# Securing Serial Control Systems

**Robert T. Sill**

**ICSJWG 2010 Spring Conference**

# Introduction

Asked to describe his job, Mike Selves, director of Emergency Management and Homeland Security in Johnson County, Kan., recalls what he once told county commissioners who also posed the question.

*"My job," he said, "is to tell you things you don't want to hear, asking you to spend money you don't have for something you don't believe will ever happen."*

# Current status

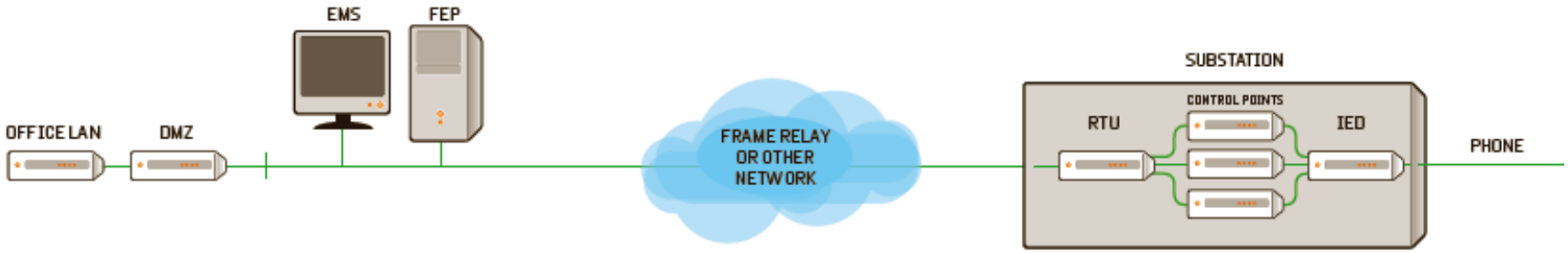
Increasing demand on Control System networks

Significant amount of legacy/serial communications

- Bit/byte-oriented protocols
- Lack of understanding of bit protocols
- Lack of security
- Lack of bandwidth

Reliability and security have already been jeopardized

# Typical control network



# Division between control center and field

Lack of understanding of entire communication network

- Network segmented with specialized expertise/knowledge
- Fewer Electrical Engineers, more IT

