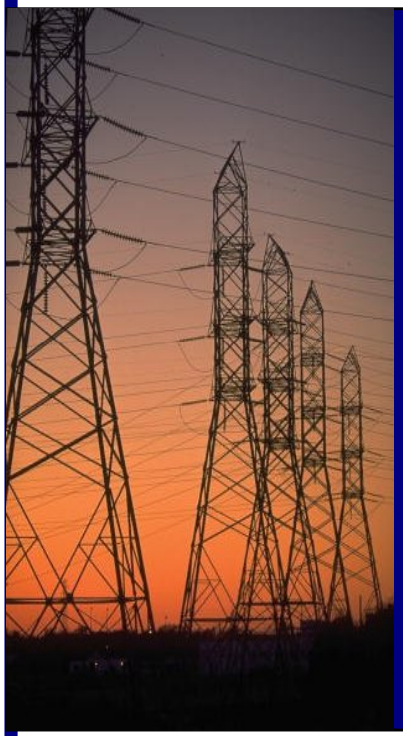
n-dimension solutions



Interoperability and Security for Converged Smart Grid Networks

Andrew Wright — **N-Dimension Solutions**
Paul Kalv — **Leesburg FL**
Rodrick Sibery — **Auburn IN**

Cyber Security for the Smart Grid™

Leesburg, FL

- municipal distribution utility with 23,000 meters
- extensive 96-count fiber backbone reaches electric utility, substations, various municipal buildings
- DOE SGIG stimulus winner $10M + $10M matching
- replacing all meters with wireless AMI smart meters
  - 15 minute usage for time differentiated rates
  - disconnect switches for prepaid
  - controllable thermostats and water heaters
- installing distribution automation for power quality
  - cap banks, voltage regulators, motor operated switches, faulted circuit indicators remotely controlled by wireless

Leesburg Smart Grid Network

- reconfigure fiber as Gigabit Ethernet redundant ring
  - SCADA communications
  - backup generation
- wireless canopy over entire city with backhaul via fiber
  - preferrably WiMax
  - AMI communications
  - DA communications
  - mobile workforce
  - police, fire, ambulance
  - WiFi hotspots?
  - residential broadband?

Auburn, IN

- municipal distribution utility with 7,000 meters
- extensive 96-count fiber-to-the-premises reaches electric utility, substations, municipal buildings
- DOE SGIG stimulus winner $2.1M + $2.1M matching
- replacing all meters with AMI smart meters
  - 5 minute usage for time differentiated rates
  - controllable thermostats and water heaters
  - website with customer usage tools
- installing distribution automation for power quality
  - cap banks, feeder relays, motor operated switches, reclosers remotely controlled over fiber

Auburn Smart Grid Network

- extend FTTP all the way to meters as partial mesh
  - SCADA communications
  - AMI communications
  - DA communications
  - WiFi hotspots
  - residential broadband, VoIP, IPTV

