

A background image showing several high-voltage power line towers silhouetted against a bright orange and yellow sunset sky. The towers are arranged in a receding line from left to right.

Increasing Your Utility's Reliability with Managed Cyber Security Services

Andrew Wright, CTO

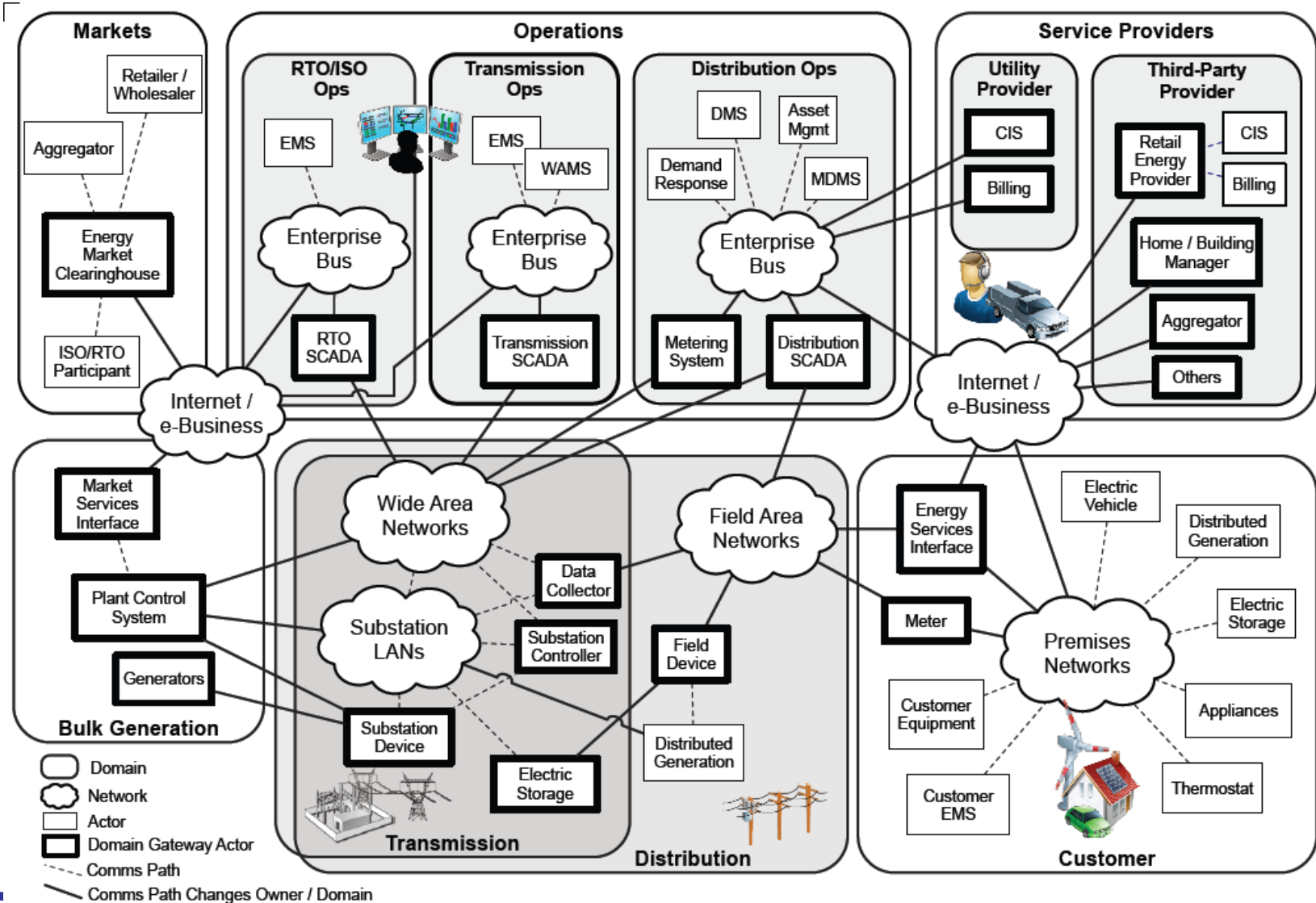
EDIST 2012

January 2012

Toronto Canada

Cyber Security for the Smart Grid™

Smart Grid Complexity



Must Not Forget About Security!



as we pile all this stuff
onto the smart grid ...

