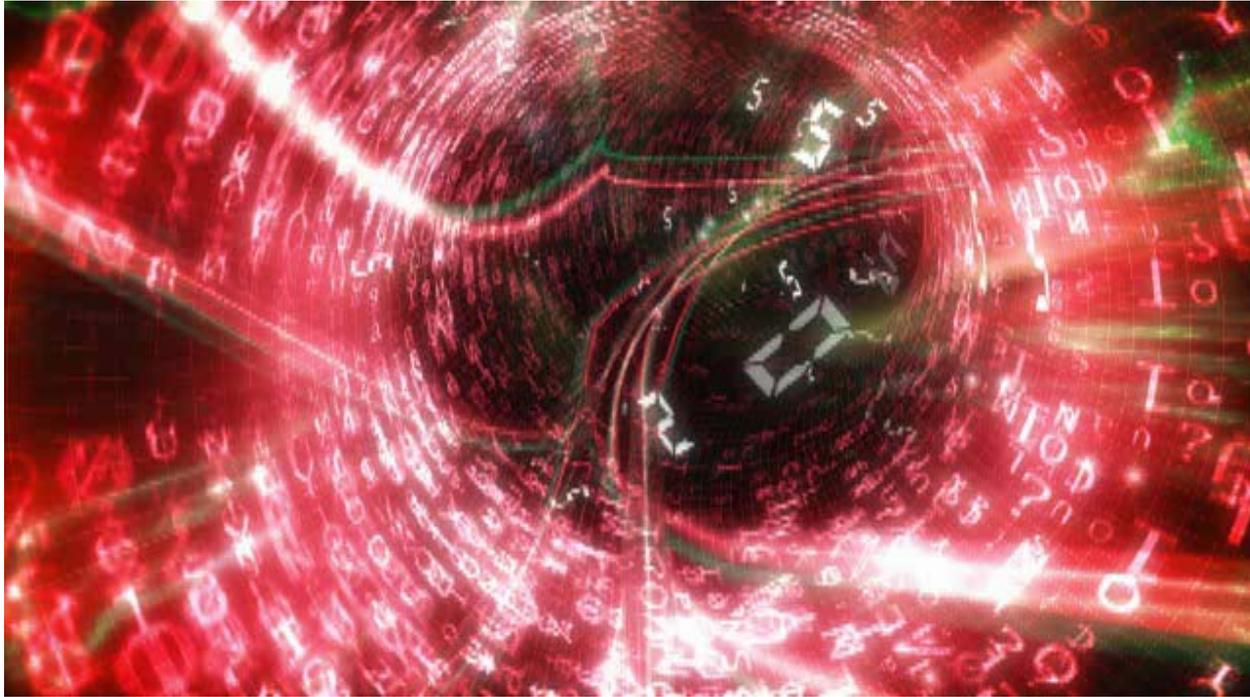


# Elecsys Corporation

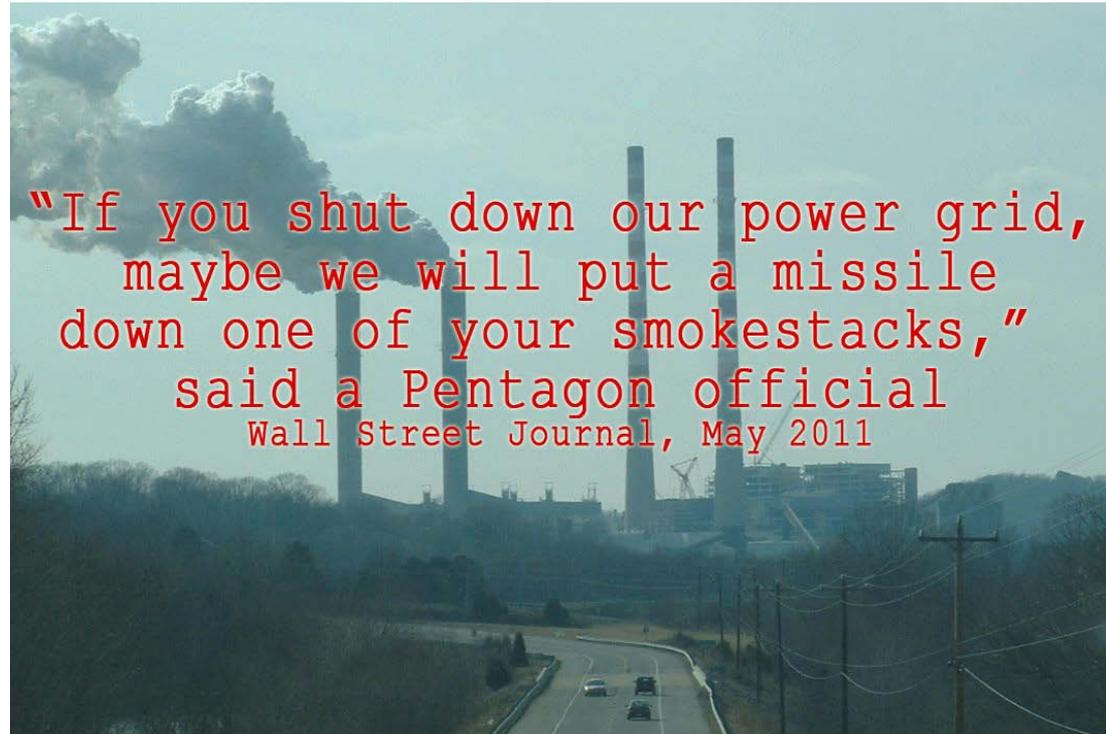


Extending Data Security in Legacy SCADA Systems



# Cyber Warfare

- **Most attacks are unreported**
- **Well known attacks**
  - Stuxnet, Night Dragon
- **Perpetrators**
  - Cyber Terrorists
  - Foreign Governments
  - Activist Groups

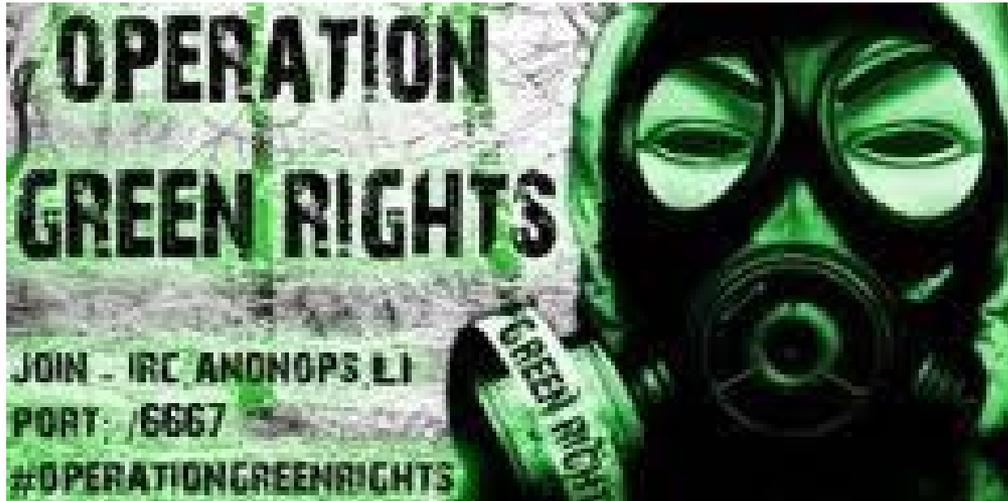


# Cyber Crime

- **Most attacks are unreported**
- **Types of attacks**
  - DDoS
  - Data Theft
- **Perpetrators**
  - Organized Computer Crime “Gangs”
  - Extortionist Hackers
  - Activist Groups



# Cyber Activism



- *We are Anonymous.*
- *We are Legion.*
- *We do not forgive.*
- *We do not forget.*
- *Expect us.*

***Free-thinking citizens of the world:***

***Anonymous' Operation Green Rights calls your attention to an urgent situation in North America perpetuated by the boundless greed of the usual suspects: Exxon Mobil, ConocoPhillips, Canadian Oil Sands Ltd., Imperial Oil, the Royal Bank of Scotland, and many others.***

