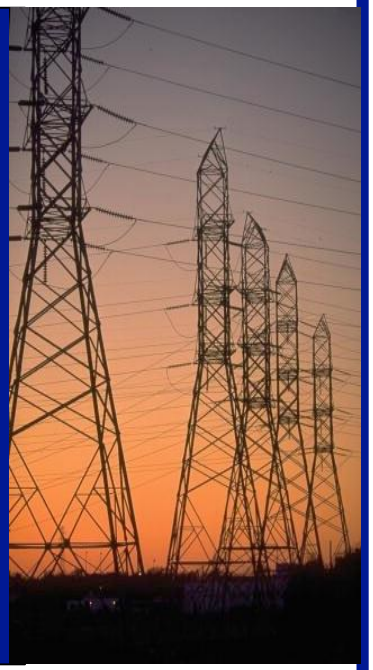
Experience with Implementing Cybersecurity in a G&T Coop

Andrew Wright, CTO

November 7, 2014



n-dimension solutions

G&T Coop

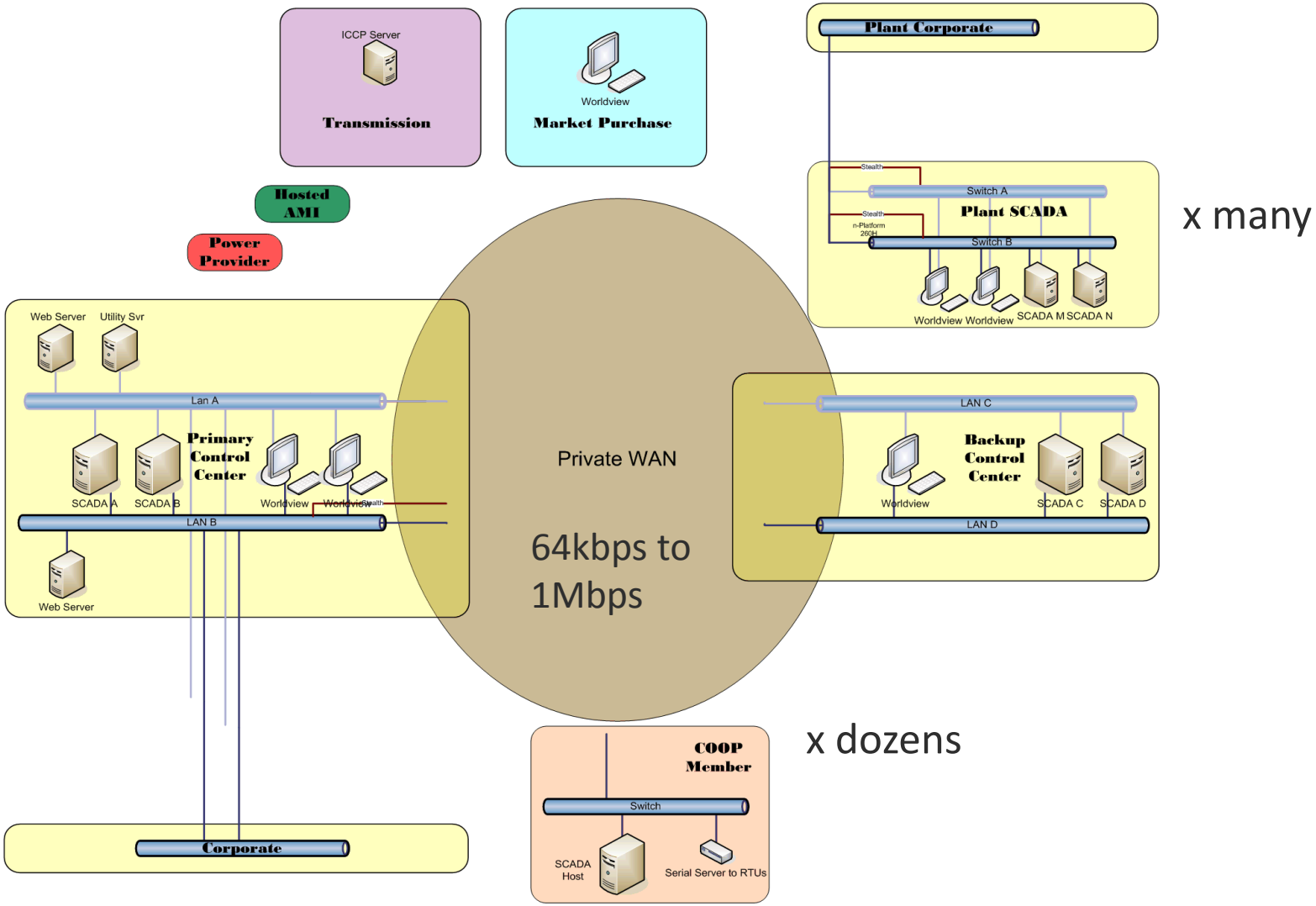
- 1 Primary Control Center
- 1 Backup Control Center
- dozens of Member COOPs
  - some with SCADA hosts
  - some with dual SCADA hosts
  - some with only RTUs
  - most with AMI
- several gas power plants
- several wind farms
- 1 Transmission provider
- 1 Power Provider
- 1 Power Market Purchaser
- 1 Hosted AMI Service

