2008 Automation Summit
A Users Conference

ID#: 2481
Title: Control System Security Assessments
Track: Industrial Security

Presenters: Marty Edwards
Idaho National Laboratory

Todd Stauffer
Siemens

SIEMENS

Cyber Security Series at the Summit

2488 – Catch me if you can

Real Life Examples of Security Professionals Breaking into Industrial Control Rooms and Corporate Offices

Jonathan Pollet (Industrial Defender)

2481 – Control System Security Assessments

You are here !

6 – Cyber Security Panel Session

4:15pm – 5:30pm

Room 327

Control System Security Assessments

2008 Siemens Automation Summit

Program Sponsor:

Control Systems Security Program

National Cyber Security Division

U.S. Department of Homeland Security

Homeland Security

Presenter

Marty Edwards

Idaho National Laboratory

17+ yrs of experience working with control systems from the perspectives of a vendor and an end user

Marty.Edwards@inl.gov

(208) 526-9372

Homeland Security

Session Overview

- Introduction
- Vulnerabilities and Threat Trends
- Assessment Findings
- Control Systems Security Program Review
- Summary and Questions

- Hand over to Todd Stauffer – Siemens

Definition of a Control System

The term “Industrial Control System” (ICS) refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety Instrumented System)
- Any other automated control system

Homeland Security

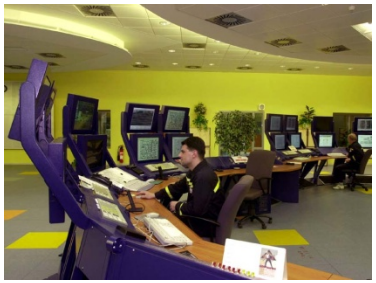
Control System Basics

Sensors

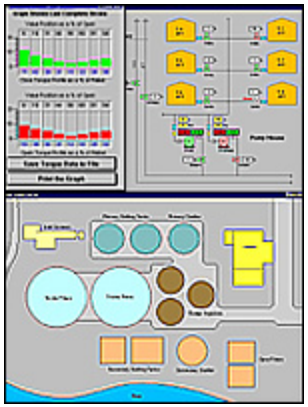
Motor Controls

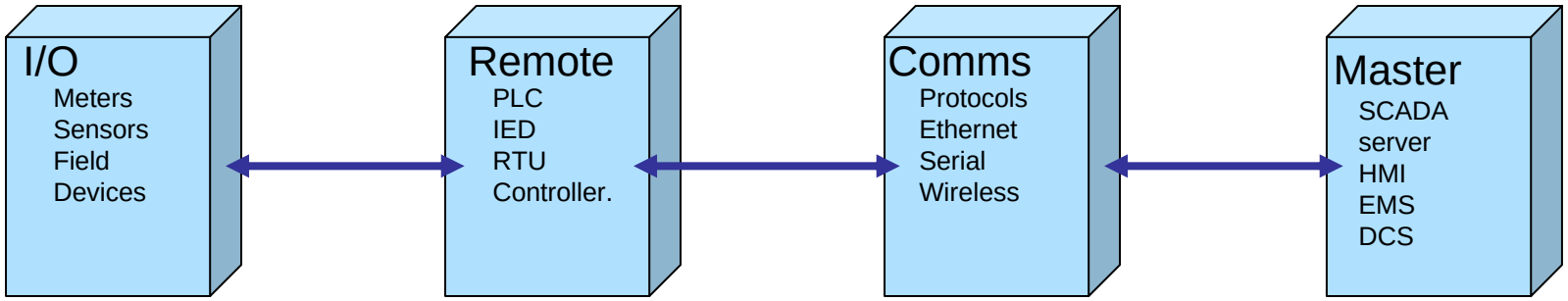
Control Valves

Programmable Logic Controllers (PLC)



Human Machine Interfaces (HMI) and Operator Displays





Field Devices

Control Center

Homeland Security

Evolution – Panel Based Controls

- Push Buttons
- Single Loop Controls
- Stand Alone
- No Networks
- No Communication

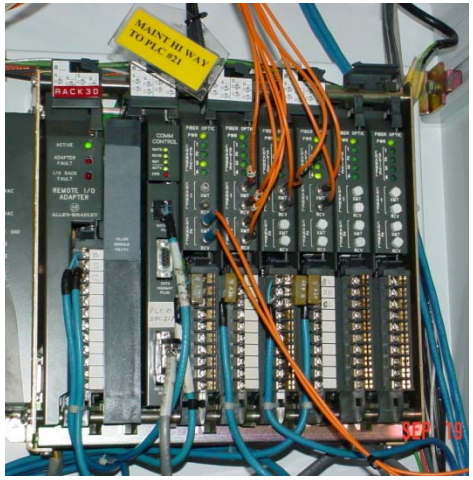
From a cyber security standpoint this system is

'isolated'

Homeland Security

Evolution – Legacy Equipment

- Proprietary Networks
- Proprietary OS
- No Ethernet
- No Intranet connections
- “Security by Obscurity”



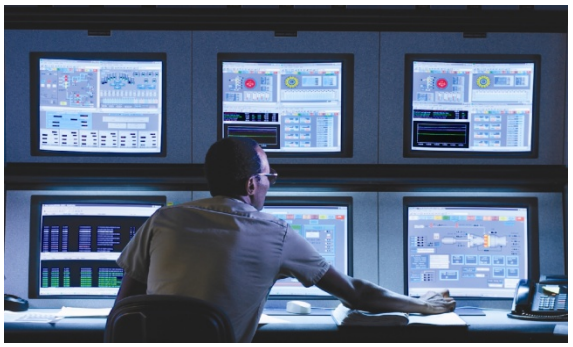
From a cyber security standpoint this system is

‘exploitable – but not a trivial task’

Homeland Security

Evolution – Modern Equipment

- Ethernet everywhere
- Wireless ‘in the rack’
- Remote configuration
- Windows & Linux OS
- Commercial Off The Shelf (COTS)



From a cyber security standpoint this system is

‘a huge challenge – readily exploitable’

Homeland Security

Control from your PDA

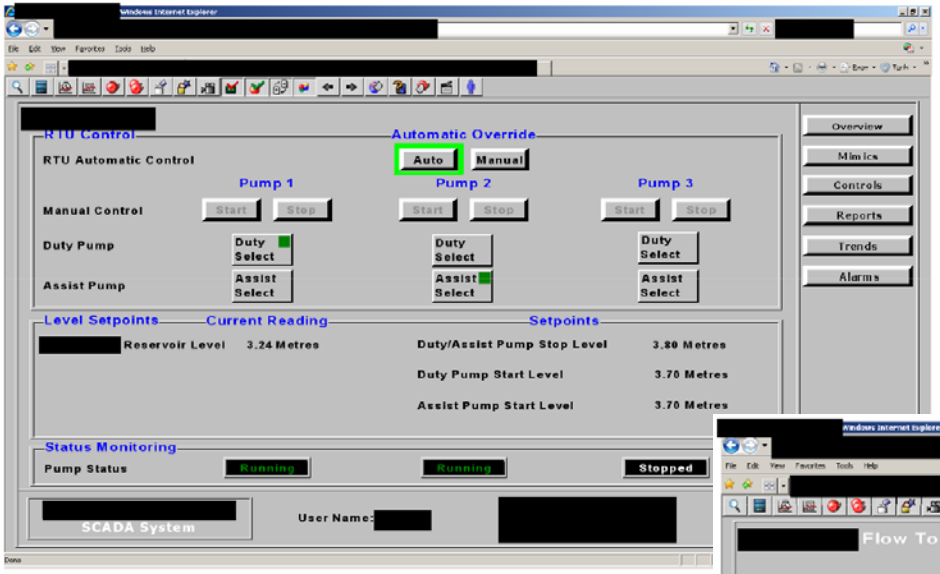
- Advancements will make accessing key systems very easy
- Applications running on known-to-be-vulnerable systems

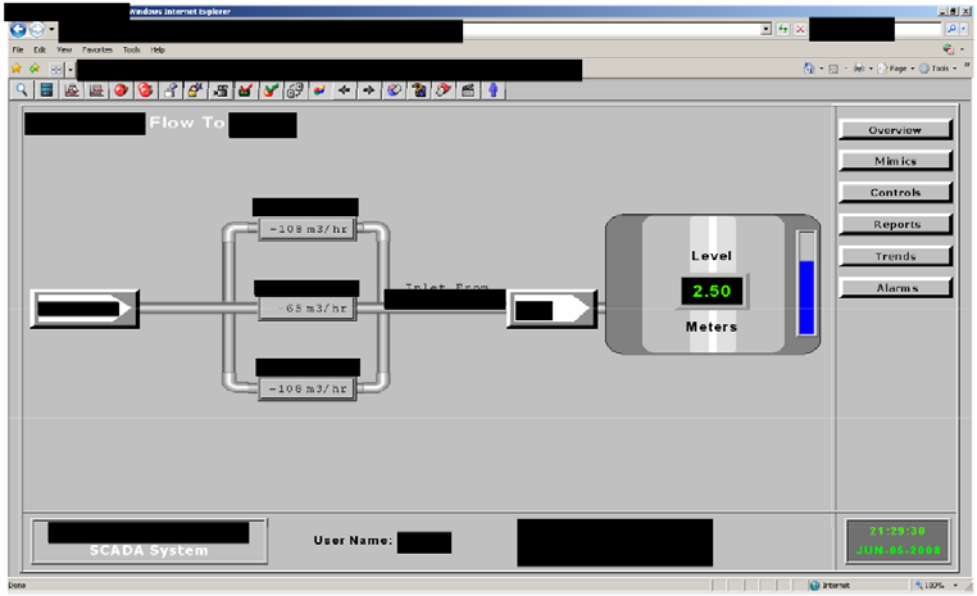
Homeland Security

Control via the Internet

- Systems are DIRECTLY connected to the Internet
- Some of these systems have very poor security:
  - Lack of encryption methods (like VPN access)
  - Sites use published vendor default passwords
  - Sites using domain names that point to function like “SCADAforyourcity.com”
- Utilizing Internet search engines it is quite easy to find some of these sites…

Example HMI access from the web





These screens actually have control of a city's water pumping facility

Real HMI screens pulled off the Internet

HMI only required vendor default usernames to login

Homeland Security

Control Systems Are Gaining Interest

- Currently, a cyber attack on Industrial Control Systems is one of the only ways to induce real-world physical actions from the virtual realm of the Internet
- This is leading to an increased level of interest in Industrial Control Systems by ‘black hat’ groups

Due to the complex nature of network-based control systems, it becomes very hard to distinguish between normal operational nuances and an actual attack.