***<http://anonnews.org/?p=press&a=item&i=1021>, July 12, 2011***

# Common Security Threats to Industrial Data Networks

- **Types of attacks**
  - Denial of Service (DoS, DDoS)
  - Man in the Middle
  - Masquerade and Replay
- **Objectives**
  - Cyber extortion
  - Data theft
  - Publicity and public embarrassment

# Legacy Devices

- There are literally millions of field devices
- Known protocols and common ports are easily found on the internet
- Typically not secure
- Costly to update or replace



# SCADA System Vulnerabilities

<b>Attack Type</b>	<b>Objective/Effect</b>
Denial of Service	Disruption of communication/system shutdown
Trojan or Malware	System takeover, data theft, data corruption, device disabling/corruption
Communication Interception	Data theft, data corruption, espionage

# Security Strategies and Challenges

- **Objectives**

- Protection/availability of data
- Network protection
- Device security
- Mitigation of liabilities
- Regulatory compliance

- **Tasks**

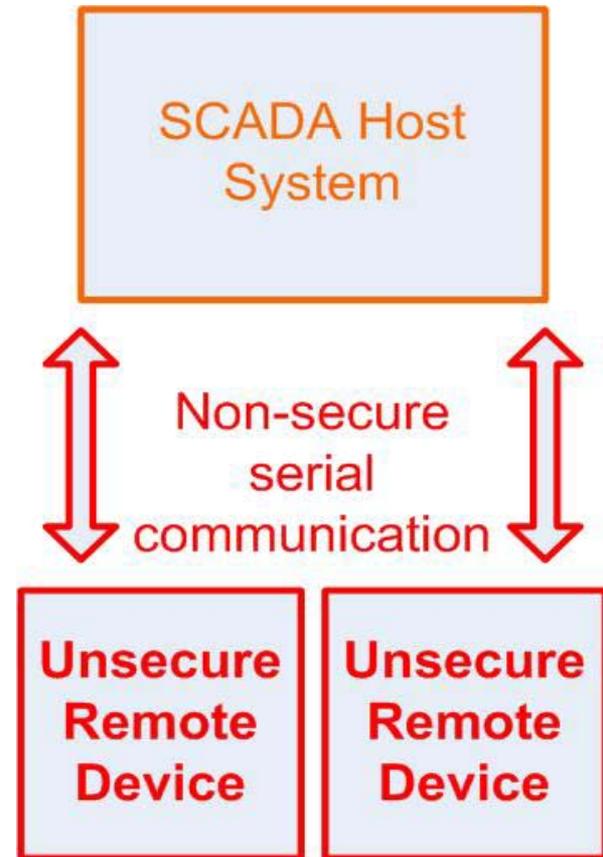
- Threat assessment
- Implementation/training
- Operation and management



# Security Strategies for Remote Systems

- **Invisibility or “Security by Obscurity”**
  - Perception that non-IP communication is invisible to hackers
  - Perception field data and devices are of no interest to hackers

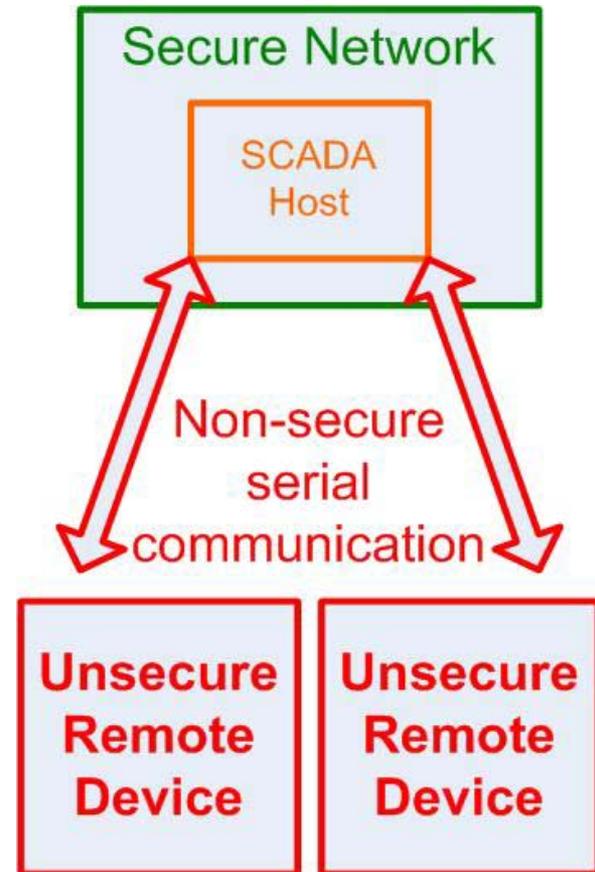
Operational data, host system, and field devices fully exposed to attack.