- 2000 MW combined peak load
  - residential
  - commercial
  - agricultural
- no critical assets per NERC CIP
- primary function of G&T is energy trading to provide members best possible rate

G&T Operations Technology (OT)

- SCADA
  - load data collected from members
- AMI
  - aggregate member usage information
  - provide hosted AMI functions to members
- OsiSoft PI
  - data historian for power plant data
  - historical analysis, forecasting

G&T Interconnect



n-dimension solutions

Security Goals

- protect OT
  - G&T from attack through members, plants, 3rd parties
  - plants, members from attack through members, plants, 3rd parties
  - all from private WAN compromise
- monitor for intrusions
  - G&T OT
  - plant OT
  - member OT

Reliability Goals

- improve resilience against cyber threats
- improve reliability of communications

- ensure
  - availability, integrity, and confidentiality
  - of load and plant data
  - to enable market trading $$$

N-Dimension Network Security

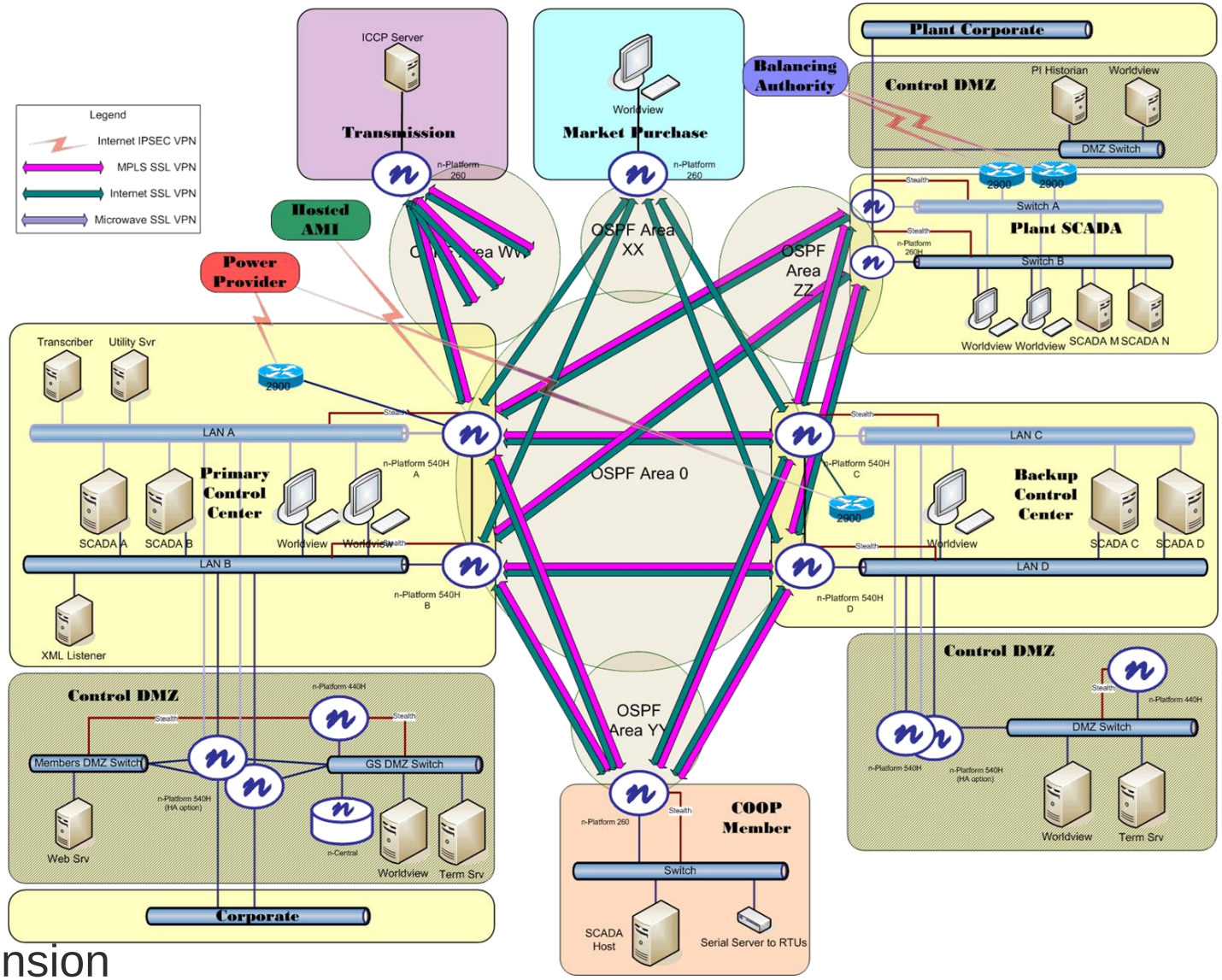
- n-Platform Unified Threat Management
  - UTMs provide a variety of security functions
    - perimeter and interior security for operations systems
    - passive and active security functions
    - Control DMZs segregating control from enterprise
    - encryption over private WAN, Internet, Radio
  - several dozen UTMs deployed in this soln
- n-Central Log & Event Management
  - one system providing central log & event mgmt