Homeland Security

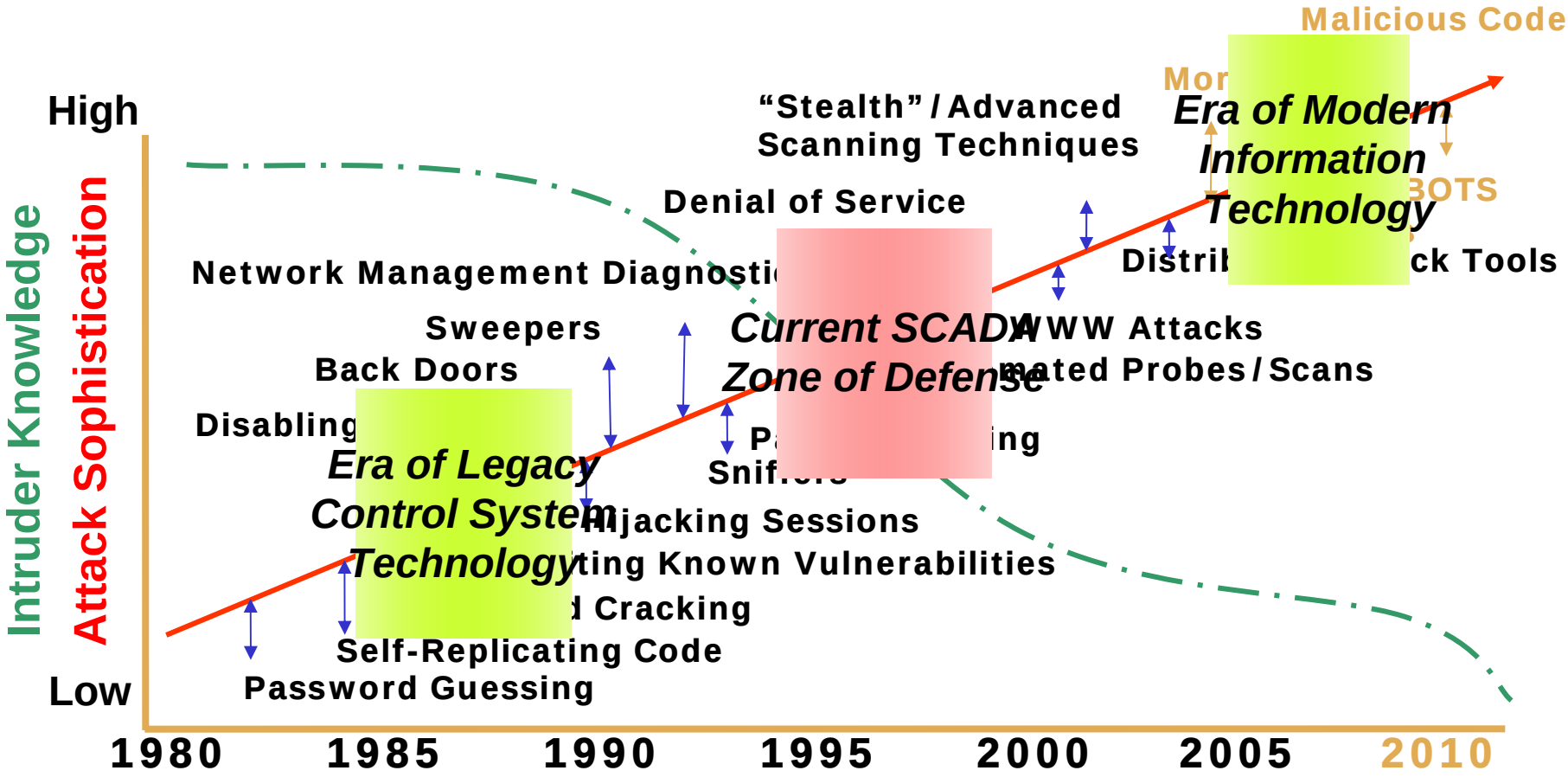
Risk Drivers: Threats

- International and domestic terrorism, and nation state cyber warfare – asymmetric warfare
  - Interdependency of critical sectors can increase the overall appeal using cyber as an attack tool
- Internet increases availability of hacker tools along with information about infrastructures and control systems
- Emergence of a strong financial motive for cyber crime to exploit vulnerabilities

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities." – CIA Senior Analyst

Homeland Security

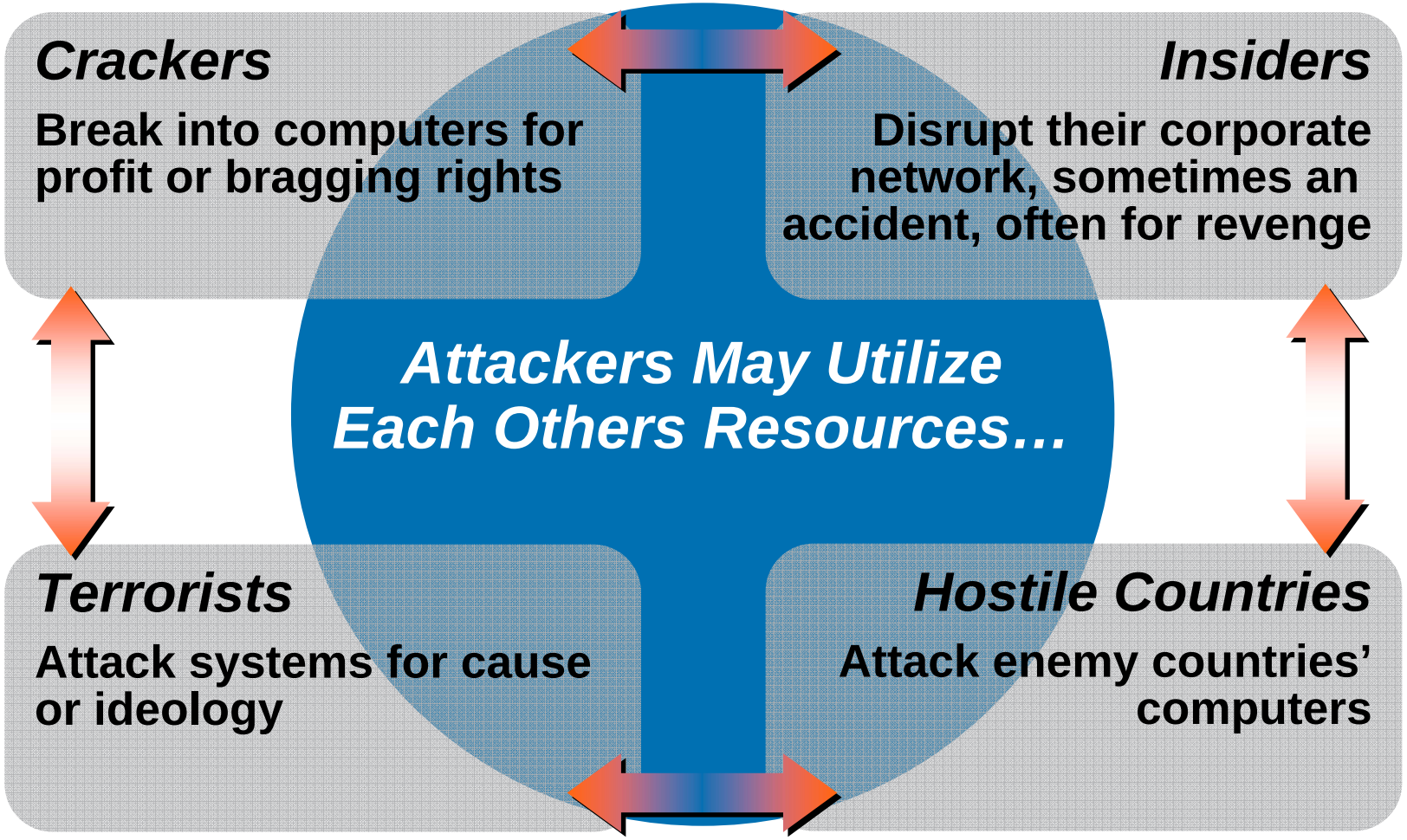
Cyber Threat Trends



Lipson, H. F., *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Special Report CMS/SEI-2002-SR-009, November 2002, page 10.

