

# SCADA Security

Oregon InfraGard Members Alliance

World Forestry Center

March 17<sup>th</sup> 2005

# Introduction

**Hello, I'm Patrick Miller...**

- Senior Information Security Consultant and Advisor
- 18+ years experience in general IT and Telecom
- 7+ years experience in Information Security
- 5+ years in the Energy Industry
- Industry certified
  - **CISSP** (Certified Information Systems Security Professional)
  - **ISSAP** (Information Systems Security Architecture Professional)
  - **SSCP** (Systems Security Certified Practitioner)
  - **IAM** (NSA InfoSec Assessment Methodologies)
  - **TCP** (Tripwire Certified Professional)
  - *Etc...* (Miscellaneous Information Technology certifications)

# Overview



- **SCADA Security: Past, Present and Future**
- **Regulatory Climate: “Perfect Storm”**
- **Secure SCADA network architectures**
- **Partnerships and participation**



# **SCADA Security**

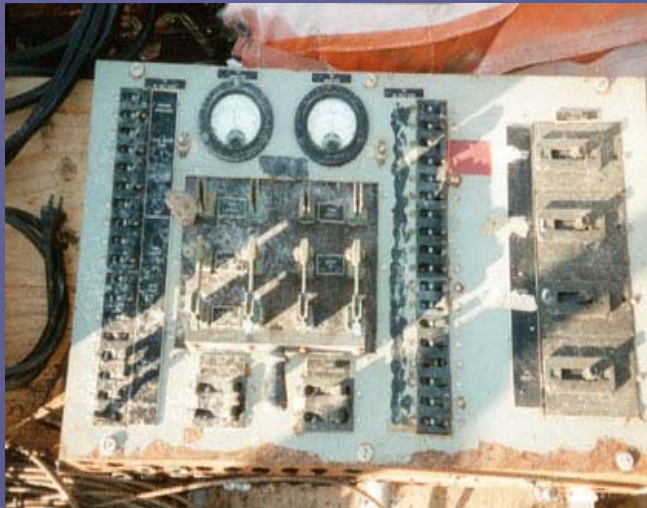
**Past, Present and Future**

# SCADA Security - History

- Legacy systems built for reliability and performance -- *not security*
- Terrorism wasn't a concern
- No Internet...
  - No Internet-connected SCADA
  - SCADA was often air-gapped
  - No SCADA information available on the Internet
- Obscure systems with obscure documentation



# SCADA Security - History



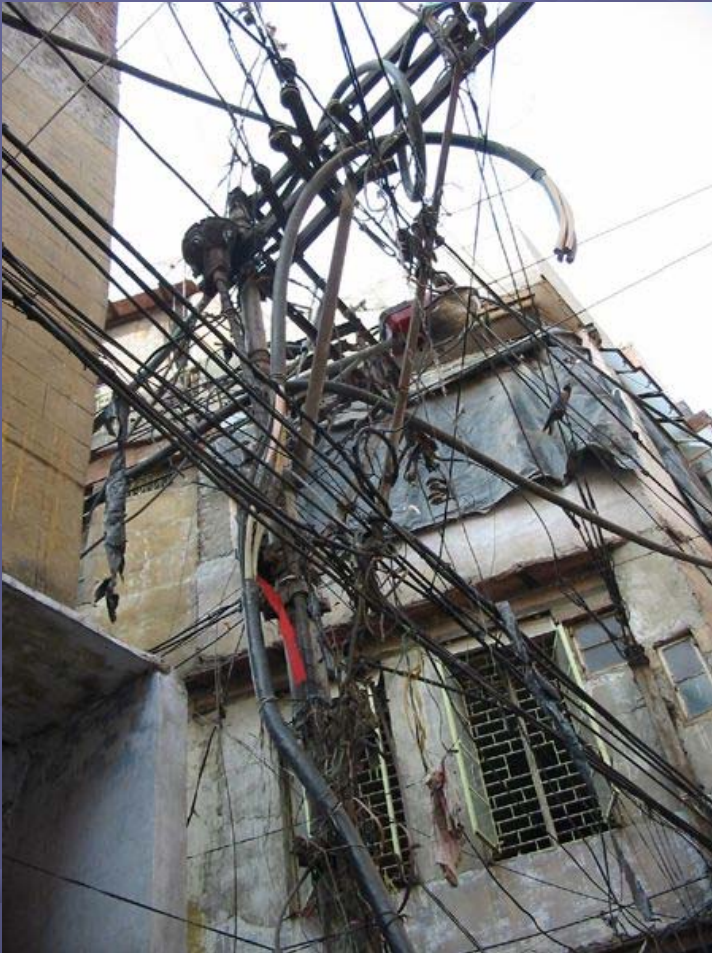
- Minimal interoperability with proprietary protocols
- Enormous amount of software customization
- Patching was uncommon and painful, if even done
- SCADA hacks were rare; often required insider knowledge/expertise