# Security Strategies for Remote Systems

- **Central Network Secure Zone**
  - SCADA host within secure network
  - Perception that field data and devices secure by invisibility
  - Non-secure communication to host exposes overall network

Host “secured” in network zone, remote systems exposed, network security is questionable.

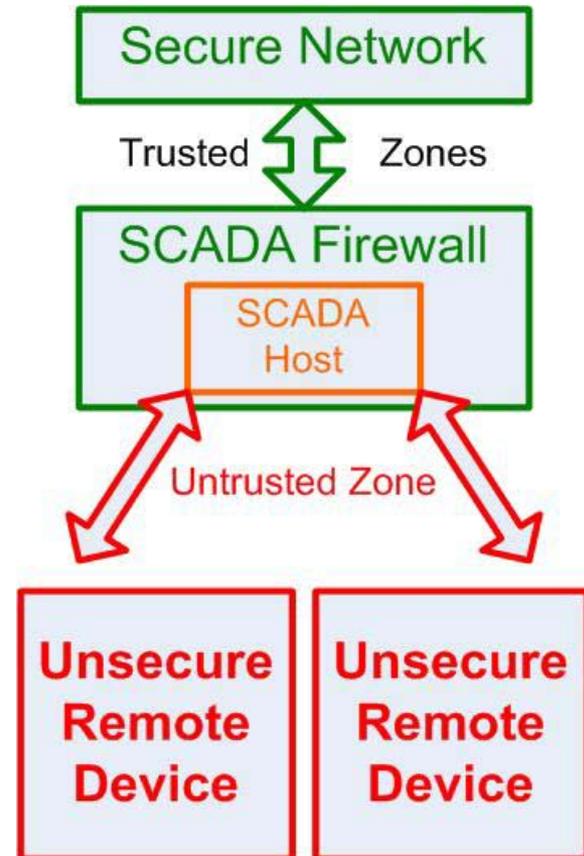


# Security Strategies for Remote Systems

- **SCADA “DMZ”**

- SCADA host isolated via dedicated firewall and router
- Trusted zones can be authenticated
- Dedicated control over SCADA traffic

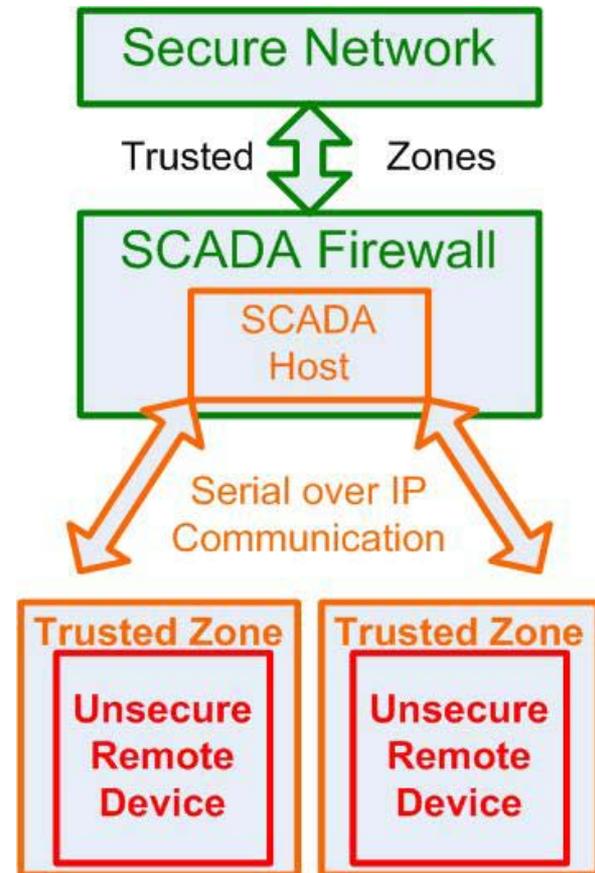
Central network and SCADA network security enhanced, remote data and devices still exposed.