Homeland Security

Types of Attackers



Homeland Security

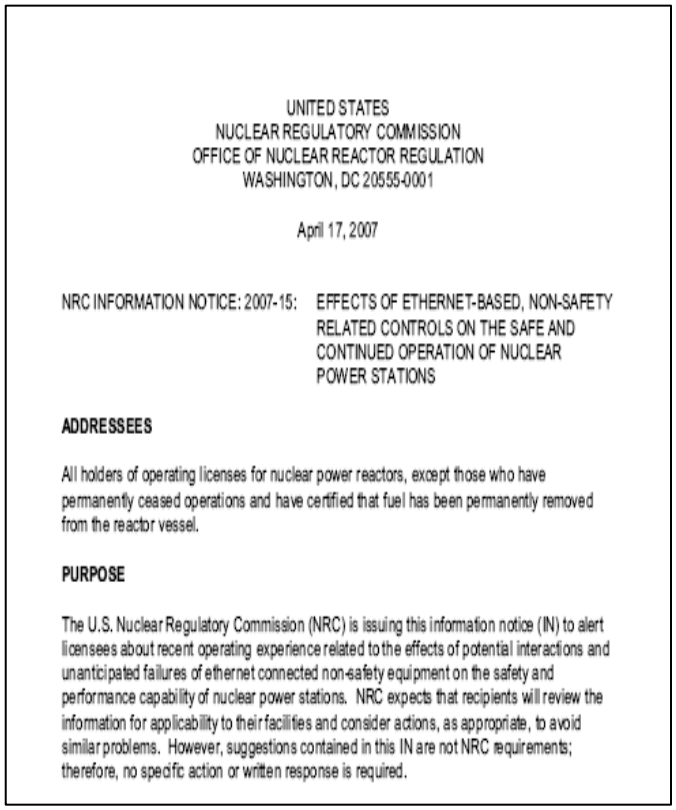
Cyber Incidents

Incident
Plant shutdown from game installed from infected disk onto a PLC workstation.
Virus ‘fix’ erased licensing keys.
2003 SoBig virus affected rail dispatch and signaling systems, halting train service for 6 hours.
2004 Sasser worm disabled oil platforms for 2 days by crawling through the network via HTTP and NetBios ports.

- 100’s of documented cases exist, but details are often sketchy

Homeland Security

Brown's Ferry (TVA)



UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
WASHINGTON, DC 20555-0001

April 17, 2007

NRC INFORMATION NOTICE: 2007-15: EFFECTS OF ETHERNET-BASED, NON-SAFETY RELATED CONTROLS ON THE SAFE AND CONTINUED OPERATION OF NUCLEAR POWER STATIONS

ADDRESSEES

All holders of operating licenses for nuclear power reactors, except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel.

PURPOSE

The U.S. Nuclear Regulatory Commission (NRC) is issuing this information notice (IN) to alert licensees about recent operating experience related to the effects of potential interactions and unanticipated failures of ethernet connected non-safety equipment on the safety and performance capability of nuclear power stations. NRC expects that recipients will review the information for applicability to their facilities and consider actions, as appropriate, to avoid similar problems. However, suggestions contained in this IN are not NRC requirements; therefore, no specific action or written response is required.

- August 19,2006
- Not a cyber attack, but clearly shows impact of a cyber incident on NPP operations
- Variable Frequency Drives (VFD) on recirculation pumps became non-responsive

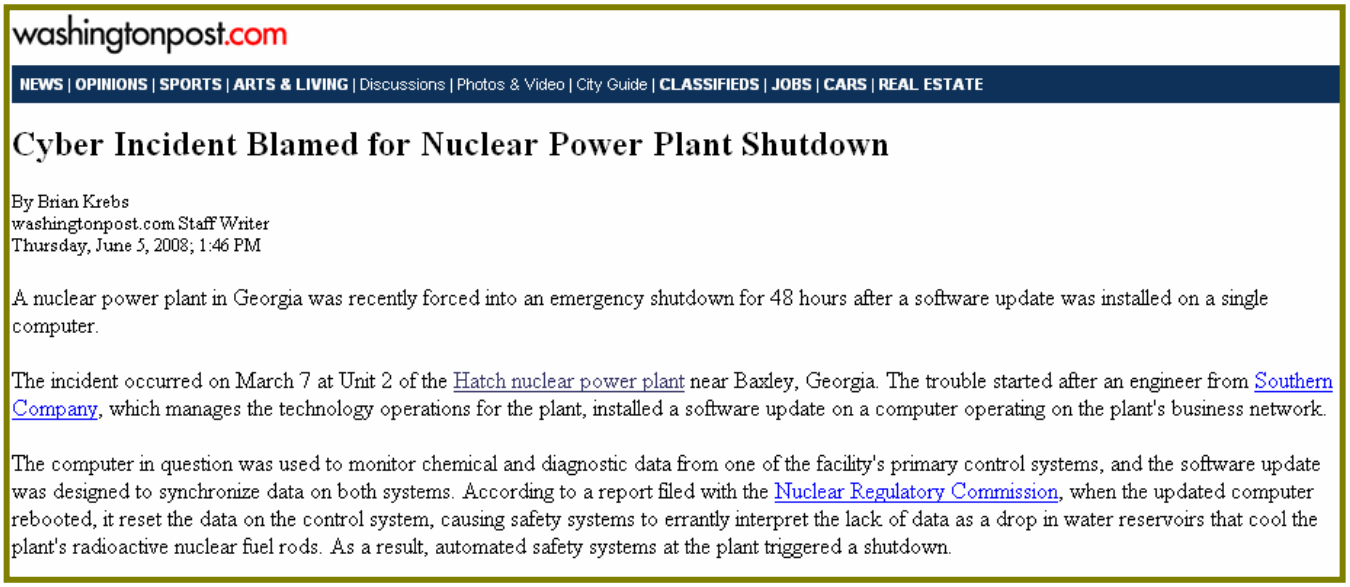
The licensee determined that the root cause of the event was the malfunction of the VFD controller because of excessive traffic on the plant ICS network.

Homeland Security

Hatch NPP

- Introduction of SW caused SIS to initiate plant shutdown
- Connection from Corp to SCADA ensure a synchronization and reboot of all machines
- System behaved as it was supposed to

…there was full two-way communication between certain computers on the plant's corporate and control networks.



washingtonpost.com

NEWS | OPINIONS | SPORTS | ARTS & LIVING | Discussions | Photos & Video | City Guide | CLASSIFIEDS | JOBS | CARS | REAL ESTATE

Cyber Incident Blamed for Nuclear Power Plant Shutdown

By Brian Krebs
washingtonpost.com Staff Writer
Thursday, June 5, 2008; 1:46 PM

A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.

The incident occurred on March 7 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia. The trouble started after an engineer from Southern Company, which manages the technology operations for the plant, installed a software update on a computer operating on the plant's business network.

The computer in question was used to monitor chemical and diagnostic data from one of the facility's primary control systems, and the software update was designed to synchronize data on both systems. According to a report filed with the Nuclear Regulatory Commission, when the updated computer rebooted, it reset the data on the control system, causing safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown.

Homeland Security

Harrisburg, PA water facility

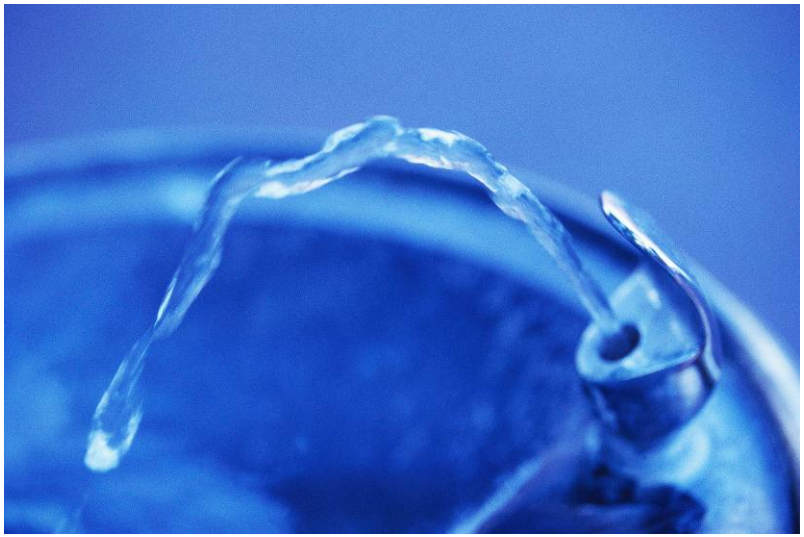
Water Tech ONLINE www.watertechonline.com

Legal Briefs - 11/1/2006 1:46:48 PM

PA water plant tapped by computer hackers

HARRISBURG, PA – The FBI is investigating a security breach in which hackers gained access to the computer system at a Harrisburg drinking water treatment plant, according to a November 1 report on InfoWorld.

The breach, which was discovered earlier this month, occurred after a laptop used by a plant employee was accessed by hackers via the Internet and used to install a computer virus and "spyware" on the plant's computer system, the article noted.



Homeland Security

Polish Trains

Telegraph.co.uk

Schoolboy hacks into city's tram system

By Graeme Baker
Last Updated: 2:48am GMT 11/01/2008

A teenage boy who hacked into a Polish tram system used it like "a giant train set", causing chaos and derailing four vehicles.

The 14-year-old, described by his teachers as a model pupil and an electronics "genius", adapted a television remote control so it could change track points in the city of Lodz.

Twelve people were injured in one derailment, and the boy is suspected of having been involved in several similar incidents.

The boy, described as a 'genius' and some of the equipment he used

The teenager, who was not named by police, told them he had changed the points for a prank.

A police statement said he had trespassed at tram depots in the city to gather information and the equipment needed to build the infra-red device.

Homeland Security

Insider Threat

2 deny hacking into L.A.'s traffic light system

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

By Sharon Bernstein and Andrew Blankstein, Times Staff Writers - January 9, 2007

Back in August, the union representing the city's traffic engineers vowed that on the day of their work action, "Los Angeles is not going to be a fun place to drive."

City officials took the threat seriously.

Fearful that the strikers could wreak havoc on the surface street system, they temporarily blocked all engineers from access to the computer that controls traffic signals.

But officials now allege that two engineers, Kartik Patel and Gabriel Murillo, figured out how to hack in anyway. With a few clicks on a laptop computer, the pair — one a renowned traffic engineer profiled in the national media, the other a computer whiz who helped build the system — allegedly tied up traffic at four intersections for several days.