lest we get caught with
our ass in the air



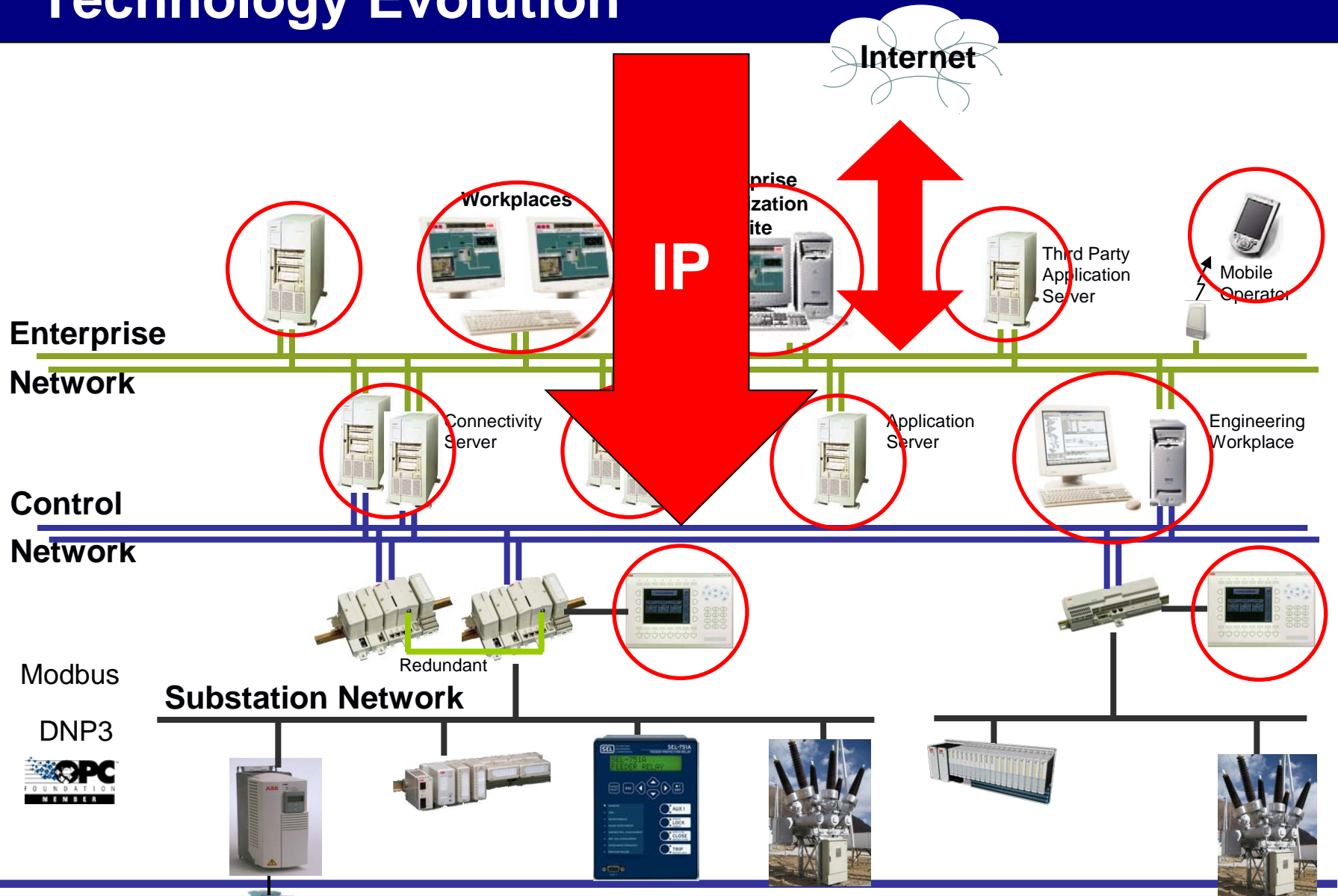
Recent Cyber Security Events

- Water plant pump attack Nov 2011
- Duqu – son of Stuxnet Oct 2011
- Anonymous threatens control system attacks Oct 2011
- Predator and Reaper drones Oct 2011
- Comodo, DigiNotar CAs Mar 2011, Aug 2011
- ORNL, PNNL National Labs Apr 2011, Jun 2011
- Lockheed Martin May 2011
- Sony Playstation Apr 2011
- RSA SecurId Mar 2011
- Night Dragon Jan 2011
- Stuxnet Aug 2010
- Operation Aurora (Google) Jan 2010



Vulnerabilities in Utility Operational Systems

Technology Evolution



Security Vulnerabilities in Operational Systems

- COTS + IP + connectivity = many security vulnerabilities
- All of those of Enterprise networks and more

Worms and Viruses

DOS and DDOS impairing availability

Unauthorized access

Unknown access

Unpatched systems

Little or no use of anti-virus

Limited use of host-based firewalls

Improper use of operations workstations

Unauthorized applications

Unnecessary applications

Open FTP, Telnet, SNMP, HTTP ports

Fragile control devices

Network scans by IT staff

Legacy OSES and applications

Inability to limit access

Inability to revoke access

Unexamined system logs

Accidental misconfiguration

Improperly secured devices

Improperly secured wireless

Unencrypted links to remote sites

Passwords sent in clear text

Default passwords

Password management problems

Default OS security configurations

Unpatched routers & switches

See NISTIR 7628 Section 7!

Intra-System Vulnerabilities

- Enterprise Systems:
 - OS vulnerabilities
 - Application vulnerabilities

Billing

Eng

- Operational Systems:
 - OS vulnerabilities
 - Application vulnerabilities
 - Legacy vulnerabilities