n-dimension
solutions

Security Deployment

- Secure Interconnect
  - secure communications
  - restrict protocols
- Operations / Corporate Segregation
  - via Control DMZs
- Monitor
  - detect potential intrusions
  - log events for forensic analysis

Secure Interconnect

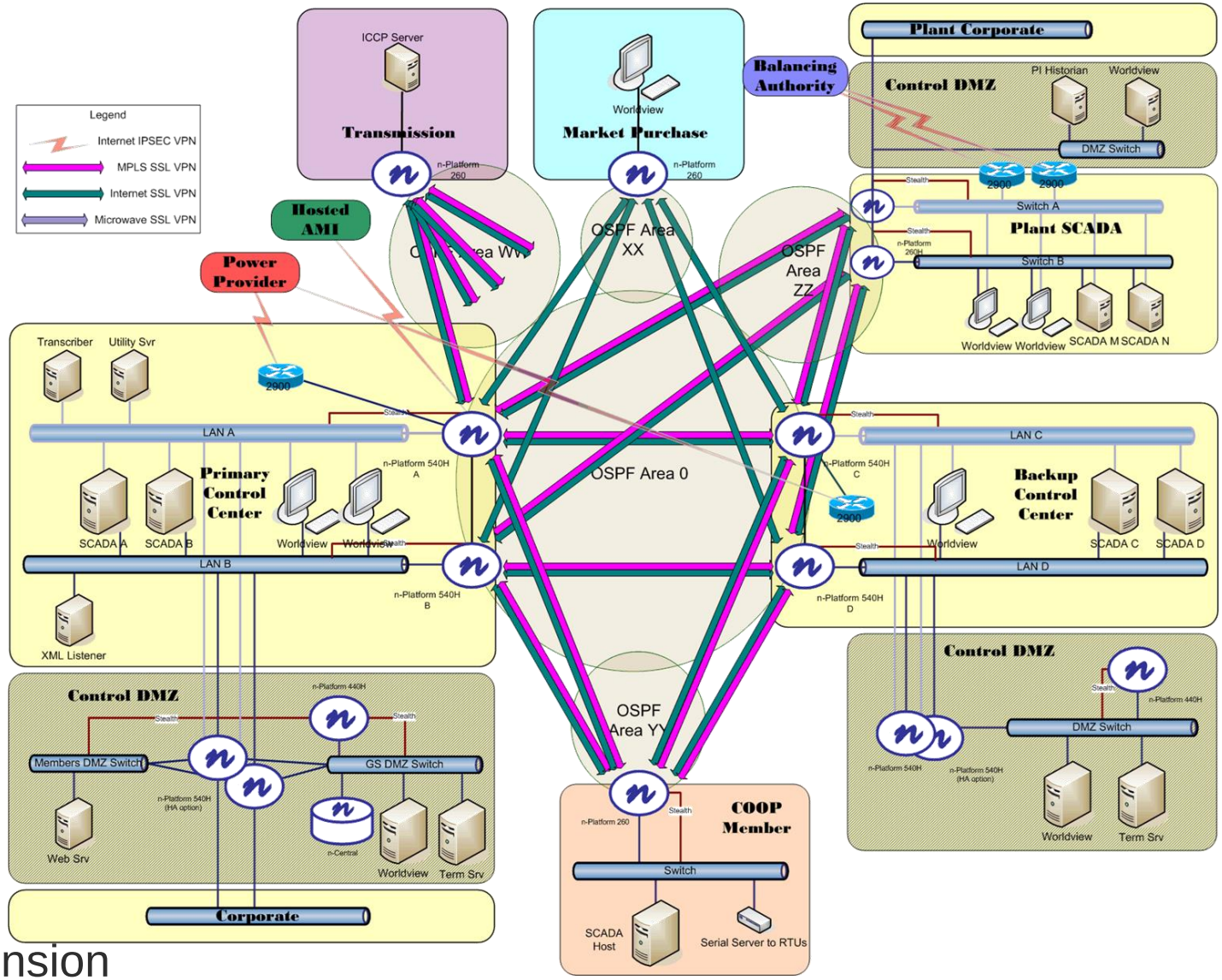


n-dimension solutions

Secure Interconnect

- SSL Site-to-Site VPNs between
  - over MPLS, Internet, Radio
- IPSEC Site-to-Site VPNs
  - for 3rd parties
- Stateful Firewall
  - to restrict protocols between sites
- OSPF Dynamic Routing
  - to improve availability
- Active / Standby Failover of UTMs
  - to improve availability