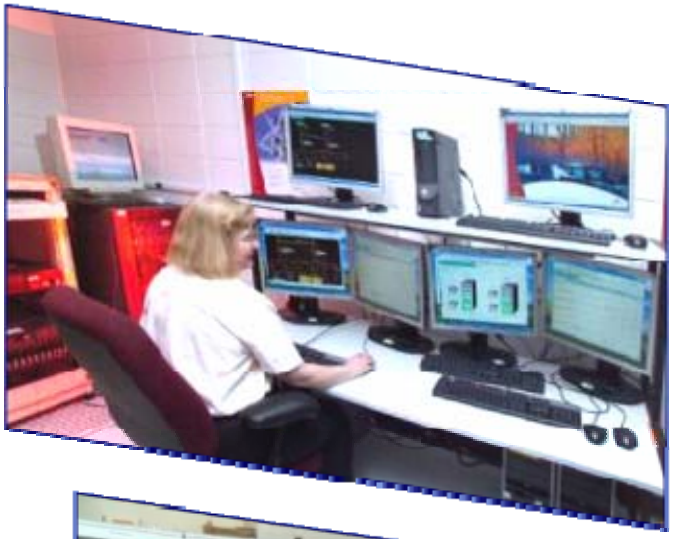
Los Angeles Times

Homeland Security

Technology Assessments

Vendor Assessment Objectives

- Control Systems Vendor Partnership
- Utilizing expertise at Control Systems Security Center (CSSC)
- Benefits:
  - Identify specific cyber security vulnerabilities
  - Mitigate vulnerability in partnership with vendors
  - Deliver cyber security solutions to end users through patches and products



Homeland Security

Assessments

- Joint findings from government sector agencies and company sponsored programs
- Assessments were both on-site and lab based
- Assessments typically consist of:
  - Interviewing control system operators, engineers, and IT staff on configuration and use
  - Touring the facility to see how things actually operate
  - Doing a “table top” review of network and security (firewalls, IDS/IPS, etc.)
  - In some cases, scanning the network and carrying out penetration type testing in a non-threatening posture (bench test, secondary system)

Assessment General Findings

- Default vendor accounts and passwords still in use
  - Some systems hardcoded and unable to be changed!
- Guest accounts still available
- Unused software and services still on systems
- No security-level agreement with peer sites
- No security-level agreement with vendors
- Poor patch management (or patch programs)
- Extensive auto-logon capability

Some findings can provide for attack vectors

Homeland Security

Assessment General Findings
continued

- Typical IT protections not widely used (firewalls, IDS, etc.)
  - This has been improving in the last 6 months
- Little emphasis on reviewing security logs (Change management)
- Control system use of enterprise services (DNS, etc.)
- Shared passwords
- Web enabled critical field devices

Homeland Security

NERC Top 10 Vulnerabilities – 2007

As identified by the Control System Security Working Group

1. Inadequate policies, procedures, and culture that govern control system security
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms
3. Remote access to the control system without appropriate access control
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained
5. Use of inadequately secured wireless communication for control

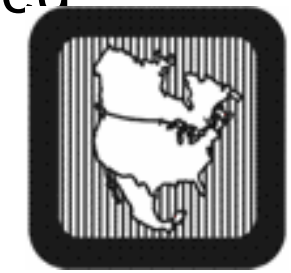
These are not in any order of importance

Homeland Security

NERC Top 10 Vulnerabilities continued

6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity
8. Unauthorized or inappropriate applications or devices on control system networks
9. Control systems command and control data not authenticated
10. Inadequately managed, designed, or implemented critical support infrastructure

These are not in any order of importance



Homeland Security

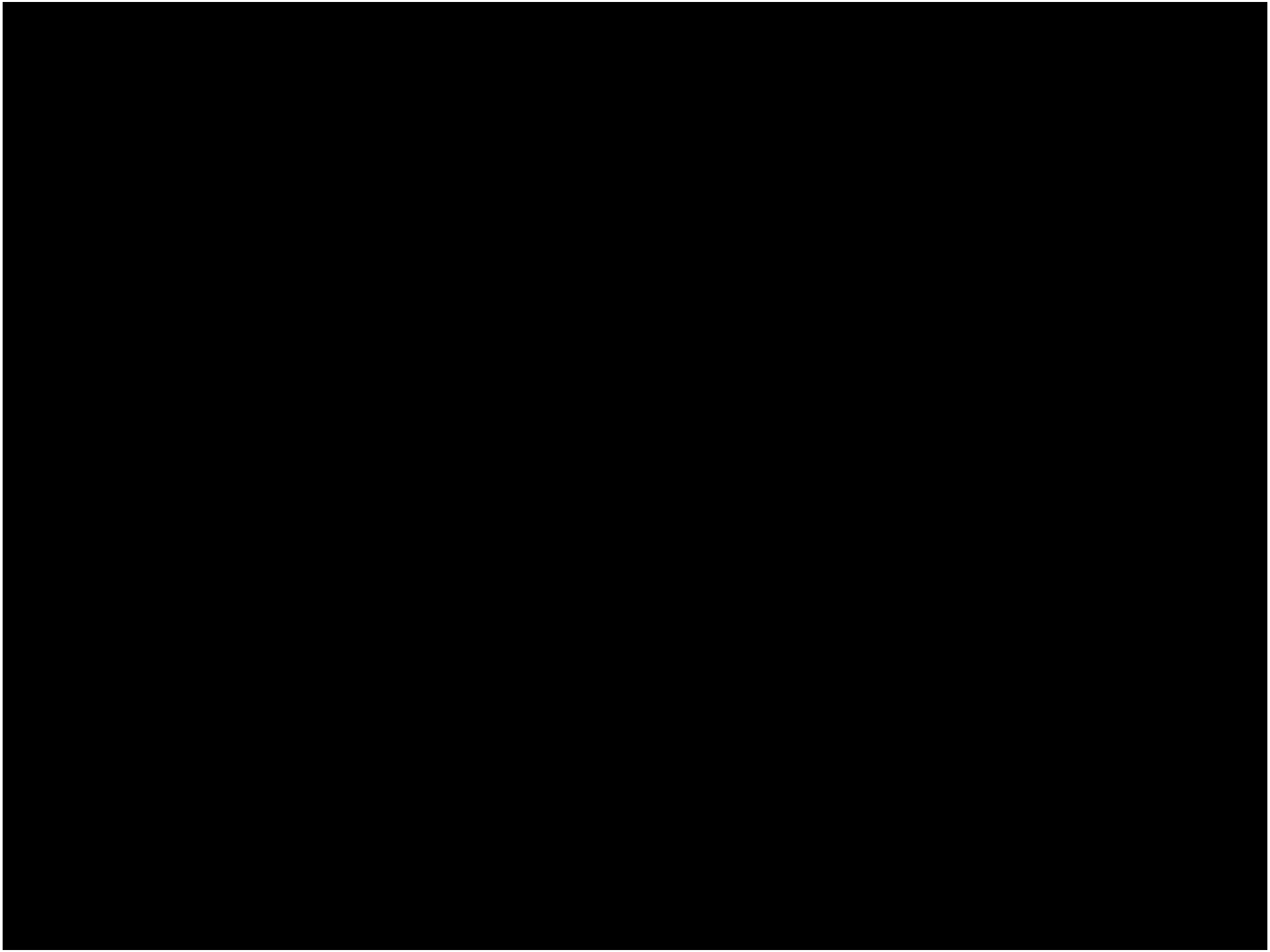
Chemical Sector Awareness Video

Developed in partnership between:

- *U.S. Department of Homeland Security*
  National Cyber Security Division
  Control Systems Security Program

- *American Chemistry Council*
  Chemical Sector Cyber Security Program

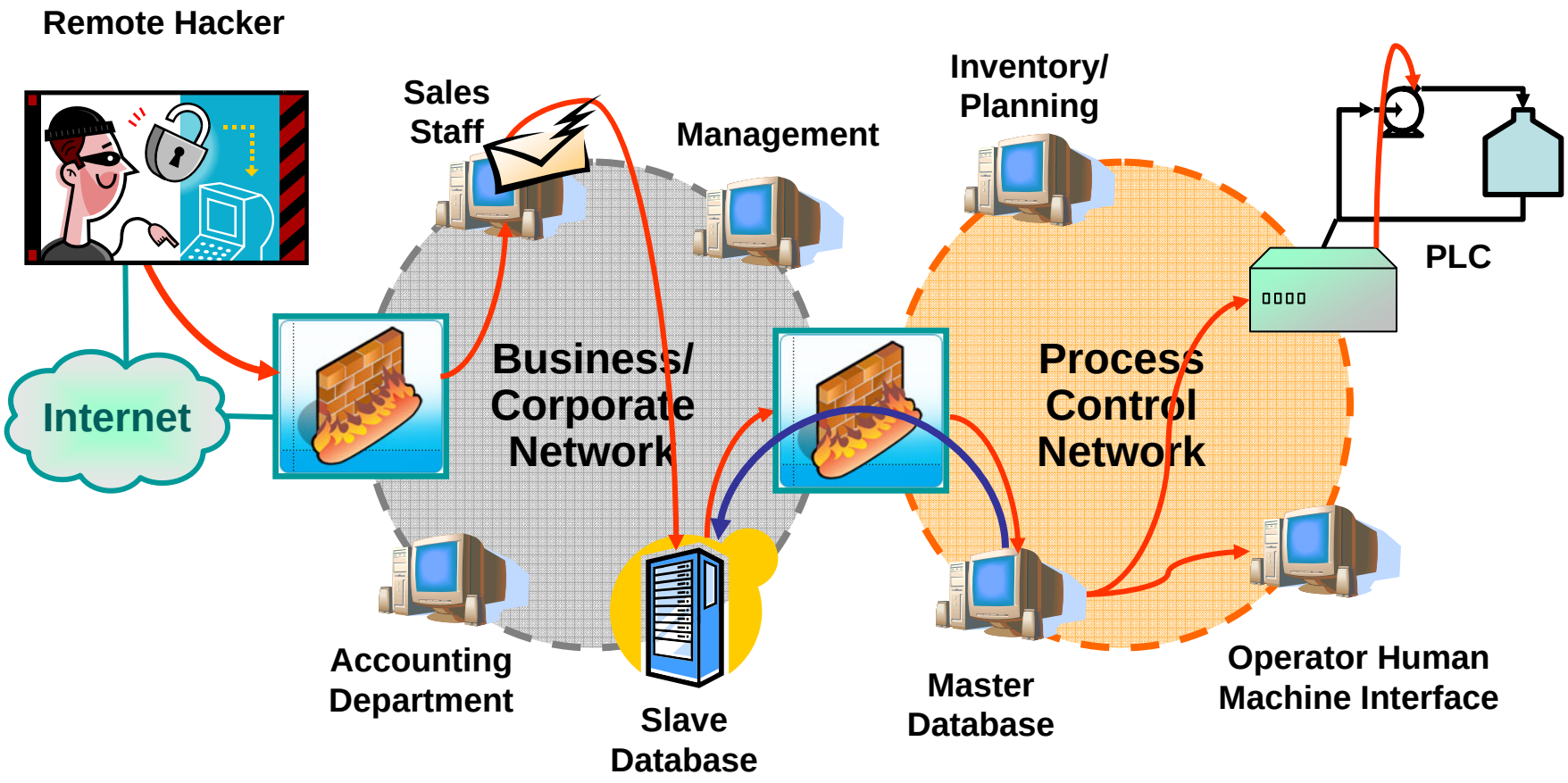
Homeland Security



Vulnerabilities of System in Video

- Clear text communications
- Network switch configuration flaws
- Dynamic ARP tables
- Poorly defined firewall policy
- IDS configured poorly, unusable
- Poor application coding practices
- Improper application and service privileges
- No anti-virus software