Converged Smart Grid Networks

AMI + DA + SCADA + DG + broadband + VoIP + IPTV

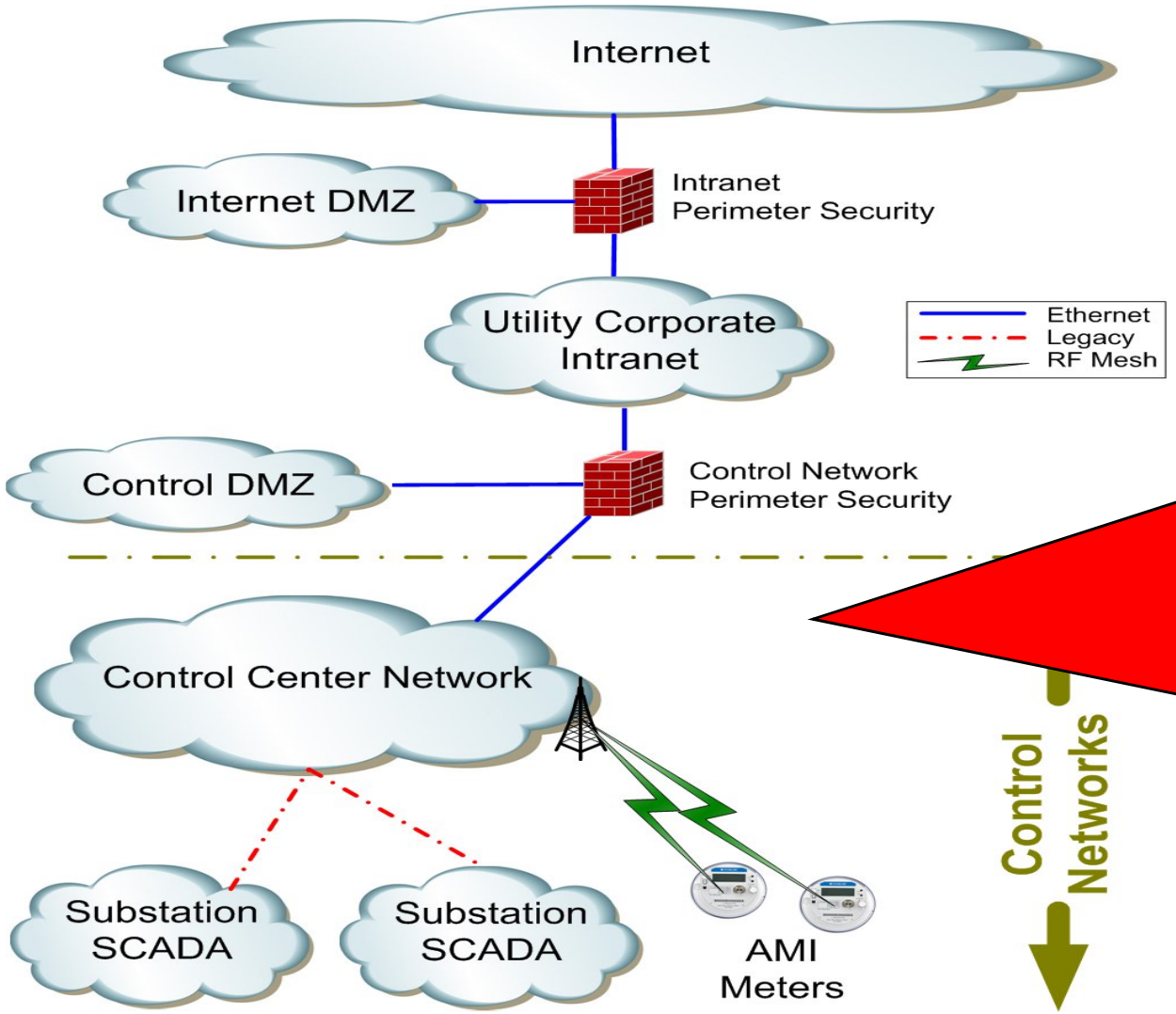
=

converged smart grid network

- interoperability – enabled by **IP**
- high speed – can support variety of applications
- economical – leverages existing technologies
- future proof – can evolve with IP technologies
- inherently standards based and multi-vendor

Security?

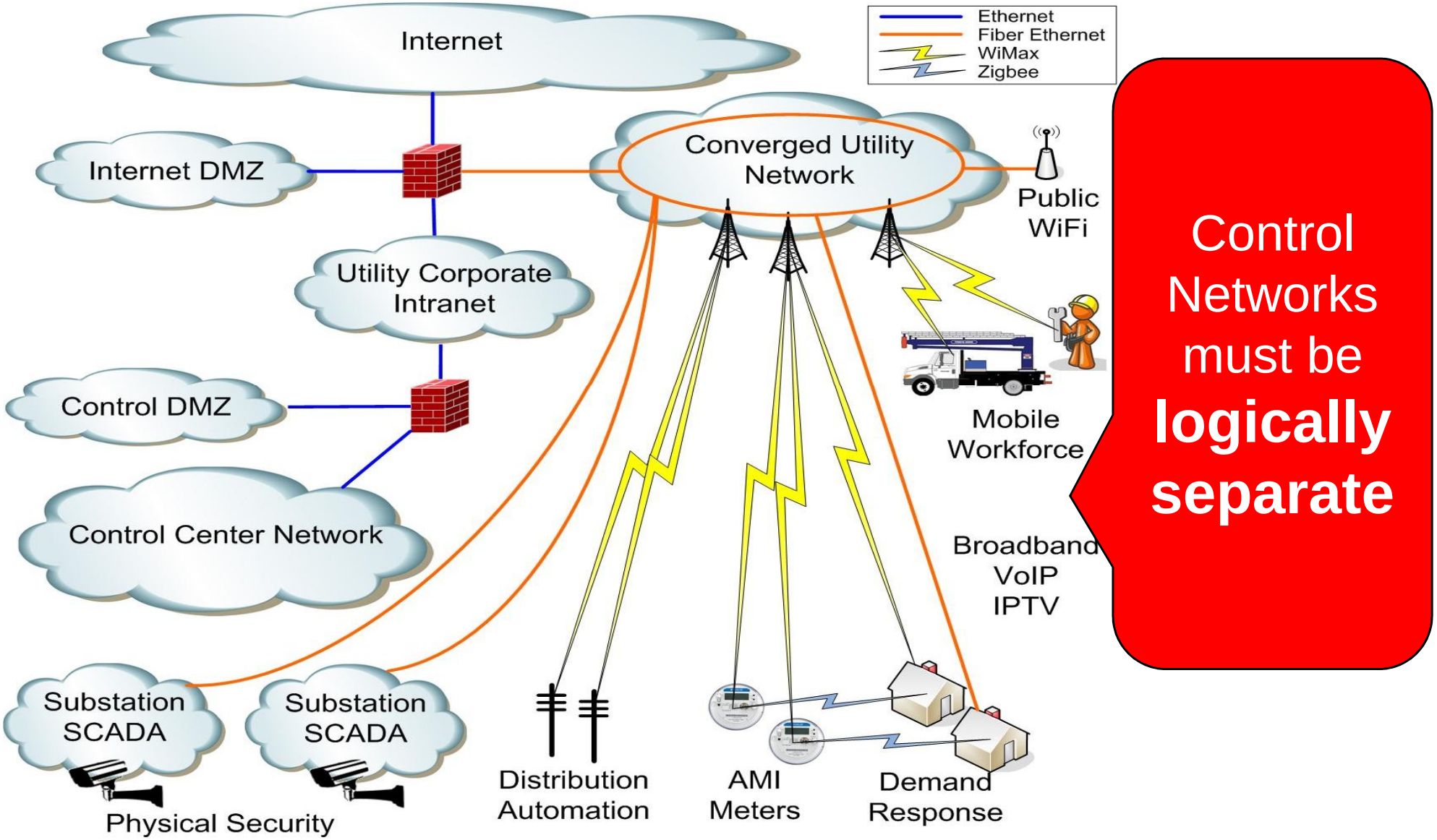
Typical Secure Control System Architecture