Segregation via Control DMZs

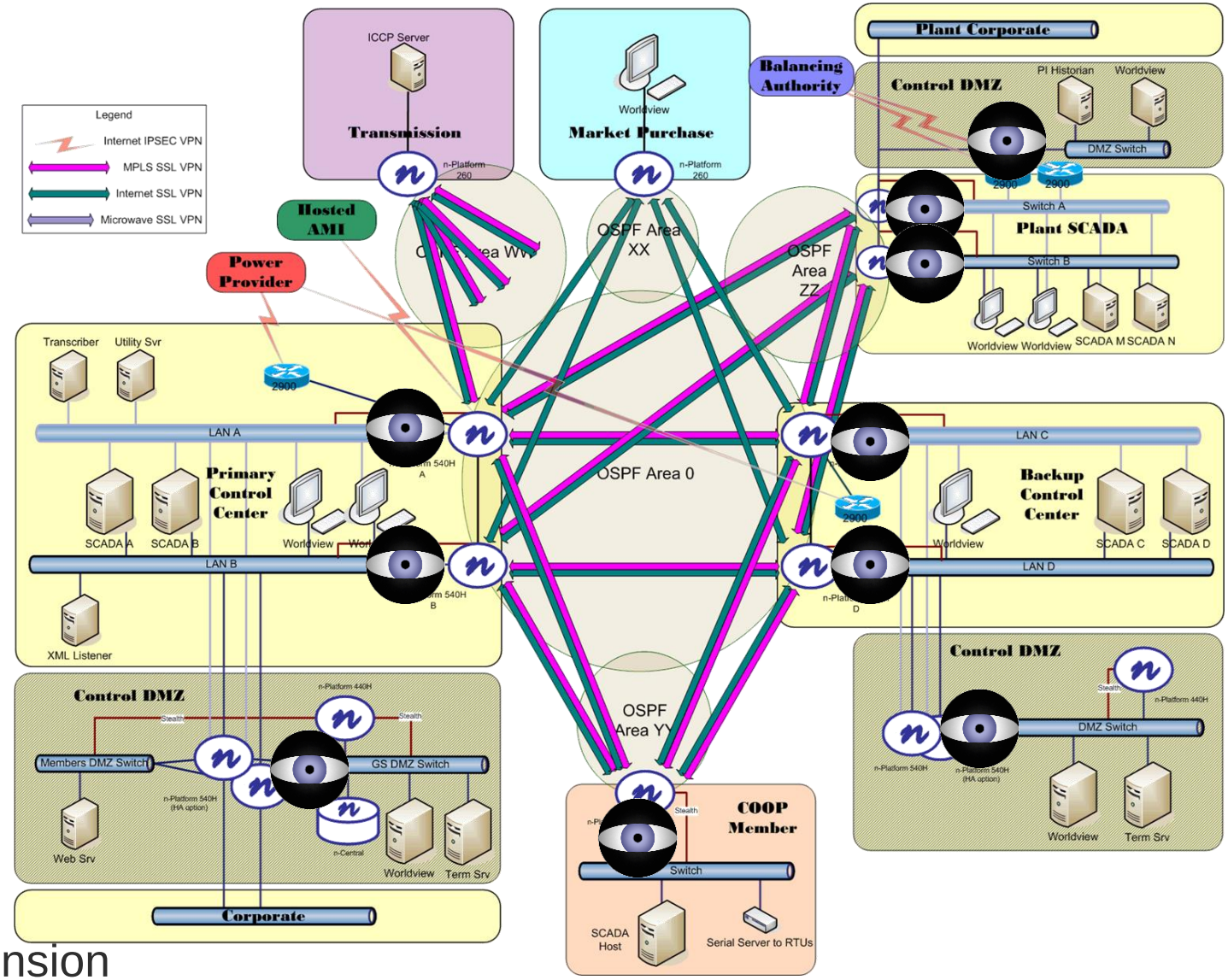


n-dimension solutions

Control DMZ Security

- Firewall limits inbound and outbound traffic
  - most traffic makes a stop at a “jump box”
- Remote access VPN authenticates connections
  - two-factor authentication
- IDS, scheduled port scanning, scheduled vuln scanning monitors DMZ servers
- Host anti-virus / whitelisting on DMZ servers
- Operations AD server providing centralized AAA for operations systems access