Attack Process Demonstration



Homeland Security

Common Perceptions

IT's View of Control Systems

- They do not comply or cooperate
- Their systems are not secure
- They are not in compliance with corporate standards
- They resist change
- Engineering sometimes viewed as future point of attack

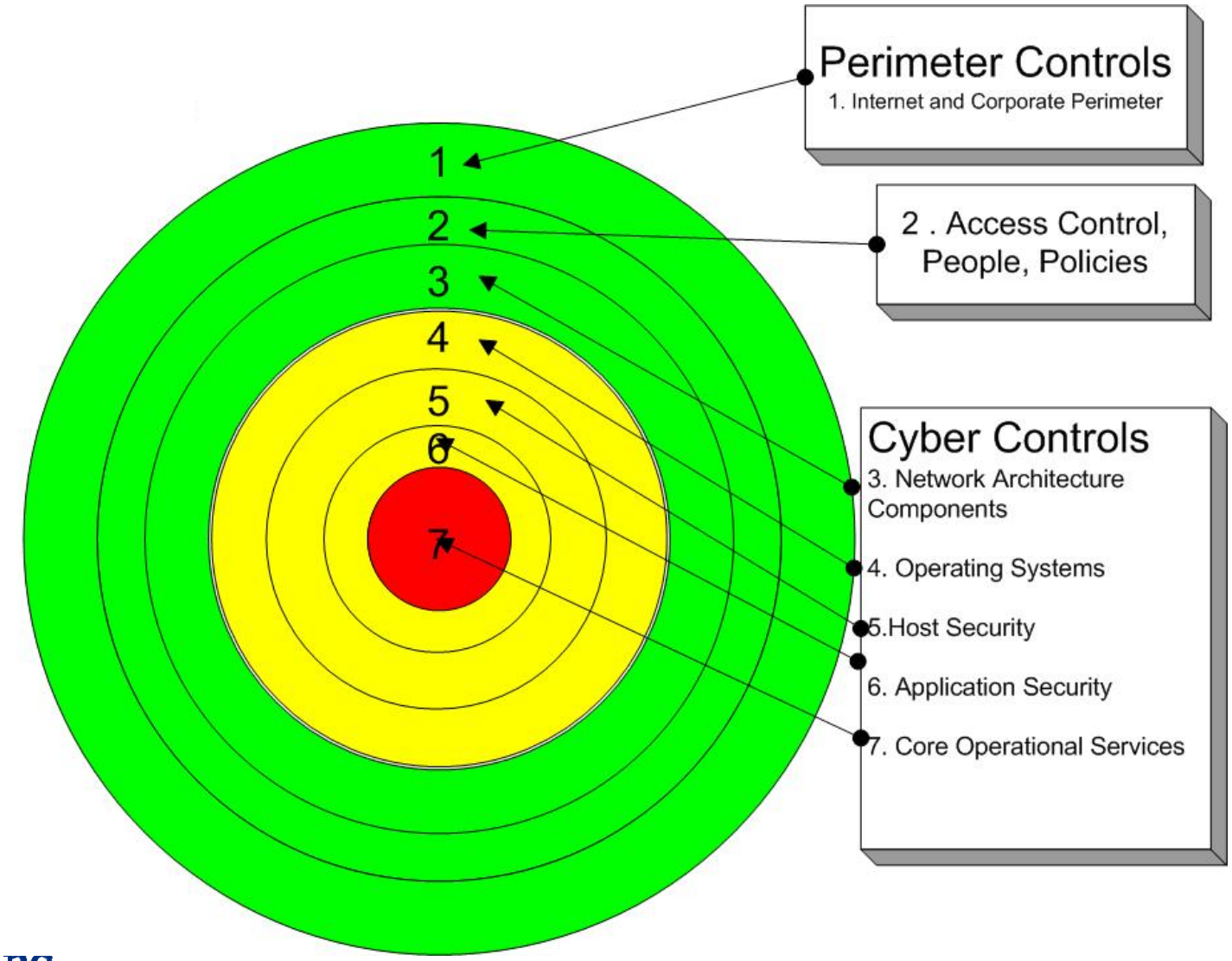
Control Systems View of IT

- They do not understand the constraints of operations
- They insist on measures that will adversely affect plant operations
- Engineers believe connecting the control system to the corporate LAN will increase the risk to operations

To secure the entire network (process control and corporate), we need to work together. Realize the importance of each network and strive for security and reliability.

Homeland Security

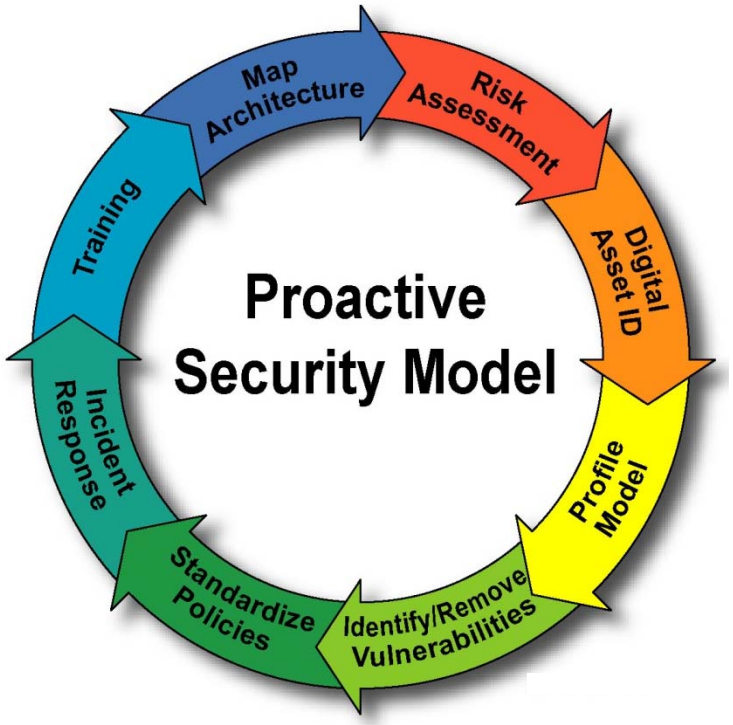
Defense-in-Depth Security



Homeland Security

Security Is A Process, Not A Product

- *Work closely with vendors and integrators to ensure security is a priority.*
- *Stay current on threats and vulnerabilities to control system environment.*
- *Get involved! Standards committees and working groups are looking for your input.*



Homeland Security

CSSP Mission and Objectives

To strengthen the control system security posture by coordinating across government, private sector and international organizations to reduce the risk

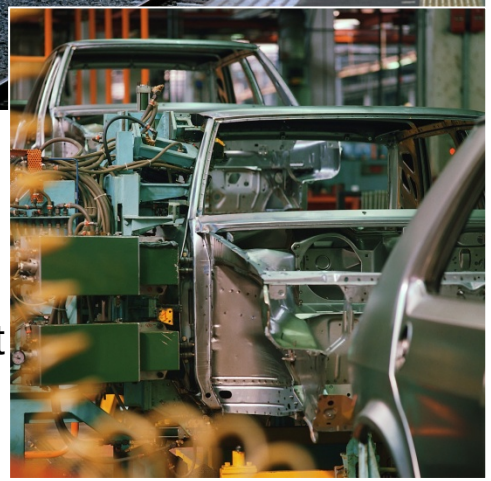
- *Build a culture of reliability, security and resilience*
- *Demonstrate value*
- *Address cross sector security interdependencies*
- *Provide thought leadership*

Homeland Security

18 Critical Infrastructure Sectors

Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure into the following 17 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water



"Critical Manufacturing" was announced as the 18th sector in April 2008

Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system.