# SCADA Security – Today

- Systems are still built for reliability and performance -- *not security*
- Terrorism is a **necessary** consideration
- The Internet...
  - SCADA networks are increasingly more interconnected
  - Large amounts of information very easy to obtain in a short amount of time – in multiple languages
- No more “Obscurity Factor”



# SCADA Security - Today



- More interoperable with public protocols
- General IT security practices still won't work entirely, but a good start
- Less software customization necessary, but still too much
- Patch management is extremely difficult

# SCADA Security – Today's Threats

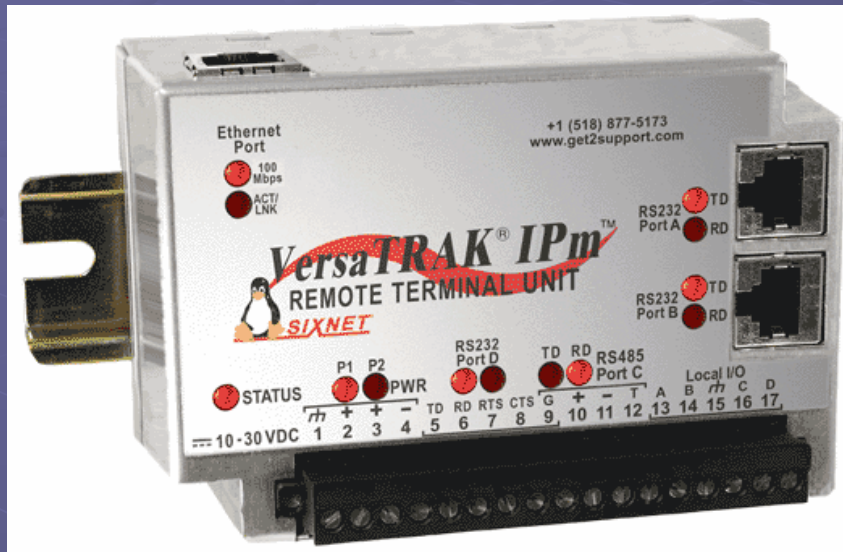
- Coordinated Physical and Cyber attack still considered to be greatest threat...
  - Confusion is not to be underestimated (August 14th)
  - Resource availability and backup/DR
  - Critical spares
  - Interconnectivity points
- Documented Cyber-attack Potentials...
  - External (remote) console access, usually via modem
  - High/low trigger values; Breakers/valves modified
  - Network sniffing and “replay” attacks
  - Many new vectors and tools; ettercap, spyware, etc.
  - Simple “bake-off” faults; NMAP, X-Mas Tree packets

# SCADA Security - Future

- Devices/systems will be built with “baked-in” security features; *expect growing pains in the process...*
- Terrorism will probably still exist; *may be worse*
- The Internet (or similar) will probably still exist



# SCADA Security - Future



- SCADA obscurity will be uncommon
- Higher degree of interoperability
- Minimal software customization
- *Easier* patching
- *Maybe* even open systems/platforms



# **SCADA Security**

## **Regulatory Climate**

# Regulatory Climate

- NERC UAS1200/CIPS
- Sarbanes-Oxley
- DHS Critical Infrastructure Protection (HSPD-7/CIPA)
- DHS CEII (6cfr Part 29)
- FERC Standard Market Design (SMD) still exists
- Several unfavorable GAO reports on SCADA