Monitoring OT Systems

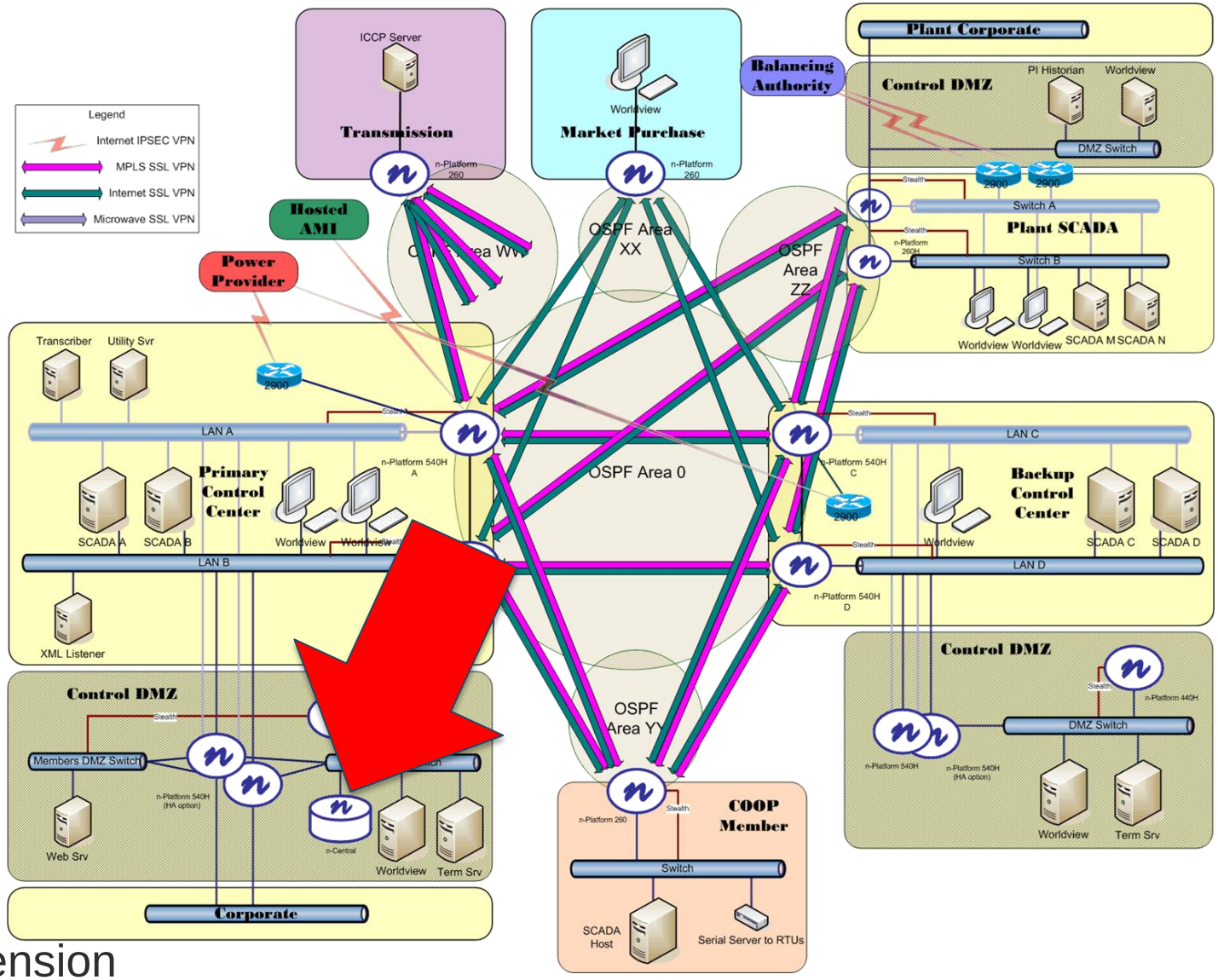


n-dimension solutions

Monitoring OT Systems

- Intrusion Detection System
  - signature based with SCADA signatures
- Port Scanning
  - scheduled
- Vulnerability Scanning
  - manually initiated
- System & Service Monitoring
  - cpu load, disk utilization, network utilization
  - service availability

Central Log & Event Monitoring



n-dimension solutions

Central Log & Event Monitoring

- events and logs collected by n-Central
  - all n-Platforms
  - certain Windows servers
- critical events forwarded to email addresses and thereby mobile phones
- summary security status displayed on SCADA

Experiences

n-dimension
solutions

Status

- “fully deployed” for more than a year
- “full deployment” took several years
- several questionable cyber events detected, but none directly identified as attacks
  - corporate network not monitored
  - firewalls may have blocked attacks
  - G&T may not have told N-Dimension of attacks
- significant improvement in communications availability due to dynamic routing

IP is Interoperability

- real world environments are heterogeneous
  - OT: ICCP, DNP3, Modbus
  - proprietary SCADA, AMI, etc.
  - IT: RDP, HTTP, HTTPS, FTP, etc.
  - many custom built devices, applications
- IP is the interoperability framework
  - only 2 serial links in this G&T
- IP network layer security protects IT & OT
  - VPN, firewall, IDS, VLAN, OSPF

Politics

- we desired to implement
  - network segregation within members
  - monitoring of member OT networks
  - secure remote access to member networks
- but ownership issues intruded!
  - members won’t provide details of their networks
  - members do not want G&T to see their traffic
  - G&T does not want to own/control equipment in member’s systems

PCI Compliance

- in several cases members refused Internet connections as backup links
  - these would need to be addressed in their PCI compliance requirements
  - poor segregation of billing functions from control functions?

Geography

- many sites are fairly remote, making any onsite work require at least a full day