Homeland Security

Cross Sector Interdependencies

- *Control systems security is not sector specific*
- *Connectivity crosses geographic boundaries*
- *Sectors are not operationally isolated*

Homeland Security

Vulnerability Analysis
Information Sharing

- Control System Vulnerability reports may be submitted via US-CERT Web Site and entered into National Vulnerability Database (NVD)
- CSSP Web site 'Vulnerability Notes'
  - 14 vulnerability Notes published between May 2006 – February 2008
  - Vulnerabilities patched by vendors
  - CSSC analysis shared across all sectors through products and trainings
- PCII is an information-protection tool that facilitates private sector information sharing with the government

Homeland Security

Scenario Development
Advance Vulnerability Discovery

- *Identifying cyber attacks capable of achieving physical damage*
- *Combining cyber vulnerabilities with specific tactics, techniques & procedures to achieve maximum consequence*
- *Requires industry experience to identify control system risks*

Homeland Security

Briefings & Training

- Web Based Training
  - Cyber Security for Control Systems Engineers & Operators
  - OPSEC for Control Systems
- Instructor Led Courses
  - Cyber Security Who Needs It?
  - Control Systems Security for Managers
  - Solutions for Process Control Security
  - Introduction to Control Systems Security
    For the IT Professional
  - Intermediate Control Systems Security
  - Cyber Security Advanced Training and Workshop

Homeland Security

Risk Reduction Products
Self-Assessment Tool – CS²SAT

- Based on industry standards
- Capability:
  - Creates baseline security posture
  - Provides recommended solutions to improve security posture
  - Standards specific reports (e.g. NERC CIP, DOD 8500.2)
- Availability:
  - To industry through licensed distributors (fee based)
  - To federal government through DHS (free)

Homeland Security

Risk Reduction Products

Cyber Security Procurement Language for Control Systems

Building Security into Control Systems

Provides sample or recommended language for control systems security requirements

- New SCADA / control systems
- Legacy systems
- Maintenance contracts

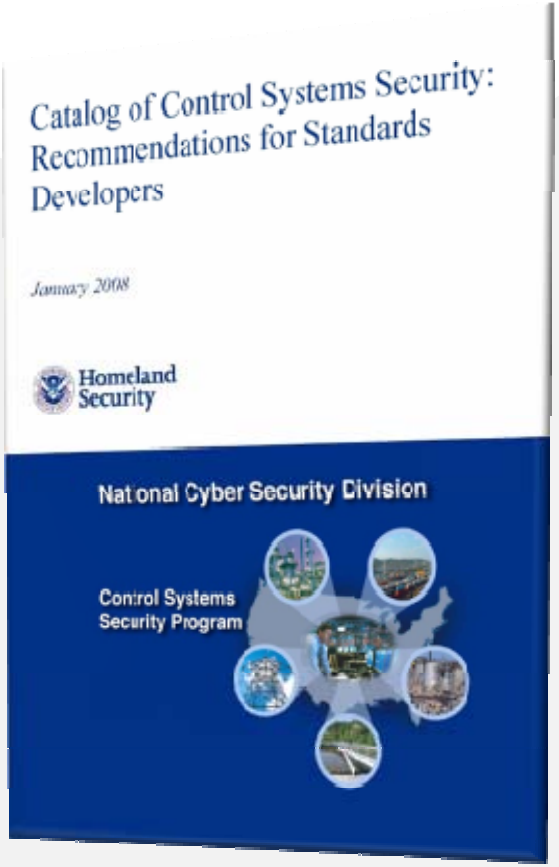
Homeland Security

Risk Reduction Products

Catalog of Control Systems Security: Recommendations for Standards Developers

Supporting Standards Development

- *Provide guidance for cyber security requirements specific to control systems*
- *Enable a common security language across all industry sectors (harmonization of standards)*
- *Support standards bodies and industry associations to implement sound security practices in current standards*



Homeland Security

Develop Partnerships – Industry

Control System Cyber Security Vendor's Forum

Develop Partnerships – Public
Process Control Systems Forum (PCSF)

- ***Mission: To accelerate the design, development, & deployment of more secure control & legacy systems***
  - Participants include national & international stakeholders from government, academia, industry users, owner/operators, systems integrators, & the vendor community
  - For more information: www.pcsforum.org

August 25-28, 2008
LaJolla CA

Homeland Security

Cyber Security is a Shared Responsibility

- Report cyber incidents & vulnerabilities at www.us-cert.gov, soc@us-cert.gov, 703-235-5110, or 888-282-0870
- Sign up for cyber alerts at www.us-cert.gov
- Learn more about CSSP at www.us-cert.gov/control_systems or email: CSSP@dhs.gov

- Contact information:
  - National Cyber Security Division
  - Seán P. McGurk, Director – Control Systems Security Program
  - Sean.McGurk@dhs.gov

Homeland Security

SIEMENS

Bio for Todd Stauffer, Siemens

- PCS 7 Marketing Manager
- SE&A Liaison to PCSF (Process Control Security Forum) Vendor Forum
- Leading Security Assessment of PCS 7 by the Department of Homeland Security at the Idaho National Laboratory
- Siemens Marketing Representative to the ISA Security Compliance Institute (ISCI)

SIEMENS

DHS Control System Security Center
Cyber Security Assessment of PCS 7

PCS 7 is being assessed for cyber vulnerabilities at the Control System Security Center.

Part of: Department of Homeland Security (DHS)
National Cyber Security Division (NCSD)
Control Systems Security Program (CSSP)

The CSSP:

- Helps industry and government improve the security of the control systems used in US critical infrastructure
  - (e.g. chemical, oil & gas, electric utilities, water & wastewater…)
- Mission is assessment of control systems to identify vulnerabilities that could put critical infrastructures at risk from a cyber attack
- Once vulnerabilities are identified, mitigation strategies are developed to enhance control system security

- Significant investment by both DHS and Siemens

SIEMENS

Motivation - Why would Siemens ask DHS to perform a security assessment on PCS 7 ?

- Validate & Improve PCS 7 Security Concept
- Leverage CSSP's unique skillsets (eg. Aurora)
- Help us enhance the security posture of PCS 7 control systems
- Knowledge transfer for members of PCS 7 Security Lab
- Expand DHS / INL body of knowledge for protecting control systems that control US Critical Infrastructure
- Help our customers comply with new government regulations (eg. DHS's Chemical Facility Antiterrorism standard)
- No official recognized body for certification at this time (ISCI will help change this)

SIEMENS

Siemens has a team within System Test that is dedicated to Industrial Security – PCS 7 Security Lab

- SIMATIC PCS 7/ WinCC security test system
  - Tests MS security patches for compatibility
  - Test Virus Scanner releases
  - Definition / Testing of Approved Architectures
- Wrote PCS 7 Security Recommendations Document
- Ensures fast response to new security threats
- Performs intense Forefront testing to proactively identify vulnerabilities and minimize risks (results are fedback to R&D)

Security Lab involvement in CSSP testing helps improve knowledge of attacker methods

ISA Security Compliance Institute (ISCI)

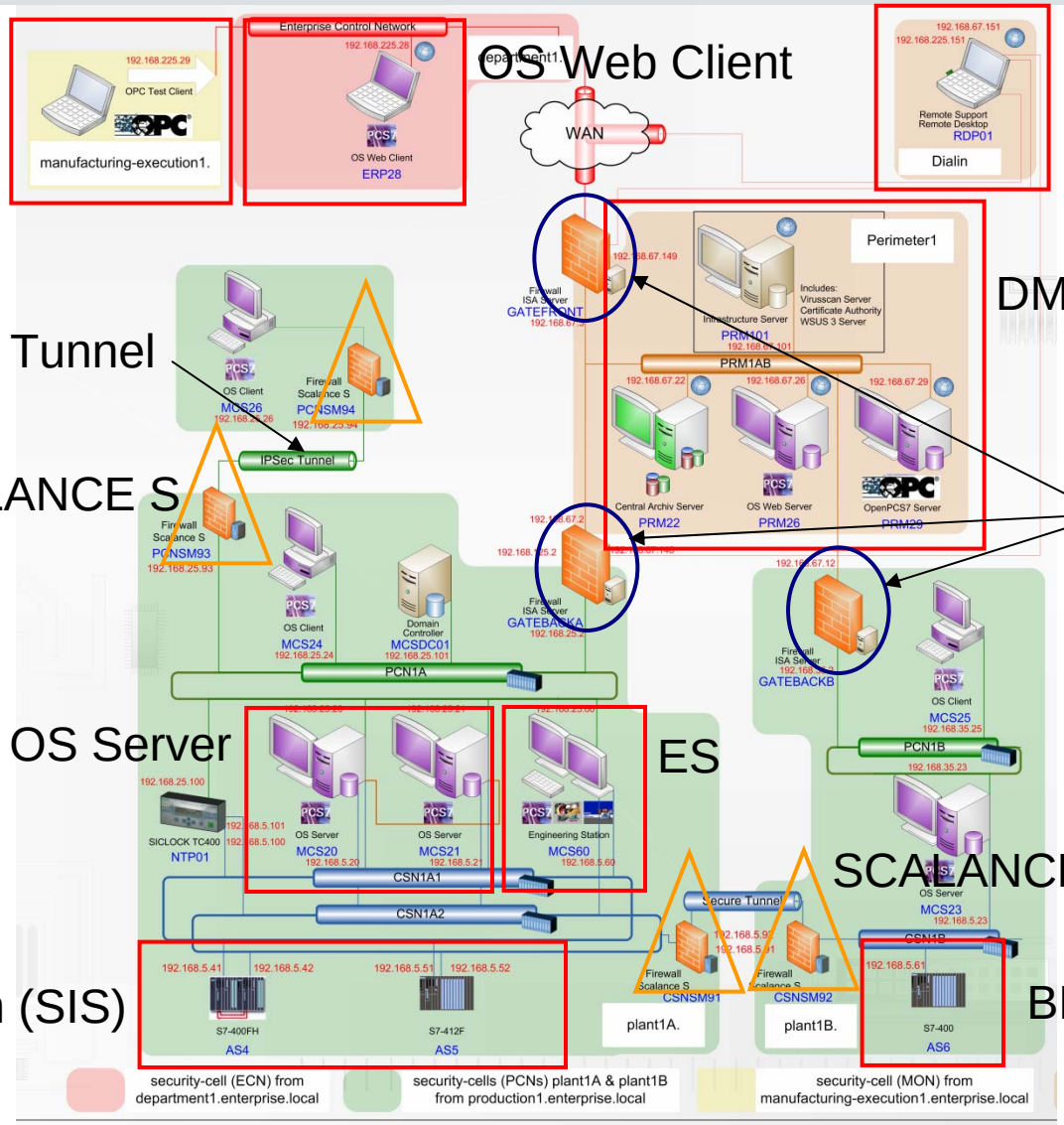
- Goal: Establish a collaborative industry-wide program that improves the security of our Nation's Critical Infrastructure by providing a Control Environment that is….
  - **Safer**
  - **More Reliable**
  - **Intrinsically Secure**