ODMS

AMI

OMS

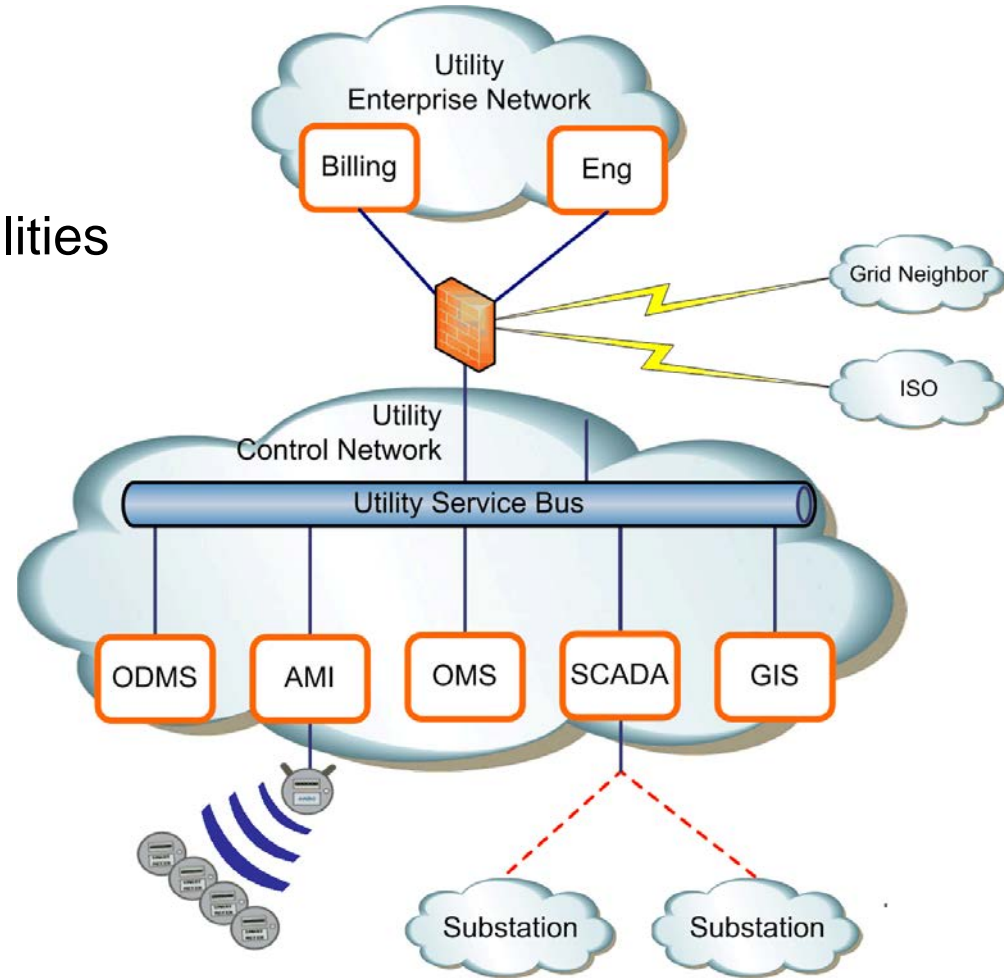
SCADA

GIS



Inter-System Vulnerabilities

- Interconnected Systems:
 - Network vulnerabilities
 - Communications vulnerabilities
 - Systemic vulnerabilities



What Are The Most Likely Attacks?

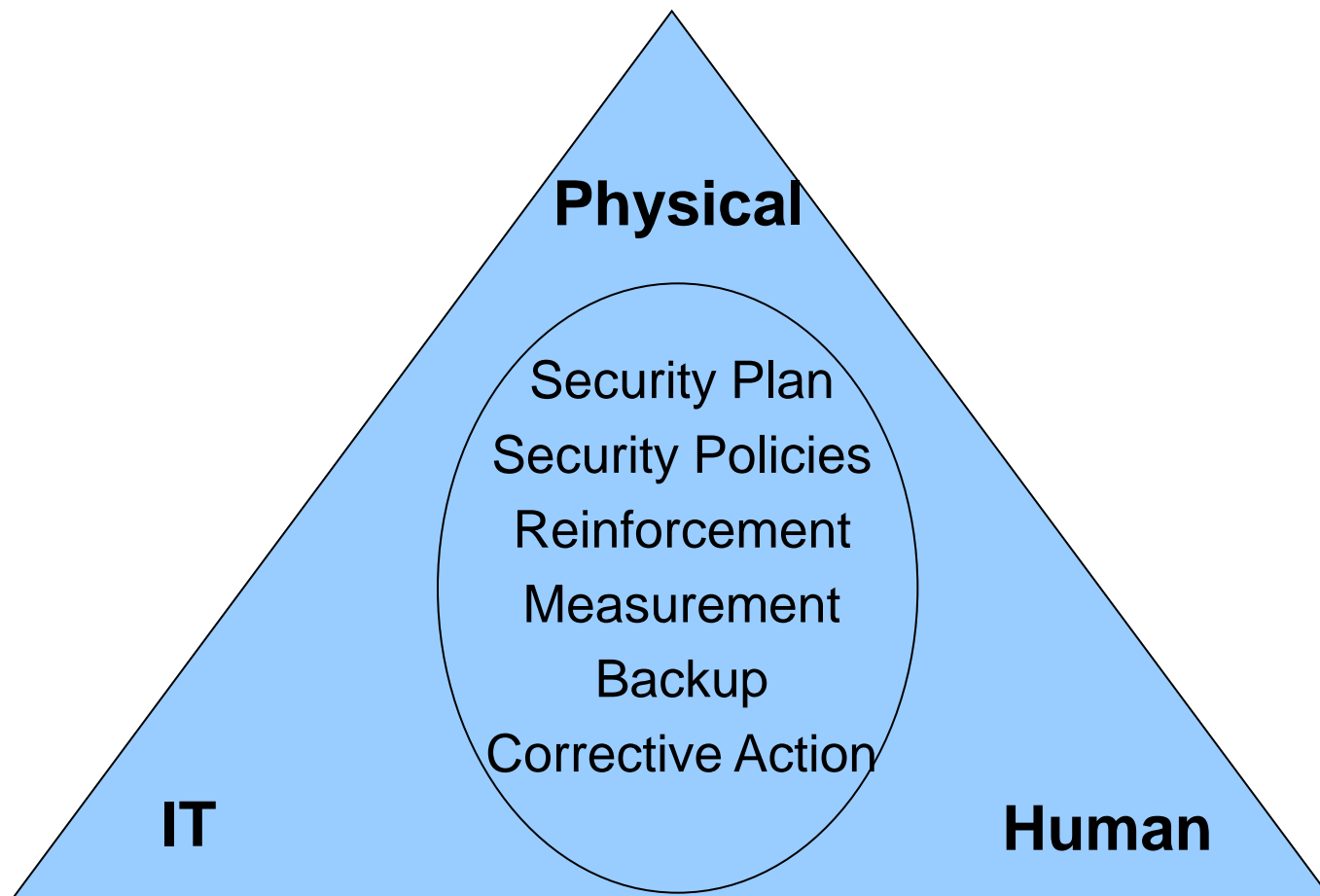
- malware impairing operations
 - no human behind the attack
 - no awareness that victim is a utility
- malware targeting specific types of utility systems
 - nations, nation states
 - combined cyber/physical attack
- dormant malware
 - activated some day in the future
- disgruntled insiders