n-dimension
solutions

Weather

- adverse weather can disrupt your plans

n-dimension
solutions

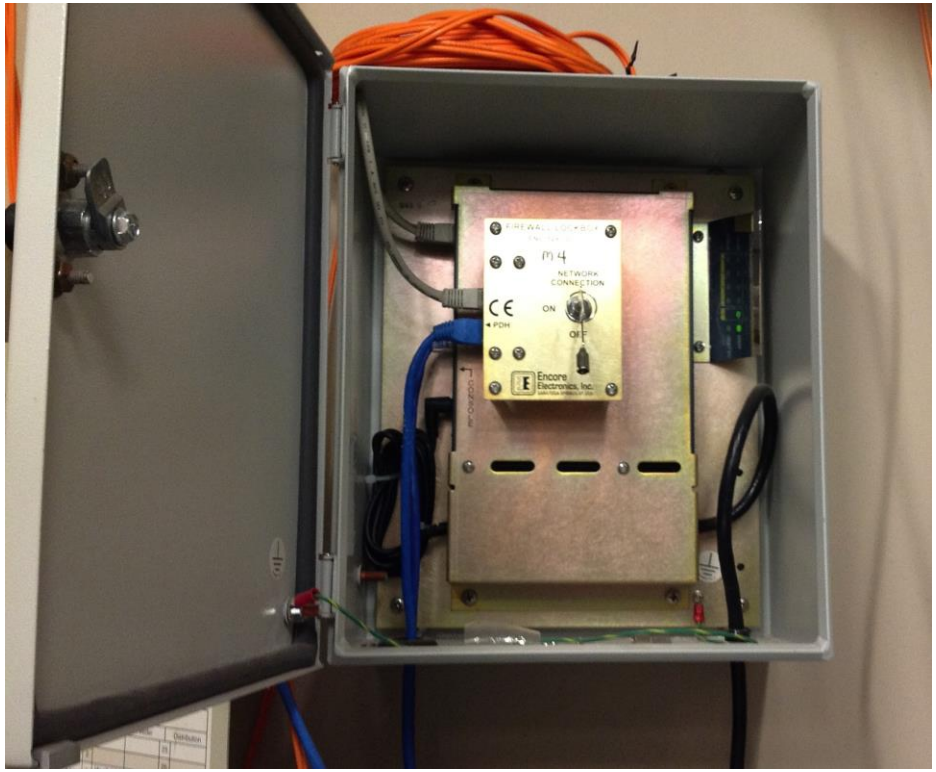
Scheduling

- outage windows may need to be coordinated weeks in advance
- last minute events may throw all those plans out the window

n-dimension solutions

Coordination with Third Parties

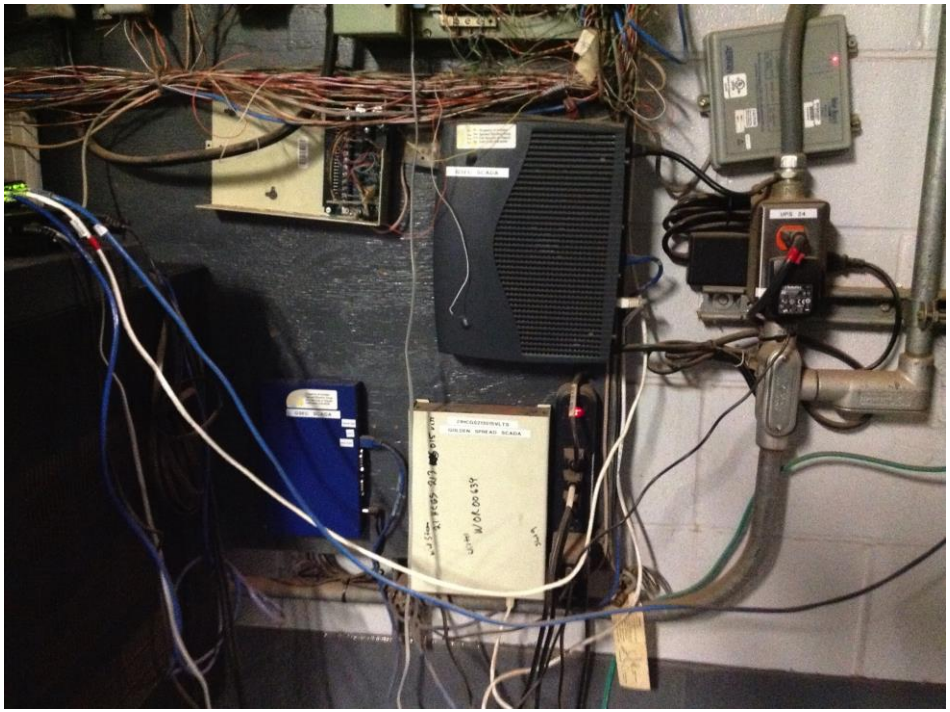
- change windows may need to be coordinated with 2 or 3 third parties