Collaboration between control center and field lacking

# Convergence of technologies

Serial: designed for reliability

IP: designed for information sharing

- Non-guaranteed delivery (without TCP)
- Shared bandwidth

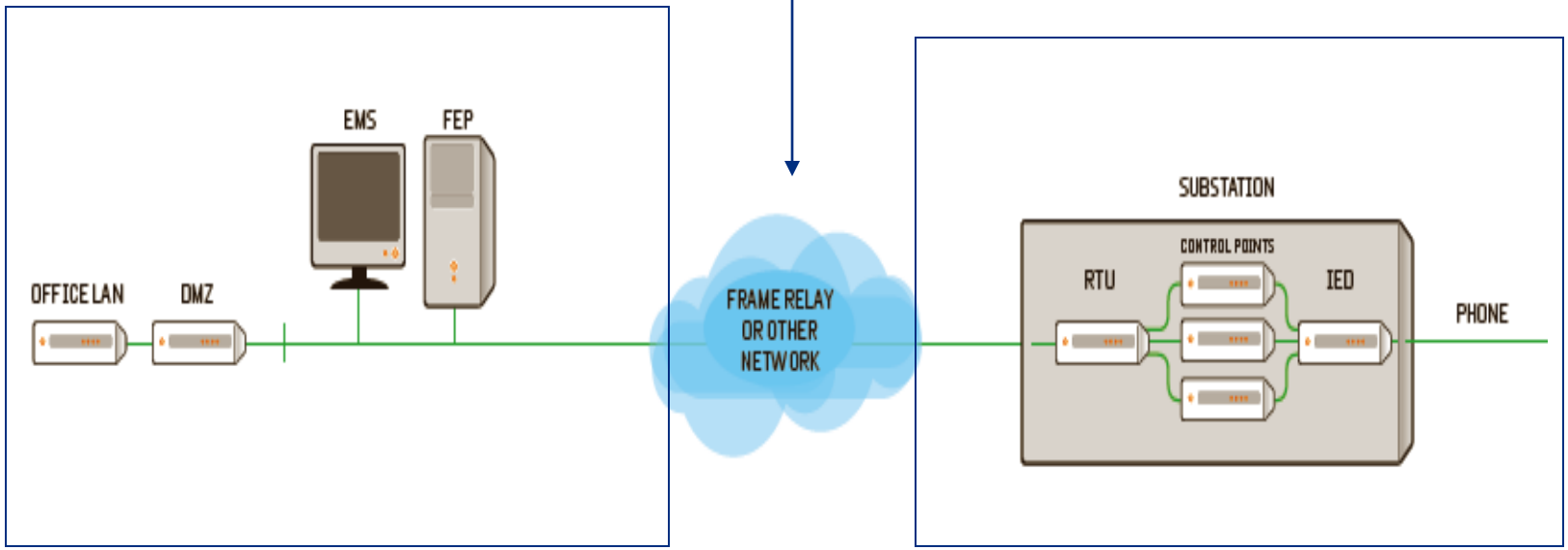
Neither system designed for security

# Control center vs. field

Who's responsibility is this?

Control Center responsibility

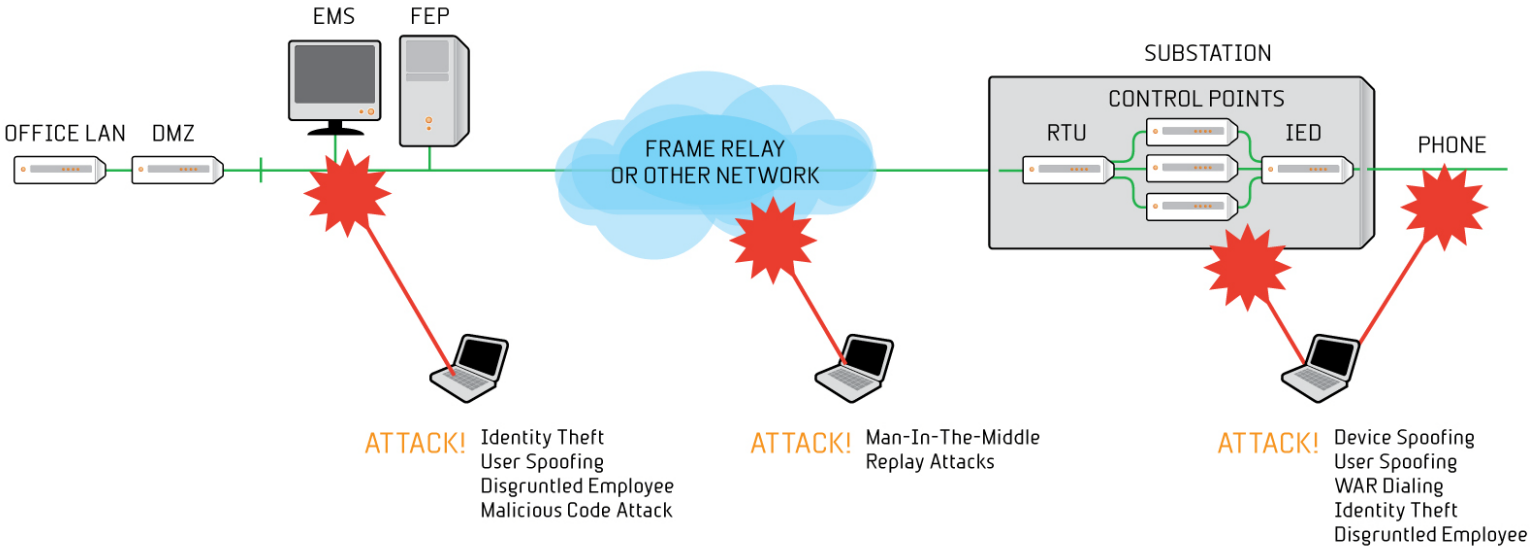
Field responsibility




IP

Serial

# Network vulnerabilities across system



# Current system upgrade options

Industry and Government moving in different directions

- Smart-Grid and Substation Automation → Interconnectivity/open
- NERC → Secure it or disconnect it
  - Routable protocols must have security measures in place
  - Non-routable protocols currently excluded

Upgrade process is time-consuming

- Budget limitations expected to cause upgrades to be piecemeal

# Securing IP networks

Industry moving towards IP networks for Smart Grid

- Consideration must be given to security, reliability, and cost of upkeep
- IP networks inherently insecure
  - 30+ years of hacking experience including annual hacking conferences
  - 25,000+ known IP network vulnerabilities (CVE list)
  - Some bugs in currently deployed security patches
  - More vulnerabilities discovered every day