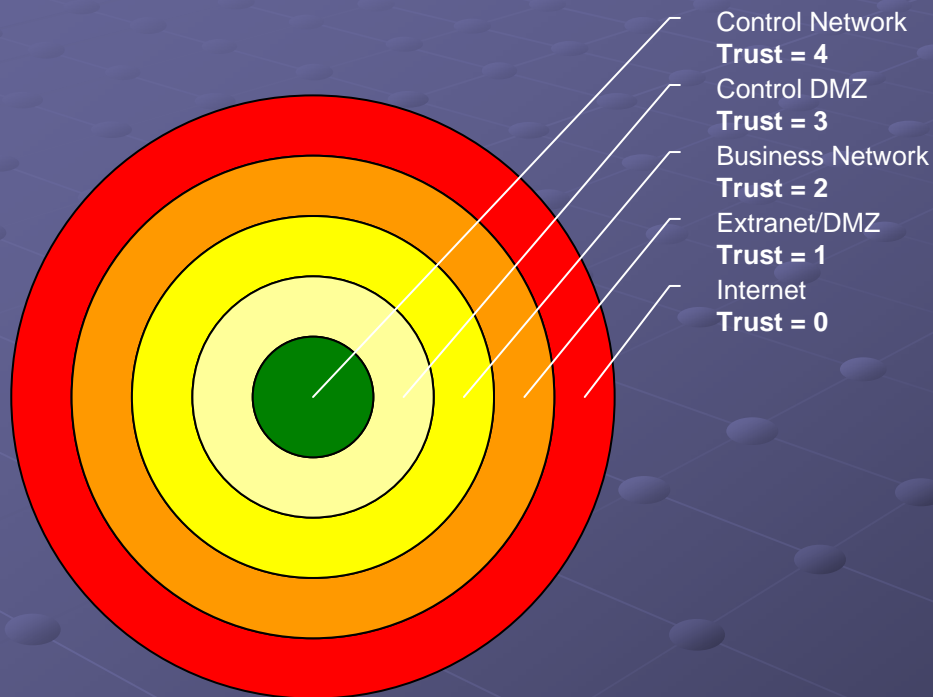




# **SCADA Security**

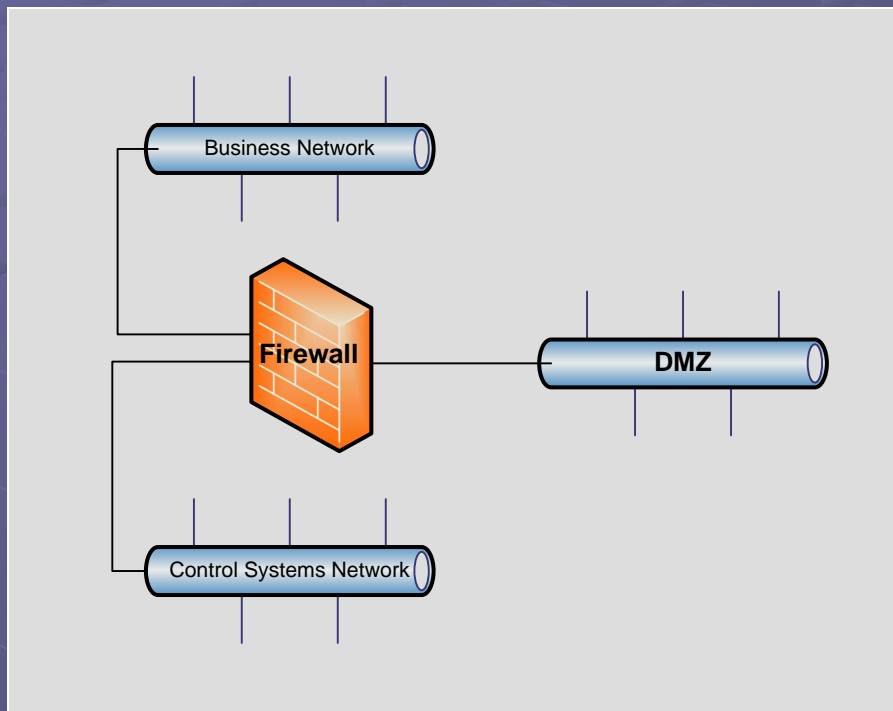
## **Secure SCADA Architectures**

# Trusted Zones

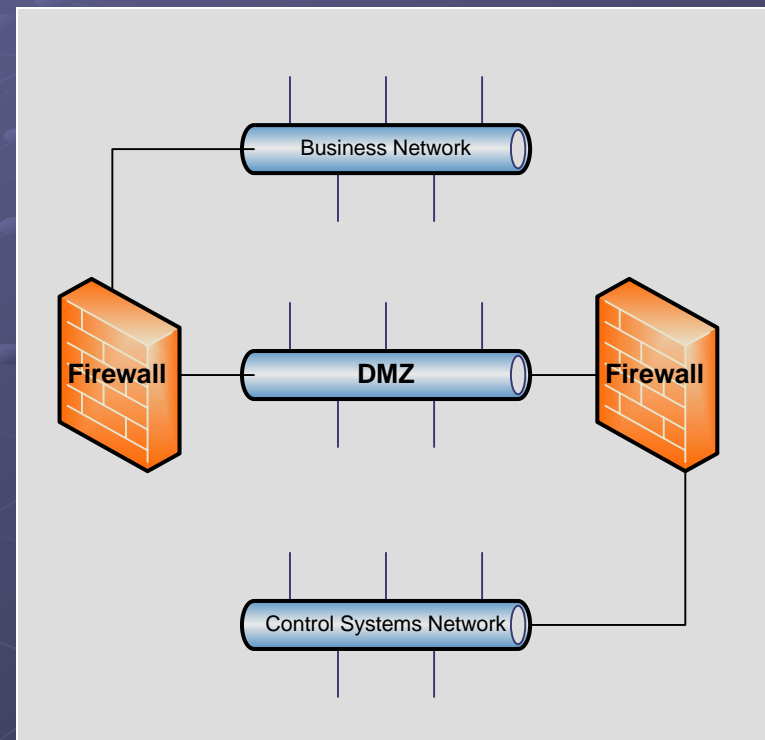


- Establish trust levels for each logical network
- Separate each network boundary with a firewall
- Employ a DMZ at each network boundary
- Establish restrictions for data transfer between zones
- Stage trusted data
- Mandate with policy

# DMZ Options



Single Firewall with DMZ port(s)