these attacks seek out poorly secured systems

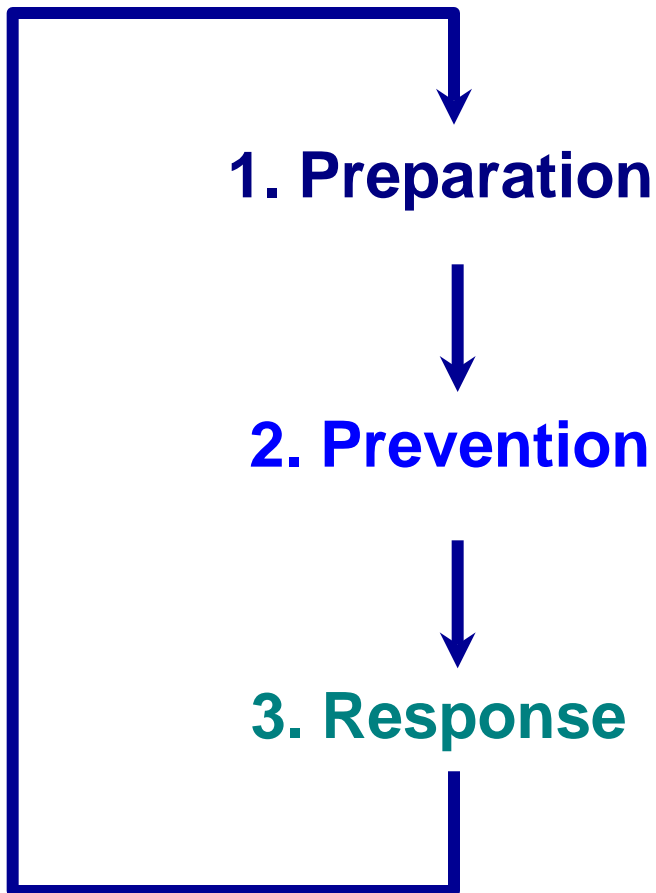


General Approach To Protecting Utility Operational Systems

Holistic Approach to Cyber Security



Lifecycle Approach to Cyber Security



1. Preparation

Preparation

- create/review policy statements
- conduct a risk analysis
- establish/review security team structure

2. Prevention

Prevention

- deploy security countermeasures
- approve security changes
- monitor security posture

3. Response

Response

- respond to security violations
- restoration
- review

Defense in Depth

- Perimeter Protection
 - Firewall, IDS, IPS, Net AV
 - remote access VPN
 - DMZ
- Interior Security
 - IDS, Scanning
 - NAC
 - Host IDS, Host AV
- Communications Security
 - VPN
 - IEEE 1711, IEC 62351
- Monitoring
- Management
- Processes
- Plans



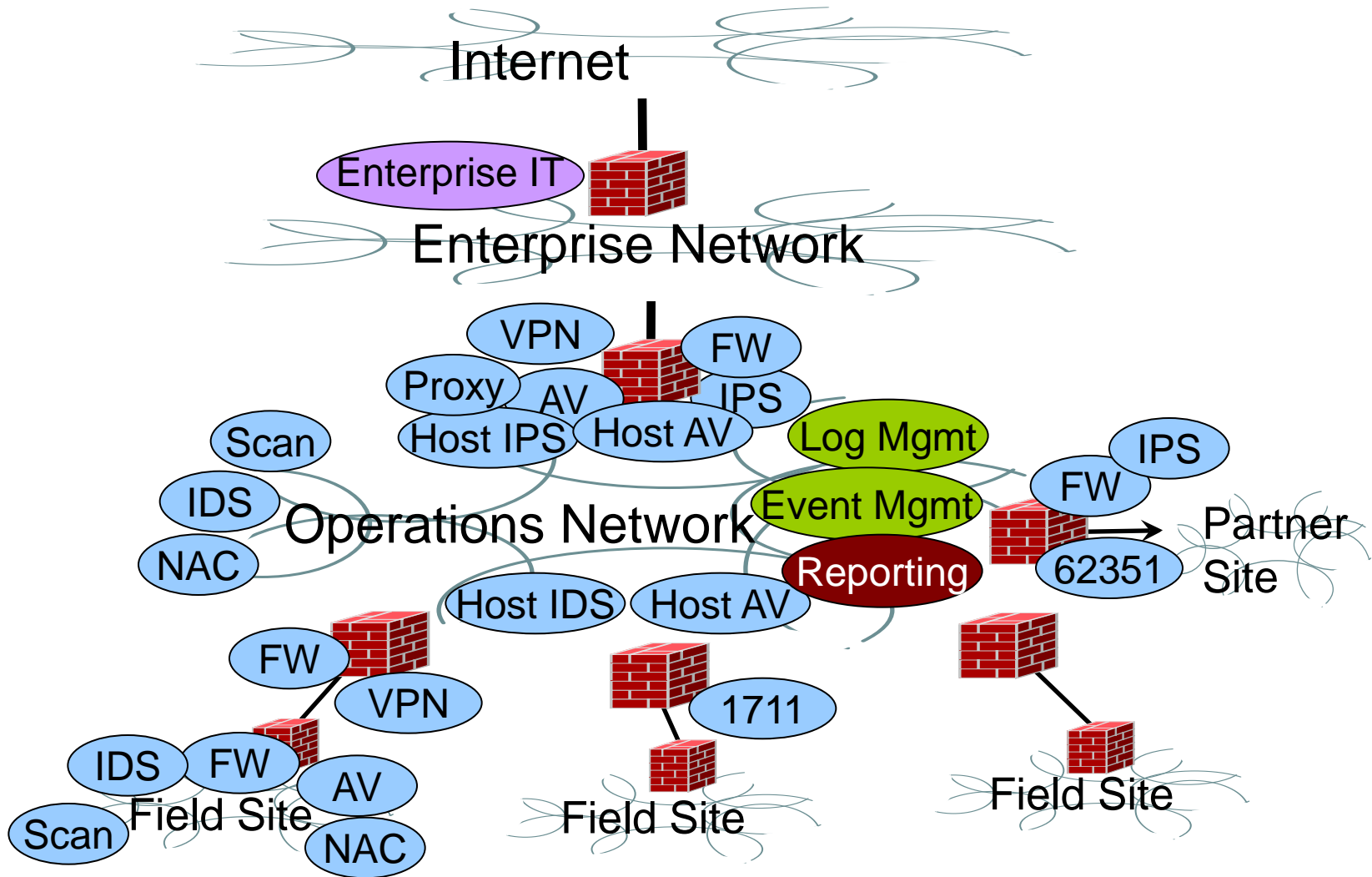
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
DMZ	DeMilitarized Zone
VPN	Virtual Private Network (encrypted)
AV	Anti-Virus (anti-malware)
NAC	Network Admission Control

Defense Without Depth



This is your network if all you have is a firewall!

