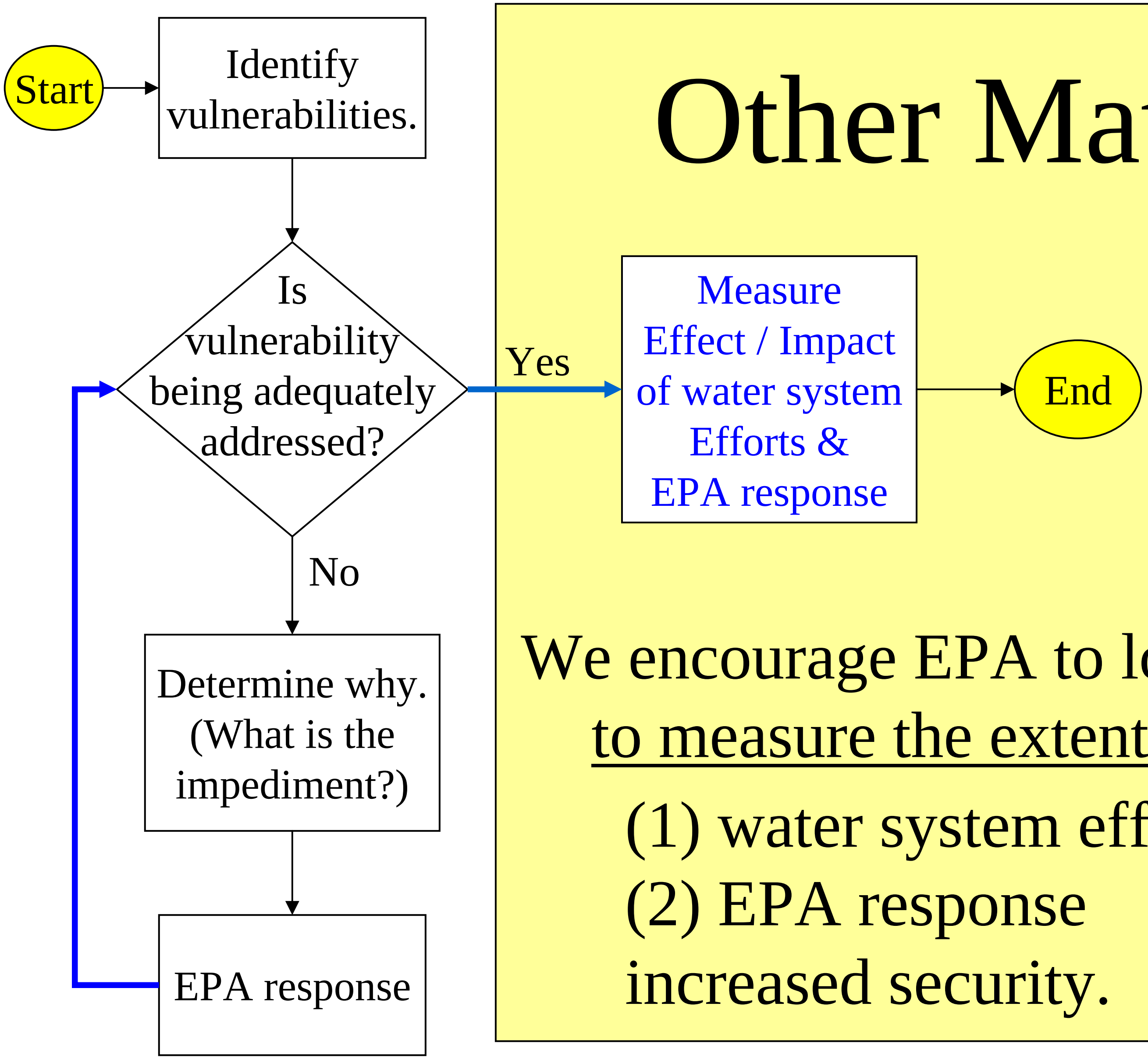
Goal 3

Determine the impediments behind instances where utilities cannot successfully reduce or mitigate identified vulnerabilities.

Goal 4

Determine actions EPA can take to remove the impediments.

Other Matters


Start
Identify vulnerabilities.
Is vulnerability being adequately addressed?
Yes
Measure Effect / Impact of water system Efforts & EPA response
End
No
Determine why. (What is the impediment?)
EPA response

We encourage EPA to look for ways <u>to measure the extent to which:</u>

(1) water system efforts and
(2) EPA response
increased security.

<u>For questions contact:</u>

Ricardo Martinez	**(212) 637-3045**
Andrew McLaughlin	**(202) 566-2591**