# Security Strategies for Remote Systems

- **Secure “Islands”**
  - Extending “DMZ” strategy to the remote site.
  - Facilitated using IP communication
  - Recognition of remote site vulnerability

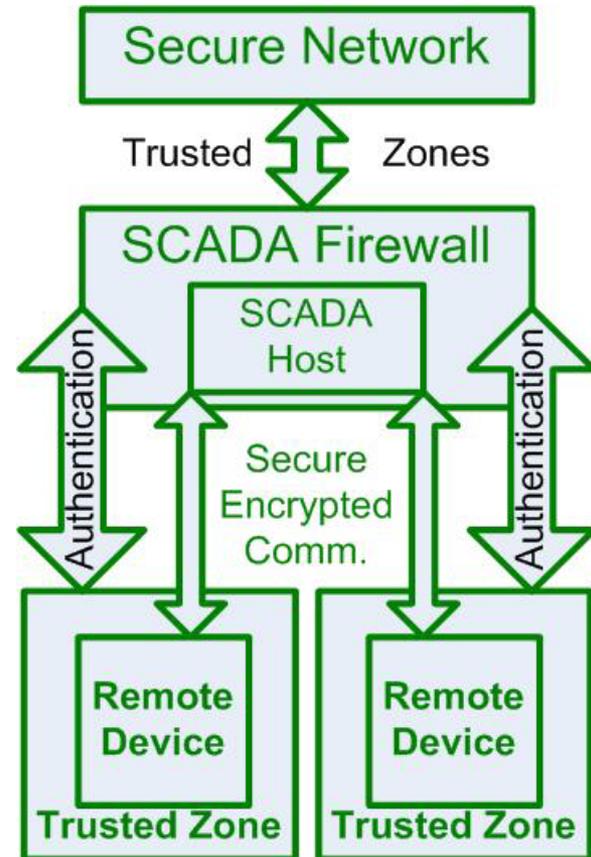
**Extended “Trusted Zone”**. Relies on use of IP based field equipment or firewalling remote sites and using serial to IP conversion.



# Security Strategies for Remote Systems

- **Authentication and Encryption**
  - Complete “Data Security Perimeter Extension”
  - All zones employing device authentication
  - All communication via secure tunnels with encryption

**Facilitates IDS/IPS. Communication fail-over and backdoors at remote sites must be eliminated or secured.**



# Common Concerns

- **Data Availability**

- Network downtime
- Latency
- Serial to IP conversion

- **Network Operations**

- SCADA vs. IT conflicting goals?
- Bandwidth management
- Network administration overhead
- Intrusion Detection

# Tradeoffs

## Strategy

Invisibility/Obscurity

Trusted/Untrusted Zones

DMZ/Secure Zones/Islands

Secure zones with full device authentication and data encryption

Replacing legacy devices

## Advantages

No initial expense.

Does not require major system overhaul, requires less administration

Provides protection for field devices, increases overall network security

Fully encompasses field data devices within the data security perimeter, and secures data transmissions

Most new devices are “IP Ready” for integration into the network

## Disadvantages

Potentially disastrous consequences.