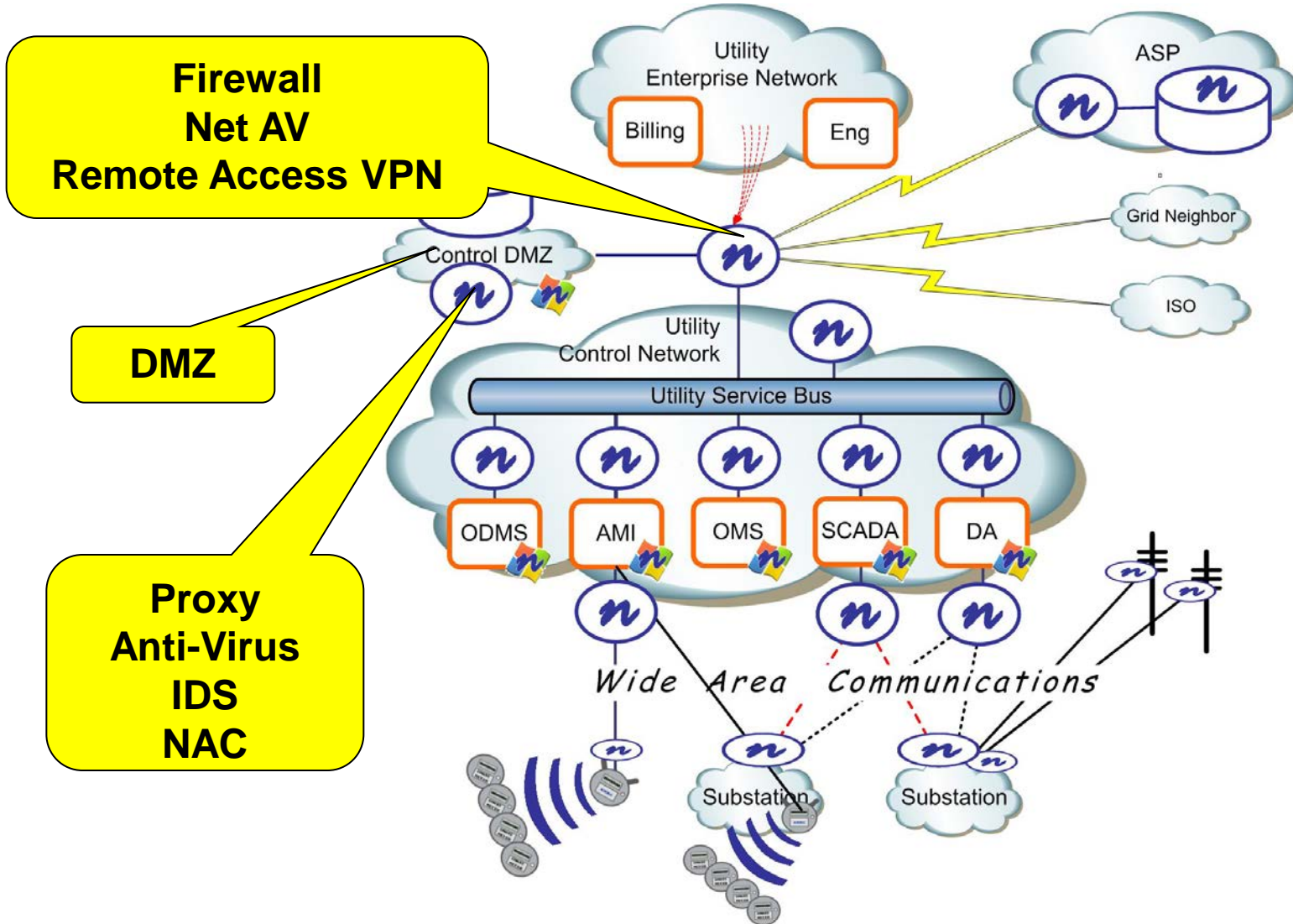
Countermeasures - Defense in Depth



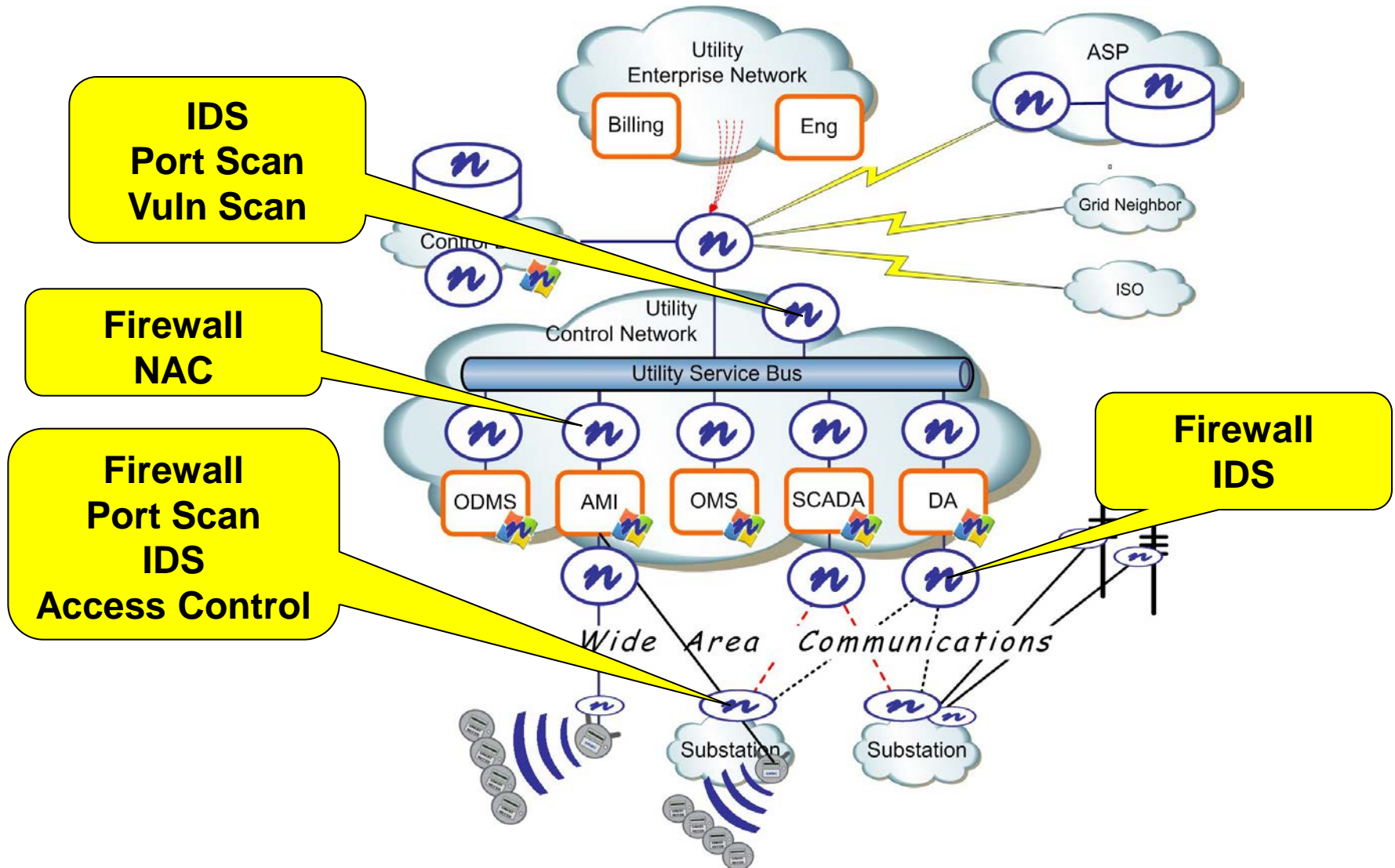


Protecting LDC Operations Systems

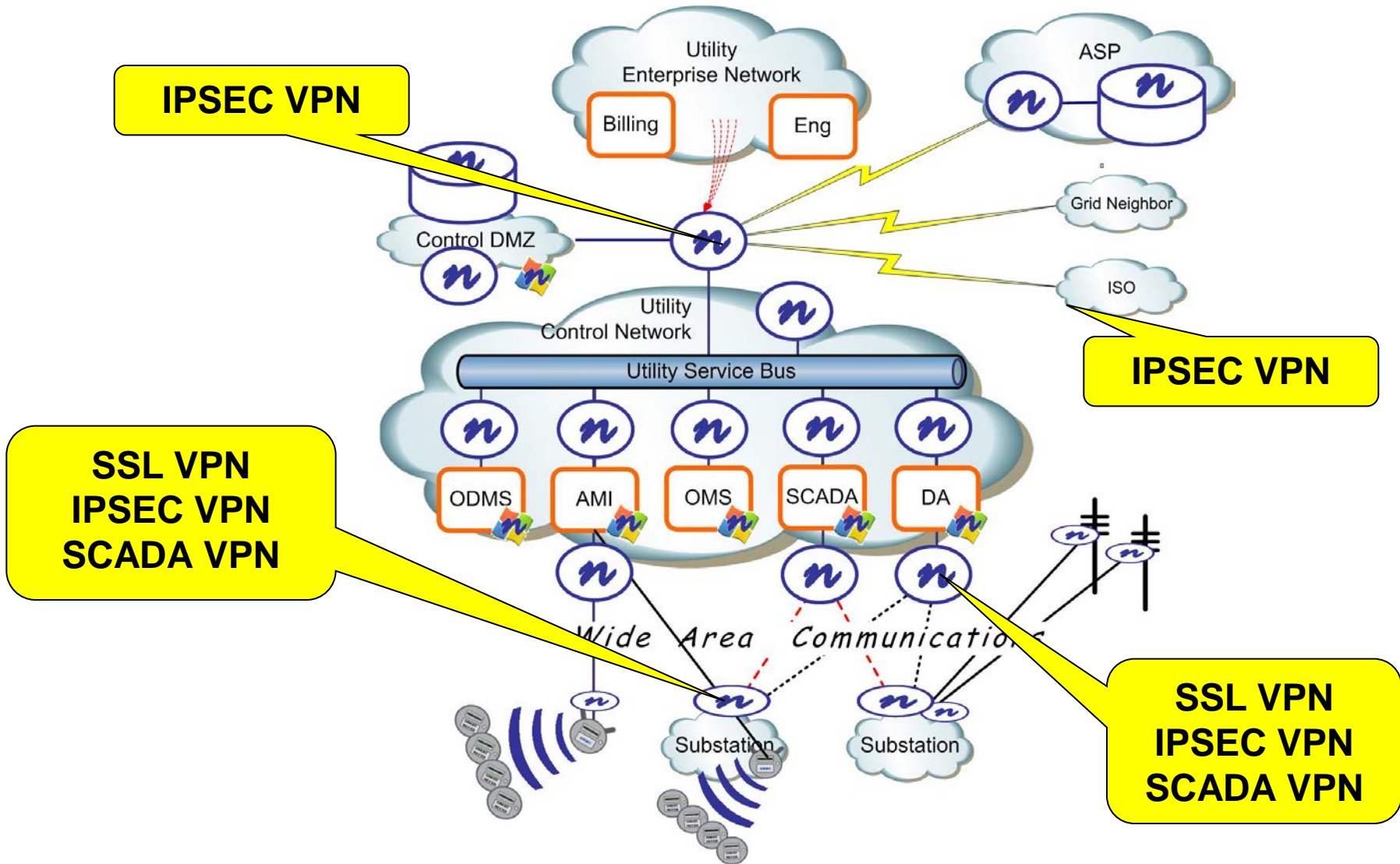
Perimeter Defense-in-Depth



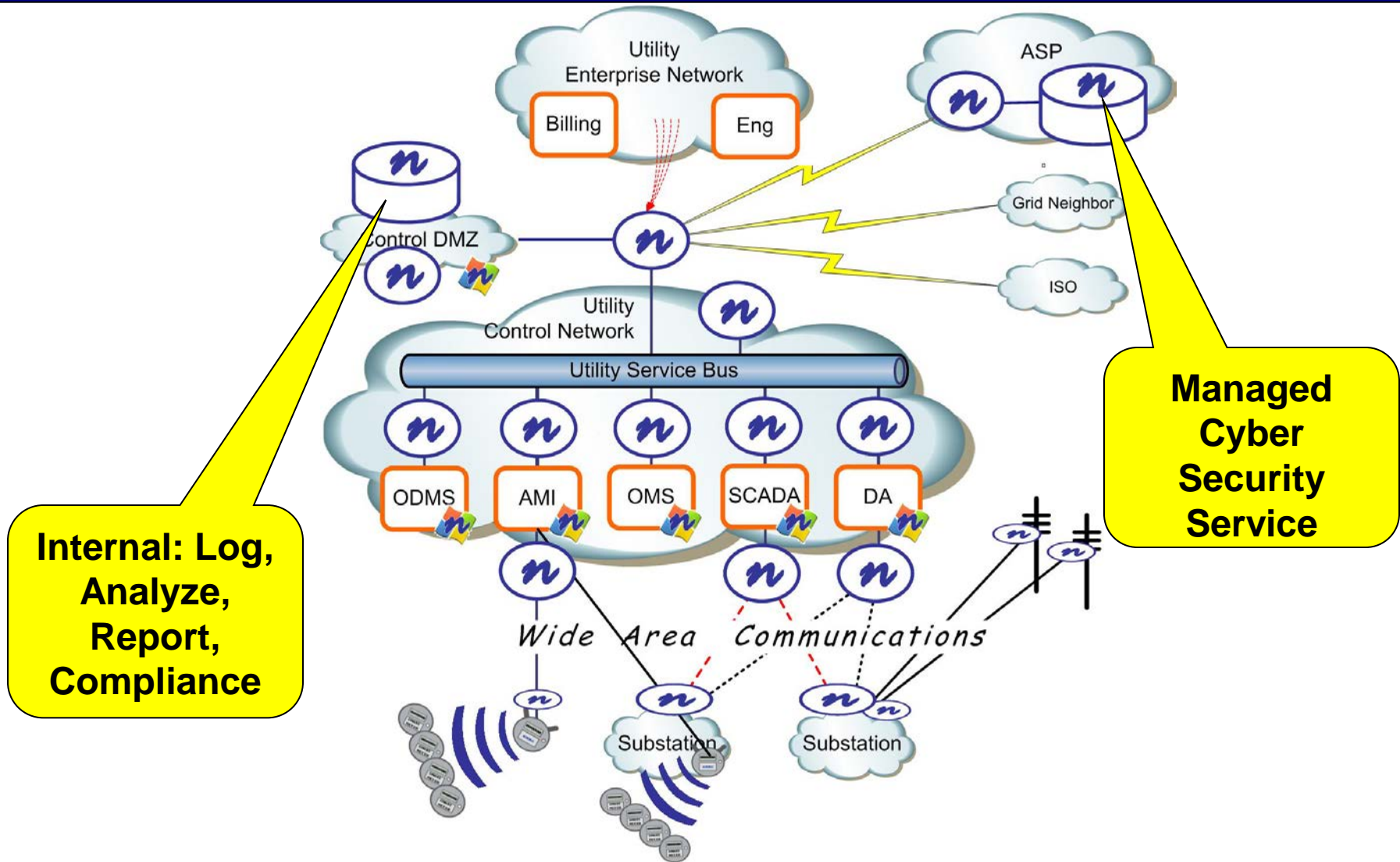
Interior Defense-in-Depth



Communications Defense-in-Depth



Log and Event Management



Internal vs. Managed Service

- Decision Criteria
 - level of internal cyber security expertise
 - installation, integration, configuration
 - tuning
 - updating signatures
 - analyzing events
 - responding to events
 - appetite for 7x24 monitoring and response
 - requirements for reporting



Managed Cyber Security Service



HD Supply / N-Dimension Managed Cyber Security Svc

- n-Platform UTM monitors utility network