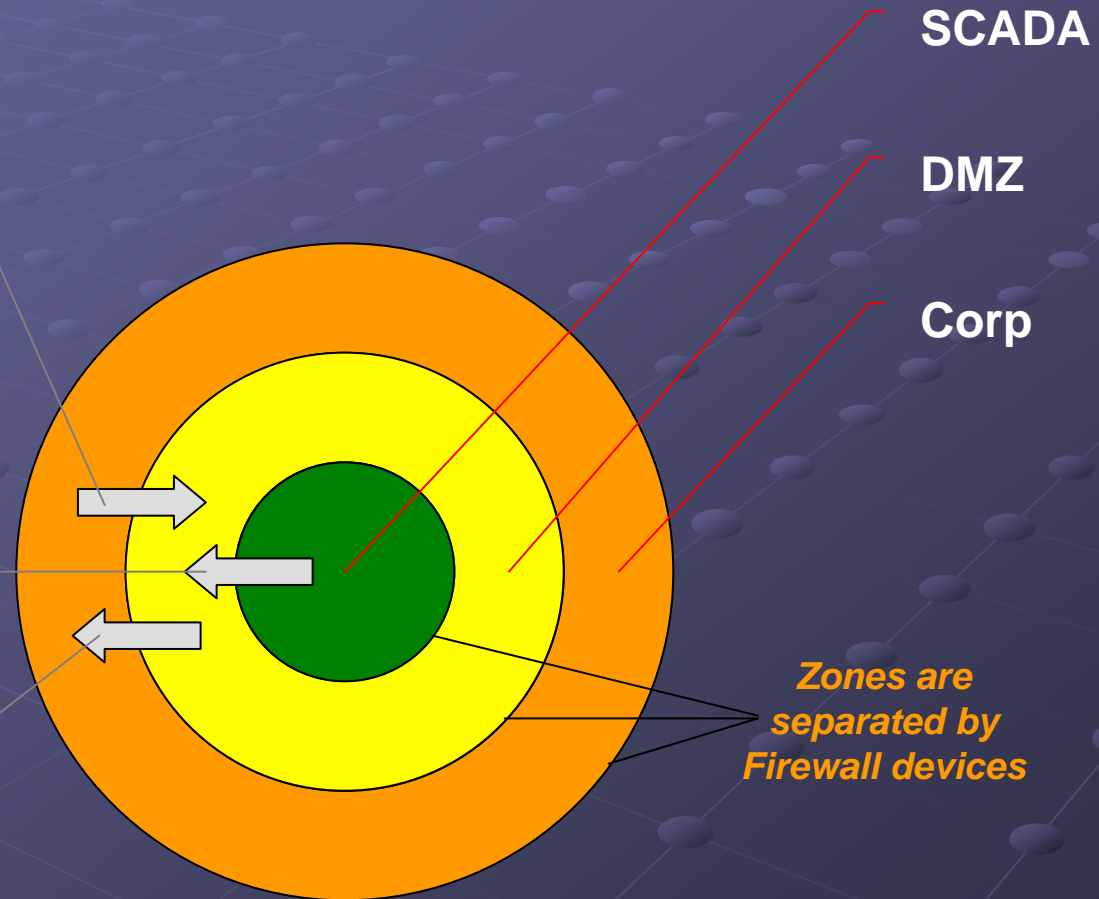
Dual Firewall

# Data Flow

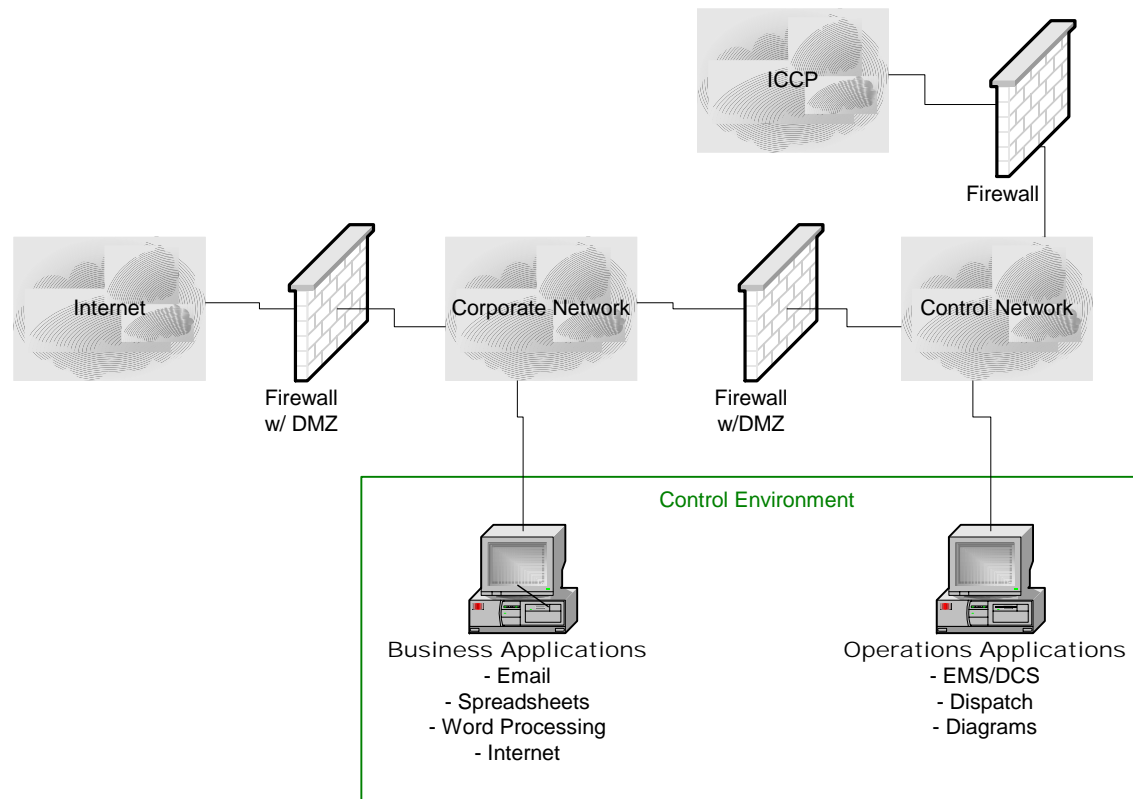
Have Corporate network retrieve all data from DMZ