- ***To create a single recognizable body for Security Compliance - just like "TUV" is for Safety...***

ISASecure

SIEMENS

Test Architecture was derived based on what is described in the PCS 7 Security Manual



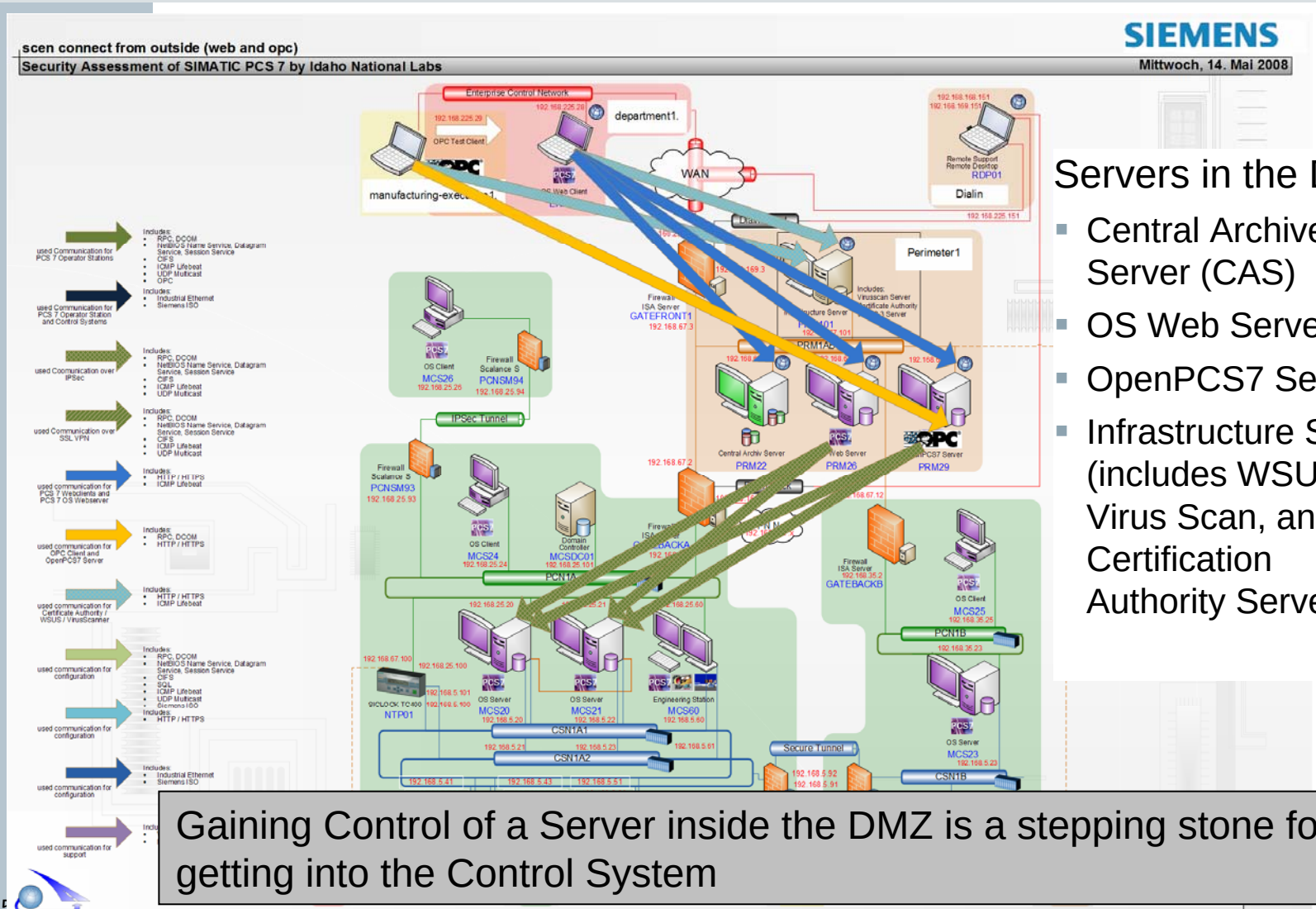
SIEMENS

Targets of Evaluation (TOE) were selected to stress key parts of the system and to leverage CSSP's expertise

- Specific targets have been selected which are key functions of PCS 7
- Test Plan Objectives cover steps that might be potential goals of a real attacker in order to exploit the control system and cause damage to equipment, service, or users

TOE Priority Number	TOE Description
1	Assess Vulnerabilities in DMZ Servers
2	Unauthorized Access to the Engineering Station
3	Unauthorized Access to Operators Workstation
4	Assess VPN Communications Security
5	Perform Protocol Fuzzing to Find Vulnerabilities
6	Unauthorized Configuration Database Access
7	Unauthorized Access to the Administrative Server

TOE 1: Assess Vulnerability of DMZ Servers – Goal is for attacker to gain control of a server inside the DMZ



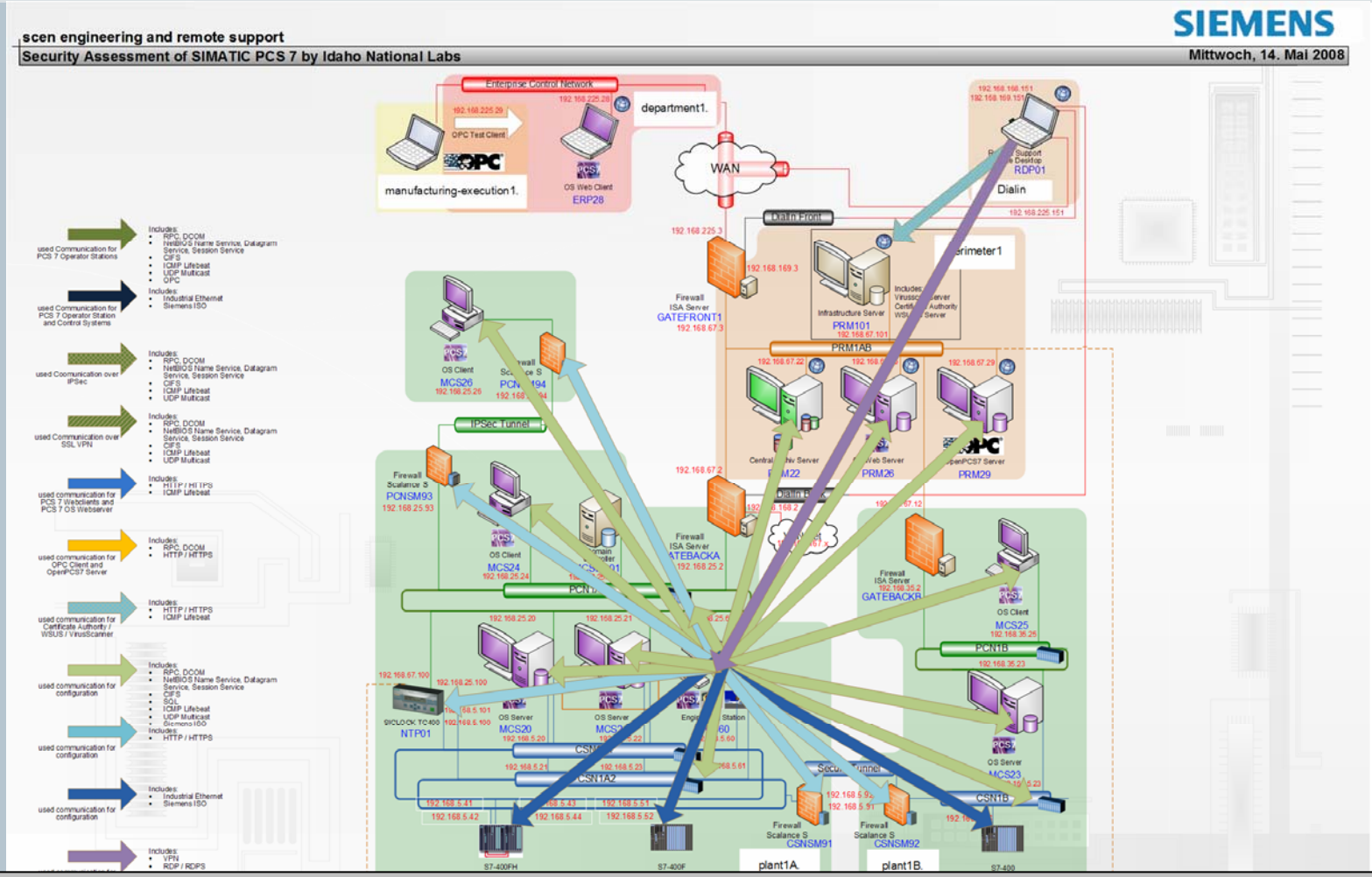
Servers in the DMZ

- Central Archive Server (CAS)
- OS Web Server
- OpenPCS7 Server
- Infrastructure Server (includes WSUS, Virus Scan, and Certification Authority Servers)

Gaining Control of a Server inside the DMZ is a stepping stone for getting into the Control System