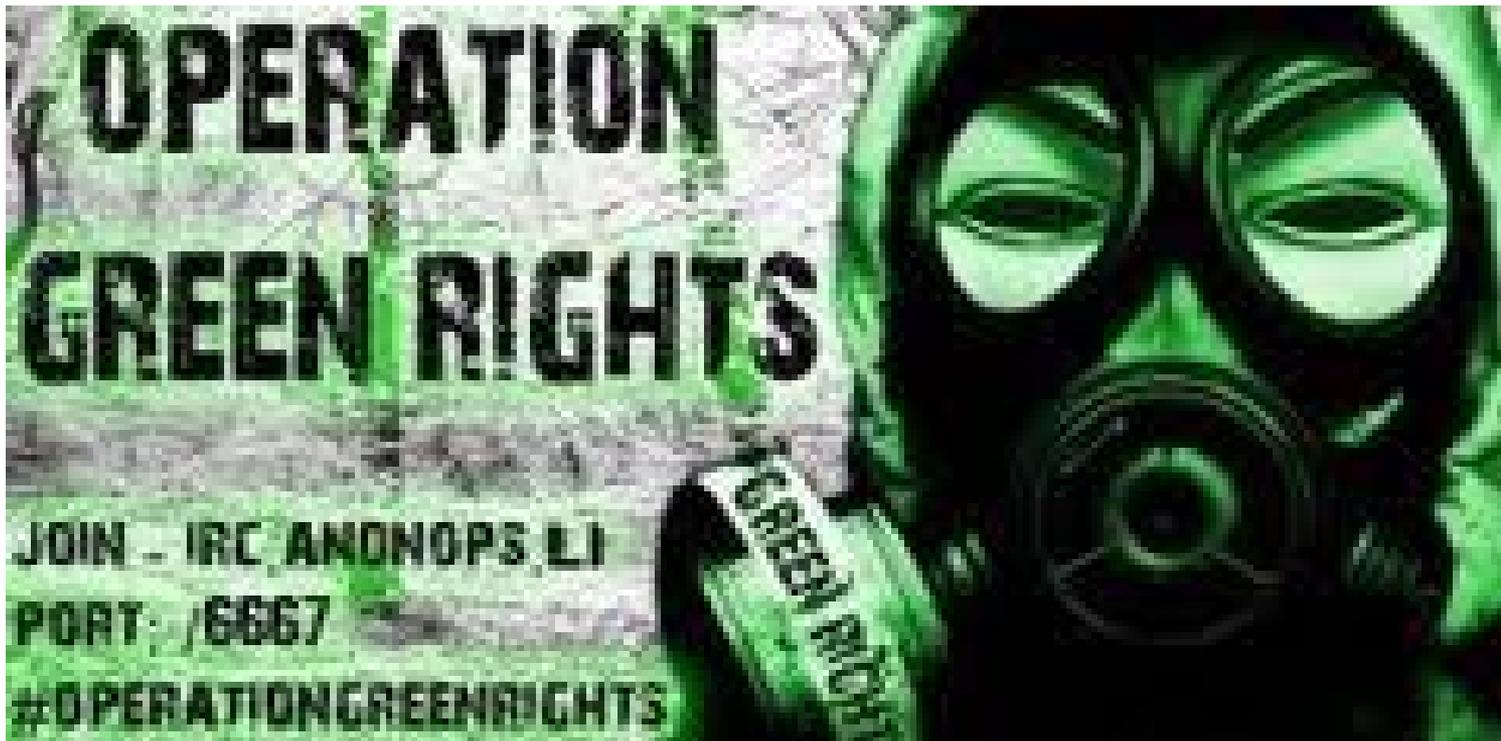
Field sites unsecure, network exposed to intrusion, data corruption and device exploitation

Secure zones require network equipment, administration, monitoring

Can be very expensive, can require extensive administration resources, can be complex to design and implement

Requires total system overhaul digital devices not necessarily as robust as legacy analog devices





**EXPECT US**

*You are Only Secure as Your Weakest Link*

# Secure Communications for Legacy SCADA Systems

?????

Jamey Hilleary

Elecsys Corporation

[Jamey.hilleary@elecsyscorp.com](mailto:Jamey.hilleary@elecsyscorp.com)