Push all data from SCADA network to DMZ

Allow DMZ to push data into Corporate network

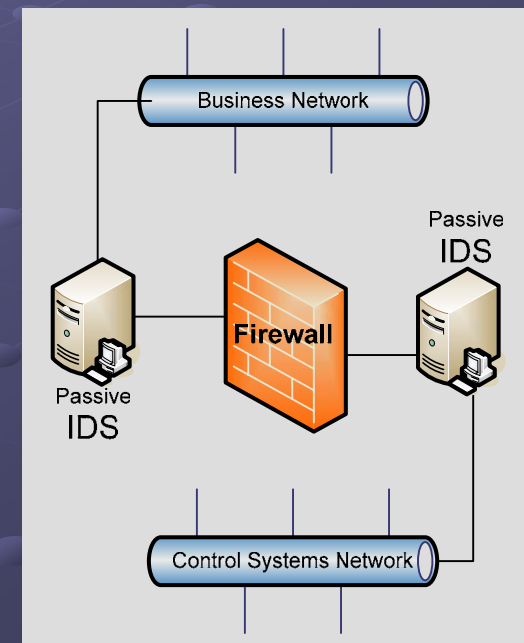


# The Big Picture



# IDS/IPS, Patching and APS

- **IDS (Intrusion Detection System):** reactive, expensive, noisy and difficult to manage
- **IPS (Intrusion Prevention System):** proactive, but may cause outages depending on implementation; expensive
- **Rigorous patch management** is the most proactive, but rarely feasible on legacy systems
- **APS (Aware Person System):** aware people with quality tools are the best defense of all...



# Don't Forget...

## Where technically feasible:

- Strong (multi-factor) authentication
- Harden systems (ports, protocols, etc)
- Encrypted sessions
- Clear policy and process language
- Incident handling
- Backup/recovery
- Risk and vulnerability assessment
- Security awareness and training



# **SCADA Security**

**Partnerships and  
Participation**

# Get Involved !!

## ● Industry conferences

- NERC, EEI, ISA, UTC, KEMA, CBI, D&T World, etc...

## ● NERC Committees and Working Groups (CIPC, CSSWG, RAWG)

- <http://www.nerc.com>

## ● IEC Technical Committee 57 Working Groups 15 and 16

- <http://www.iec.ch/>

## ● Process Control Systems Security Requirements Forum (PCSRF)

- <http://www.isd.mel.nist.gov/projects/processcontrol/>

## ● Process Control Systems Forum (PCSF)

- <http://www.pcsforum.org>

## ● INEEL National SCADA Test Bed

- <http://csstc.inel.gov/index.cfm?fuseaction=home.faq>

## ● Sandia Center for SCADA Security

- [http://www.sandia.gov/scada/National\\_Testbed.htm](http://www.sandia.gov/scada/National_Testbed.htm)

## ● Power Engineering Society

- <http://www.ieee.org/organizations/society/power/>

# Questions?

Patrick Miller, CISSP-ISSAP SSCP IAM TCP

[patrick.miller@pacificorp.com](mailto:patrick.miller@pacificorp.com)

503.813.7014 (desk)

503.312.0703 (cell)