SIEMENS

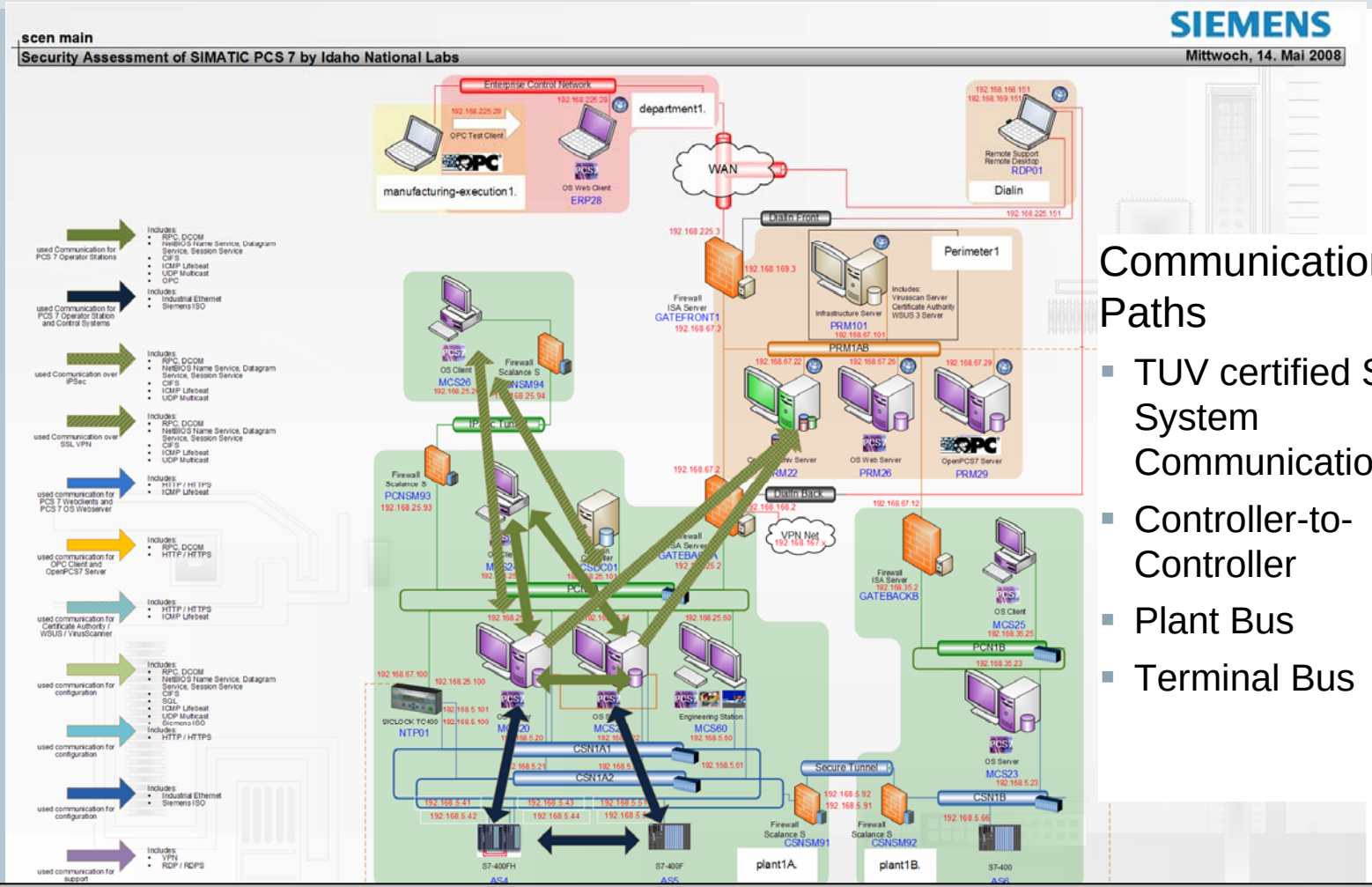
TOE 2: Unauthorized Access to the Engineering Station – Goal is for attacker to gain interactive login to PCS 7 ES



The ES is used for development, maintenance and troubleshooting of the Basic Process Control System (BPCS) and for the Process Safety System (SIS).

SIEMENS

TOE 5: Perform Protocol Fuzzing to Find Vulnerabilities – Goal is to cause a communication disruption / overload



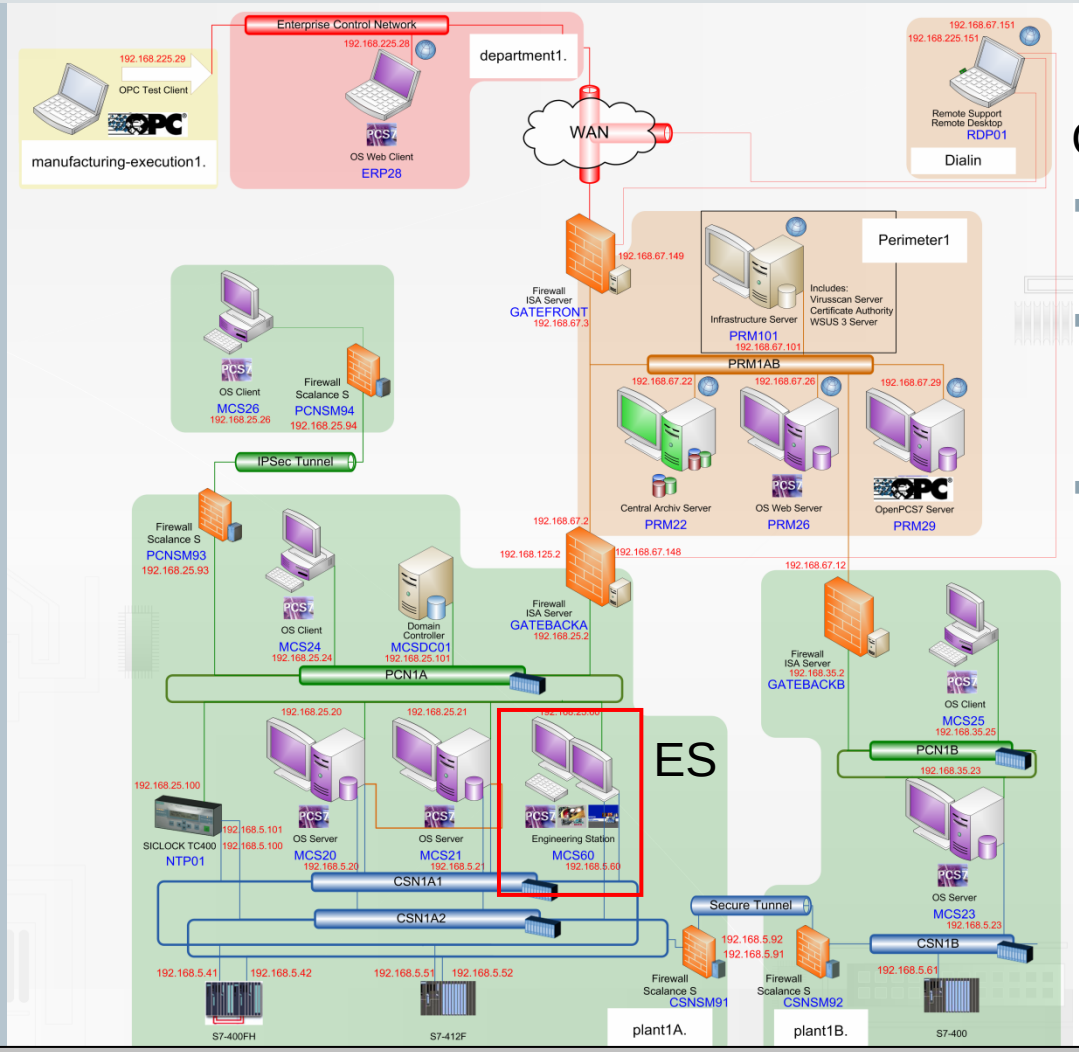
Communication Paths

- TUV certified Safety System Communication
- Controller-to-Controller
- Plant Bus
- Terminal Bus

Creating a Communication Overload Scenario is a common hacker method for attempting to take down a control system

SIEMENS

TOE 6: Unauthorized Configuration Database Access – Goal is to modify configuration from the PCS 7 ES



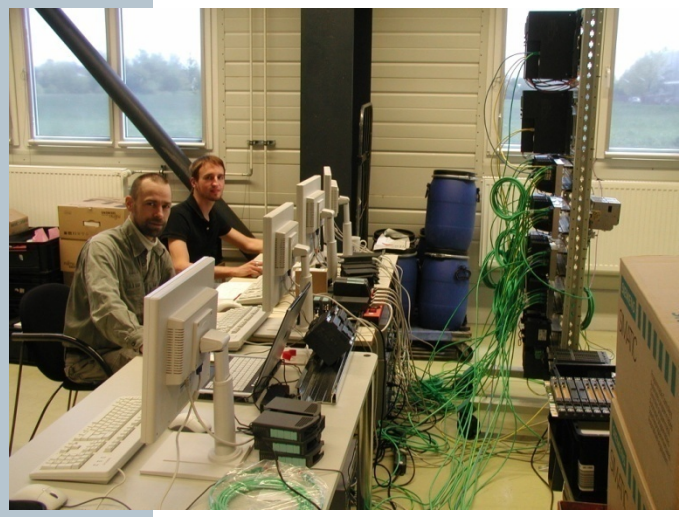
Objectives

- Infiltrate PCS 7 ES and modify configuration
- Access / modify control system configuration without being detected
- Compromise controller configurations in BPCS (AS6) and SIS (AS4 – AS5)

Hacker modifying a controller configuration would be a significant security breach

SIEMENS

Timeline for CSSP's Security Testing of PCS 7



- March (2008) – Face to-face Planning Meeting in KHE
- April / May – Procure Hardware and Stage test system
- May – Ship Test System from Germany to Idaho Falls
- June – Setup Test System at Idaho Falls
- July 1st – Begin Testing
- September 15th – Complete Testing
- Mid Sept – Mid Nov – Review & Document results
- November 15th – Deliver Final report to Siemens
- May 15th (2009) – Siemens After Action Report Due

SIEMENS

Lessons Learned

- We should make it easier for users to setup their system per the recommendations in the security manual
- PCS 7 Product documentation is inconsistent in places (Security Manual should override)
- Engineering System has the keys to the kingdom – Protect it !
- Integrated Safety System has extra security features
  - Passwords
  - CRC checking
  - Controller Switch prevents unplanned downloads
- Establishing and following a workflow process (including Change Management) is important

SIEMENS

Q&A

Thanks for Attending !