 - IDS
 - port scan, vulnerability scan, firewall
- Event & log data pushed to managed n-Central
 - strict isolation between data of different companies
- Utility has full access to all data via Web
 - all access over VPN
 - service cannot control any system at utility, even if service is compromised

Cyber Security Service Description

- Based on term agreement with each participating Utility
- Pricing is for all elements of the service including:
 - Initial design
 - Hardware / software installation, maintenance, updates
 - 24x7x365 Cyber Security Monitoring
 - Level 1, 2 and 3 customer support
 - Secure Utility Web Portal for access to reports and logs
- Add-on capabilities within term
 - AMI
 - additional substations

Its All About Reliability

- Grid Reliability
- Utility Reliability
 - Operations
 - Finance



August 14 2003

A photograph of several high-voltage power line towers silhouetted against a bright orange and yellow sunset sky. The towers are arranged in a line, receding into the distance. The sky transitions from a deep orange near the horizon to a pale blue at the top.

andrew.wright@n-dimension.com

Cyber Security for the Smart Grid™



N-Dimension Product Solutions

n-Platform UTM Capabilities

Monitoring Option Pack

- SCADA IDS
- Port Scanner
- Vulnerability Scanner
- System & Service Monitors
- Static Routing
- Admin Firewall
- NTP Server
- SCADA Integration
- VLAN Support
- Logging & Reporting
- Email & Pager Alerting
- LDAP and AD Interface

Gateway Option Pack Monitoring Option Pack +:

