

**ChevronTexaco**

# SCADA Needs from Manufacturing and Control Systems Vendors

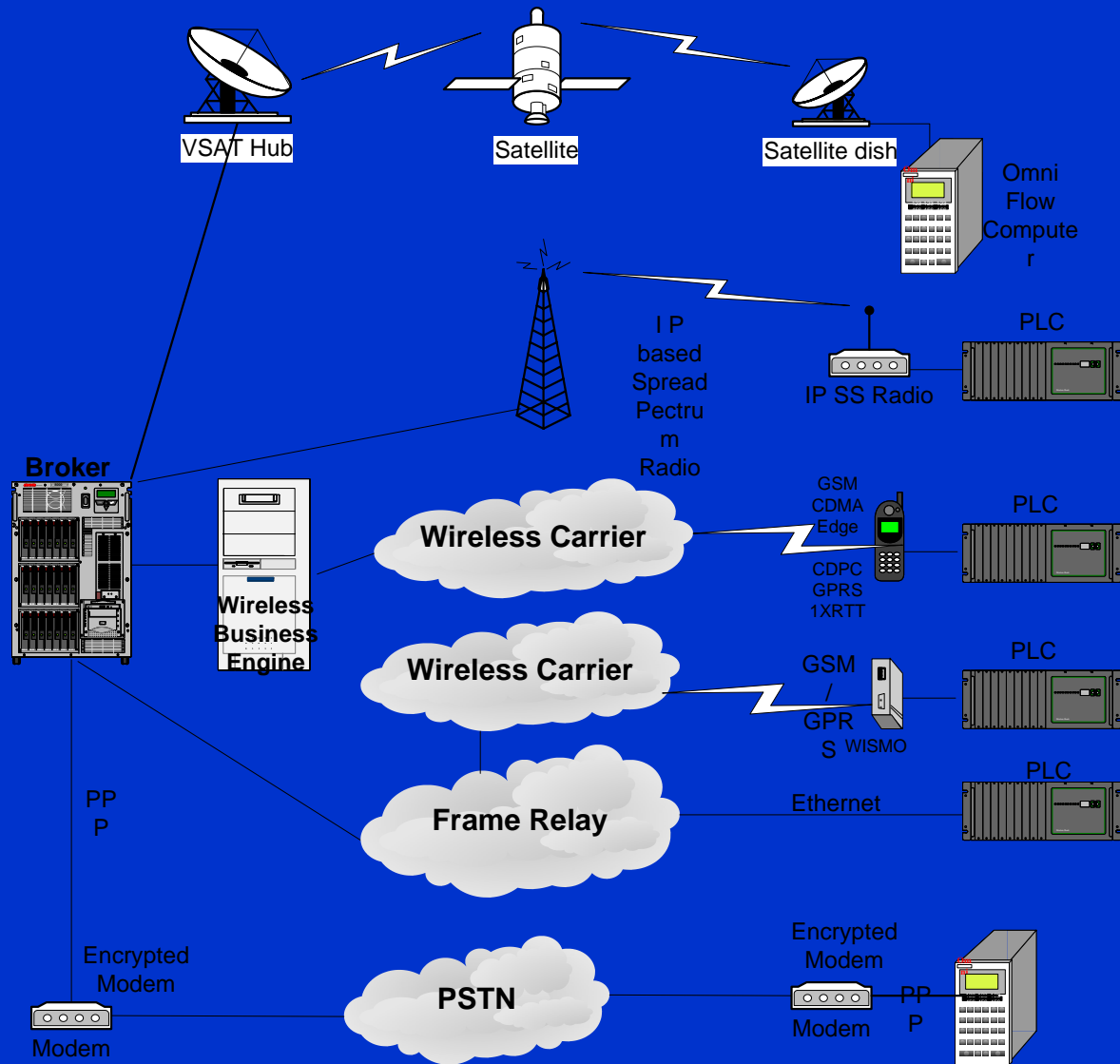
Presentation to

ISA EXPO 2004 Security Presentation

October 6<sup>th</sup>, 2004 (Houston)

Al J. Rivero, PE

# SCADA System



# System Vulnerability

- Data often sent in clear text
- Protocols are open, no security
- Control Systems networks are being integrated with corporate networks
- Vulnerability assessments have demonstrated unauthorized access to SCADA, DCS.
- PLCs can be compromised
- Remote Access (PCAnywhere, Xwindows)
- Telecom and other communications media

# System Vulnerability - Cont

- Ports and services open to outside
- Operating systems not “patched” with current releases
- Dial-up modems (already ubiquitous, trend toward wireless)
- Improperly configured equipment (firewall does not guarantee protection)
- Improperly installed/configured software (e.g., default passwords)
- Inadequate physical protection
- Exploitation of pathways that inadvertently allow access to critical assets
- Lack of sensitive information protection/disposal procedures
- Vulnerabilities related to “systems of systems” (component integration)

# Observations

- Cyber security policies and procedures lacking for Control Systems
- Corporate Culture
  - Lack of Control Systems Understanding
  - Security is of secondary importance
  - Minimal Accountability
  - Configuration management (Don't know what's out there)
  - IT doesn't understand Control Systems
- Security through obscurity
  - Poor defense against “structured adversary”

# Needs

- Firewalls for Control Systems
- Intrusion Detection Systems for Control Systems
- Secure Real Time Operating Systems
- Secure Control Systems Architecture
- Secure Protocols and Equipment Standards
- Encryption or alternatives for Control Systems
- Specifications/Standards for securing Control Systems