Control Network(s) strongly separated on physically separate networking devices

NIST SP800-82

Converged Smart Grid Network



Logical Separation for Converged SGN

- how to achieve logical separation?
- consider logical separation at the different layers of the IP stack
  - Layer 1 – Physical Layer
  - Layer 2 – Link Layer
  - Layer 3 – Internet Layer
  - Layer 7 – Application Layer

Logical Separation at Layer 1

- Separation at Physical Layer can use:
  - different fibers
  - different fiber wavelengths
  - different radio spectrum
  - different radio frequency hopping schemes
- None are 100% secure
  - geographic distribution makes physical security impractical
    - physical tapping of media – both fiber and wireless
    - interconnection points
  - frequency hopping scheme must be public for interoperability!
  - *special* licensed spectrum may impede interoperability!

Logical Separation at Layer 2

- Separation at Link Layer can use:
  - link layer encryption, eg. WiMax uses AES and CBC-MAC
  - VLANs
  - Network Access Control eg. 802.1X
  - switchport security
  - quality of service markings
- None are 100% secure
  - encryption keys can be extracted from devices
  - CAM table attacks, VLAN hopping attacks can breach VLANs
  - 802.1X has vulnerabilities, is not widely deployed in enterprise wired networks, and is complex to manage
  - switchport security can be fooled by spoofing MACs

Logical Separation at Layer 3

- Separation at Internet Layer can use:
  - firewalls
  - ACLs in switches
  - MPLS, VRF-lite
  - IPsec
  - diffserv, qos-preclassification
- None are 100% secure
  - firewalls are coarse, source IPs can be spoofed
  - distributed ACLs are difficult to manage
  - MPLS & VRF-lite rely on secure configuration of all switches
  - IPsec with IKE v2 is good, but complex to configure

Logical Separation at Layer 7

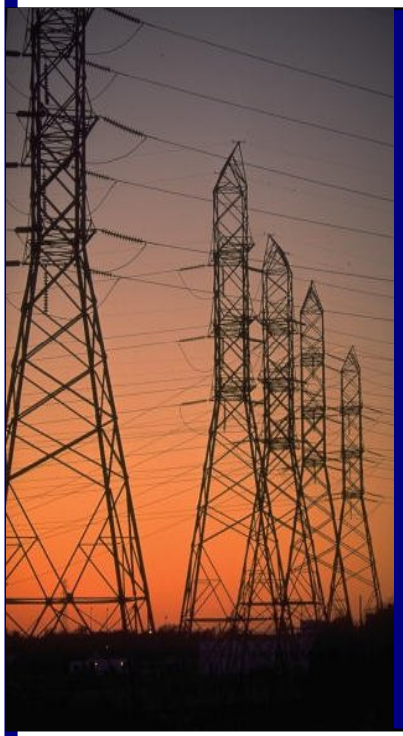
- Separation at Application Layer can use:
  - end-to-end encryption & authentication
  - TLS, DTLS
  - secure control systems protocols:
    - IEEE P1711
    - Secure DNP3
    - IEC 62351
    - SSCP
    - C12.22
- None are 100% secure
  - construction of secure cryptographic protocols, even from sound building blocks, is risky
  - application vulnerabilities can negate application protections

Secure Converged Smart Grid Networks

- secure logical separation requires multiple defenses at several different layers of the networking stack

Defense In Depth

- not just AMI/SCADA security
- not just network security
- not just OS/host security



Converged Smart Grid Networks

www.n-dimension.com

andrew.wright@n-dimension.com

full paper in proceedings has more details

Cyber Security for the Smart Grid™