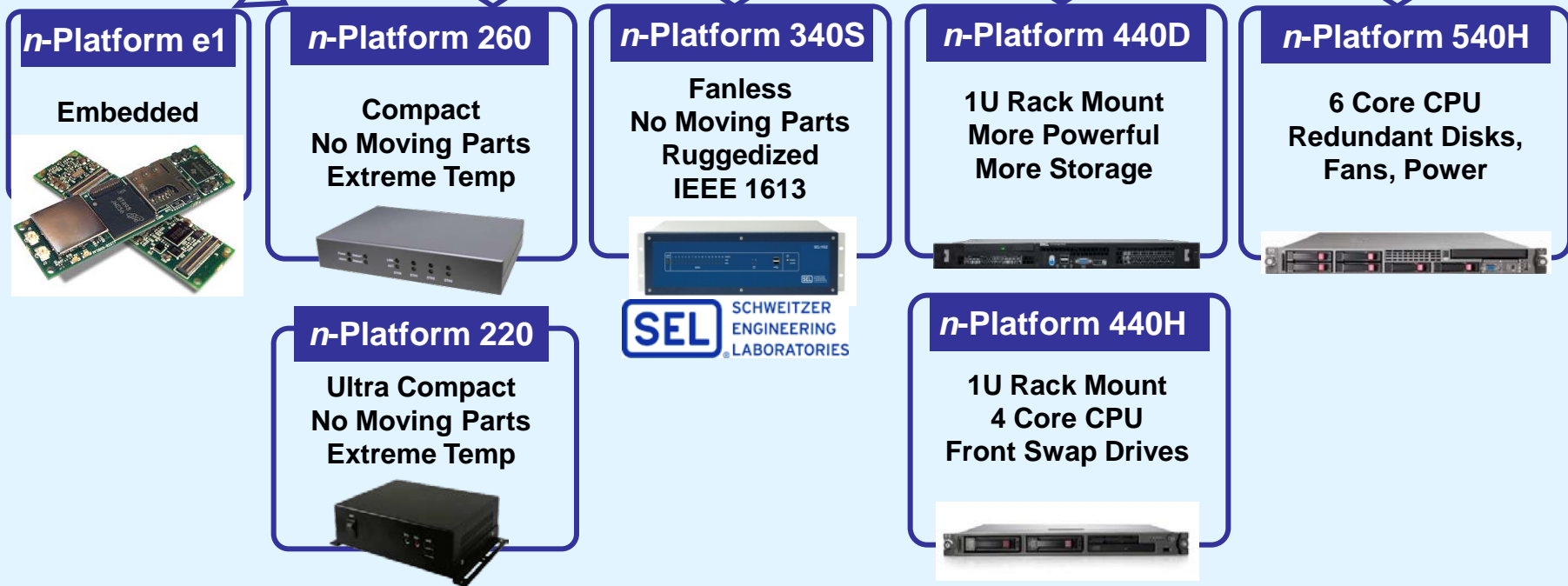
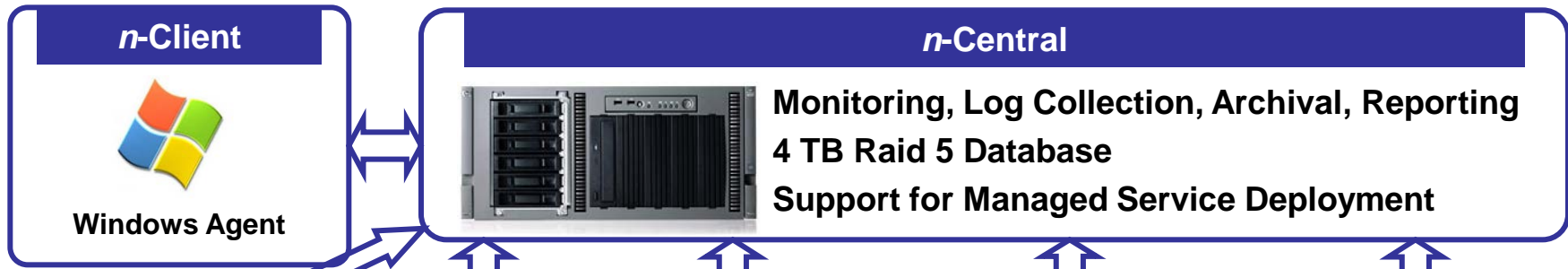
- Stateful Firewall with NAT
- Site-to-site IPSEC VPN *
- Site-to-site SSL VPN
- Remote access IPSEC VPN *
- Remote access PPTP VPN
- SCADA VPN
- Network Access Control
- Device Anti-virus
- Anti-virus with Proxy Server
- Proxy server
- DHCP server
- Google 2 factor authentication

HA Option Pack Gateway Option Pack +:

- High Availability
Active – Standby Mode

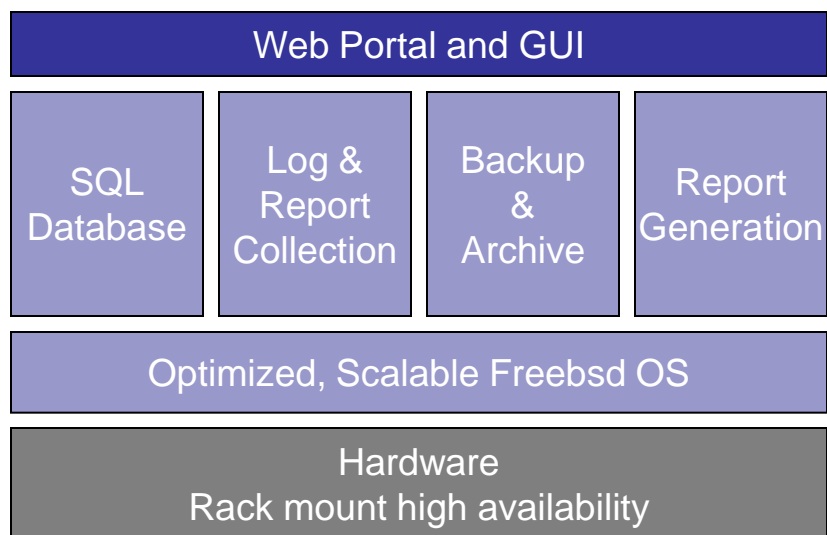
** Successfully tested in US DOE Lemnos Interoperable Security Program*

N-Dimension Product Form Factors



Unified Threat Management (UTM) Systems

n-Central Event and Log Manager



A high-performance high-capacity management system designed to store years of event & log data

- Comprehensive log & event data
- GUI-based query
- Forensic analysis
- Report generation
- NERC-CIP compliance reporting
- Partitioning for Managed Service
- Emphasis on “ease of use”