n-dimension
solutions

Can’t Touch This

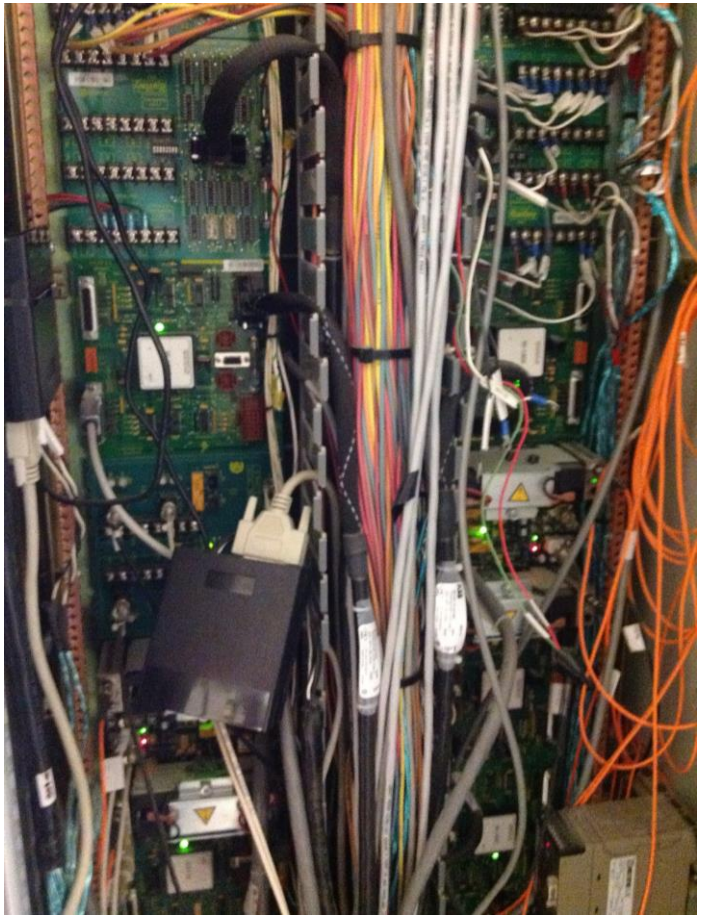
- significant periods, even whole seasons, of no changes allowed (it is critical infrastructure)



n-dimension
solutions

Complexity

- There are no detailed complete up-to-date network diagrams
- You can’t understand everything before you start



n-dimension solutions

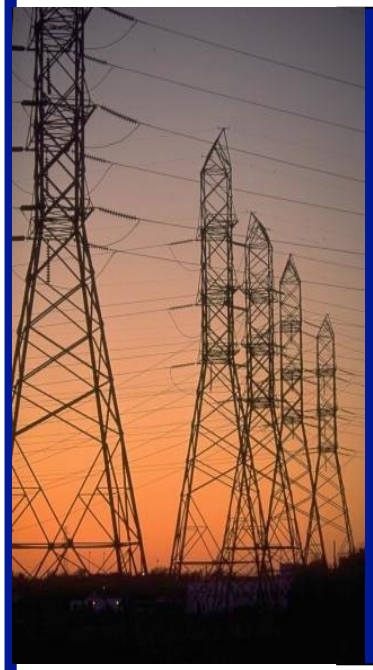
Don’t Screw Up!

have backup plans for your backup plans

Safety Briefings

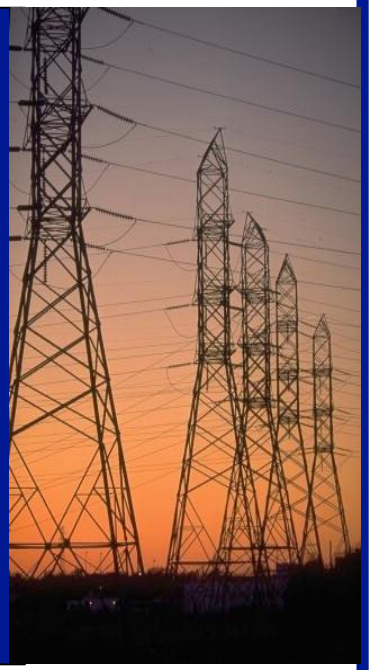
- pay attention, things DO blow up

If everyone else is running you better catch up!



Questions?

Thank you!



n-dimension
solutions