# Case study

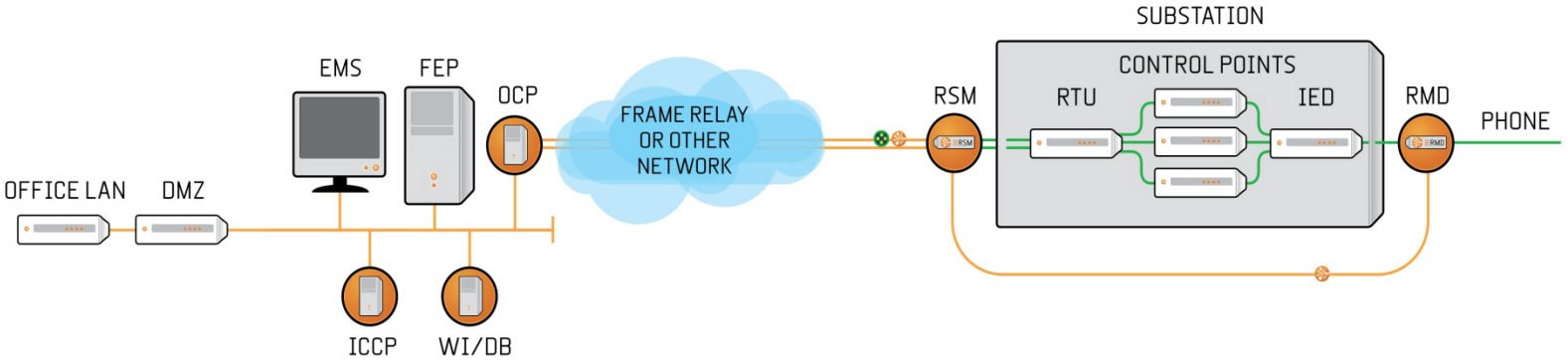
IOU deployment of secured serial communication

Extended life of existing communication infrastructure:

- Improved system performance
- Provided troubleshooting tools
- Provided centralized secure control of remote device

Securing major metropolitan area with over 100 substations

# Installed in network



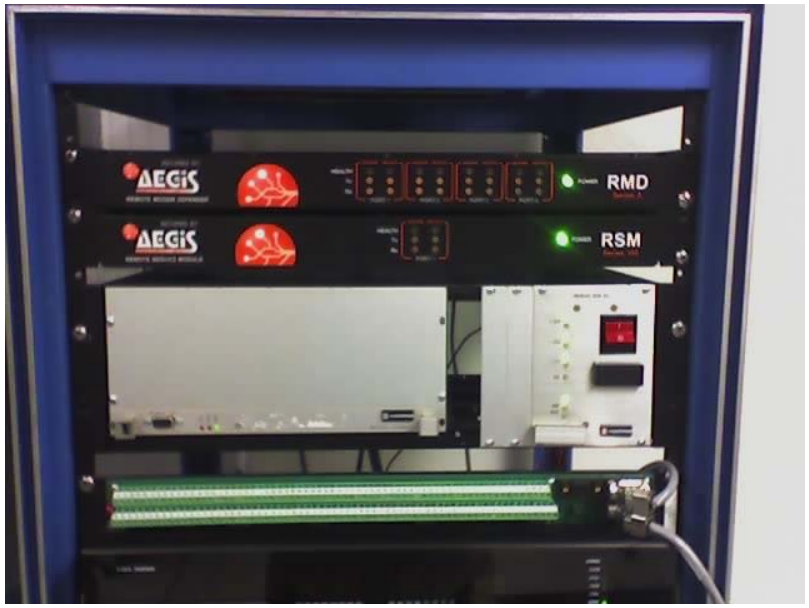
# Installation at Ops Ctr and Substation

At Operations Center:

Host installs next to EMS/DMS IEDs

At the Substation:

RSM, RMD next to RTU,



# Solution summary

Encrypted
- 2048-bit streaming encryption
- Supports TCP and serial links

Authenticated
- Device to device
- User authentication
- Configurable role-based user permission settings
- Centralized password management

Secured Remote Dialup Access

Hardened field unit installs at the substation
- Authenticates users dialing into IEDs
- Central management of dial-in users and passwords
- Real-time reporting of modem activity, alerts

# Case study results summary

- Improved secure communications
  - Configured serial maintenance ports from control center
  - Obtained higher data speeds using compression
  - Sent byte-oriented Conitel data to substation
  - Increased bandwidth without hardware modifications
  - Diagnosed communication errors from control center
- Provided comprehensive cyber-security perimeter to meet NERC CIP requirements

# Summary

- Technology to secure serial communications demonstrated in field
- Additional benefits for reliability and maintenance also demonstrated