Exelon Smart Grid Multi-Service Communications Architecture

Doug McGinnis

4/5/13

Exelon

Smart Grid (Generation 1)

Grid Automation is not a new concept

- SCADA/AMR functions have been around for years

Smart Grid is the embodiment and convergence of a standardized framework

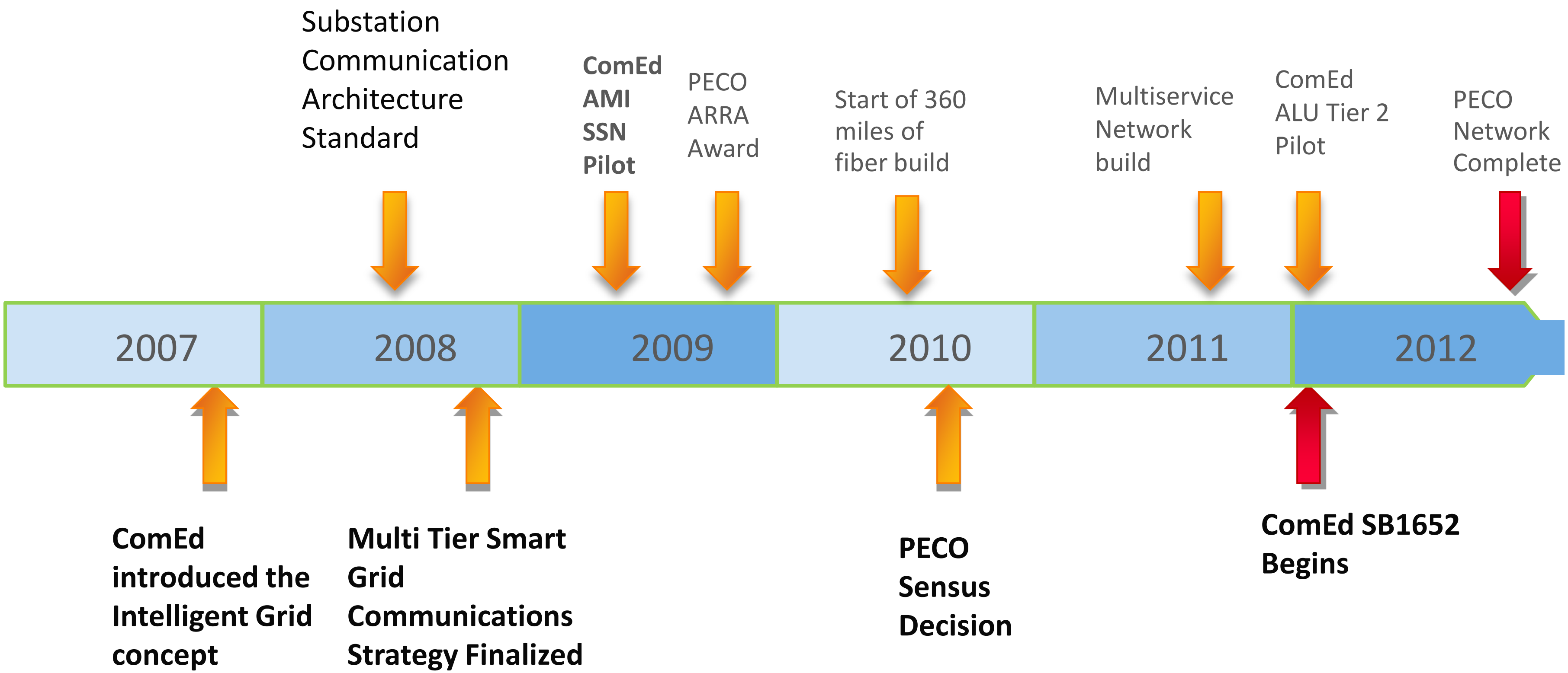
- Emerging standards driving standardization of technology
- Focused attention on grid modernization

Application requirements will drive communications technologies to their current limits

- RF technologies will be the limiting factor driven by spectrum availability

Exelon.

Smart Grid Journey



3

Exelon.

Smart Grid Communications Strategy

Bus Req
- Define Business Requirements
- What is the problem to be solved?
- How Many? How fast? How reliable?

Strategy
- Define a vision
- Define fundamental design principles/guiding principles
- Define an architecture

Standards
- Define detailed design standards
- Identify technologies

Do it
- Implementation Projects
- Support Structure

Communication Design Principles

Security

- Robust end-to-end, aligned with industry best practices aligned to NISTIR 7628 and future version of NERC CIP requirements

Converged Communications

- Smart Grid applications will share a converged shared communications infrastructure but will be logically isolated (tunneled)

Interoperable

- Industry standard open protocols will be utilized preferentially end-to-end. IP preferred
- Avoid use of proprietary protocols

Privately owned communications

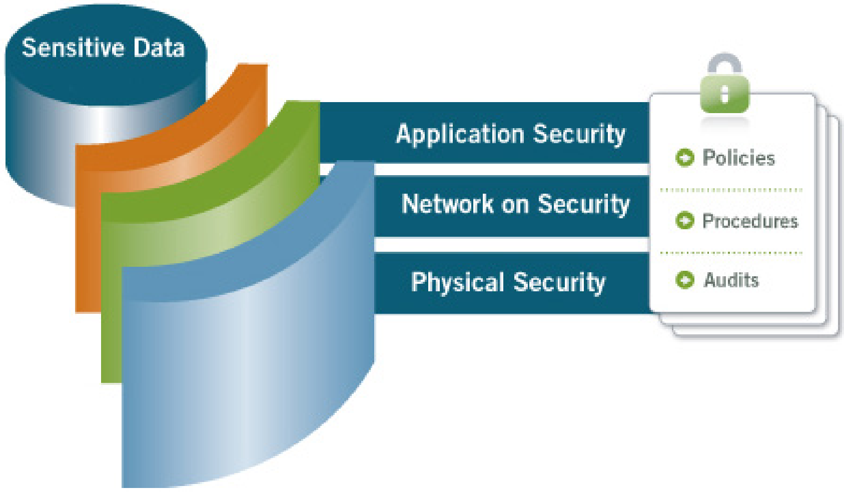
- privately owned communications enables Exelon to maintain governance and control over all aspects of the technology.

No Unanalyzed Single Points of Failure (Self Healing)

- Consistent with the deterministic philosophy, failure modes and backup schemes shall be incorporated to form a “self healing” architecture. Communications

Security Processes – Defense In Depth

- PECO has implemented a layered defense-in-depth strategy incorporating physical, platform, network and application elements including but not limited to:
  - SGSM network protection via firewall, VPN, and NIDS components
  - Network components and NIDS deployed with SEIM elements of logging, monitoring, alerting, notification (LMAN)
- Security monitoring and incident management deployed within AMI & DA field networks via the SGSM Command Center and PECO's cyber security operations
- End to end encrypted communications



Defense-in-Depth Overview - CIA

Defense-in-depth approach requires that relationships between network resources and network users be implemented within a controlled, scalable, and granular system of permissions and access controls that goes beyond simple network segmentation:

Security monitoring and incident management activities across SGSM

Implemented layers of security controls to authenticate network devices and users accessing SGSM information systems

Firewalls with stateful packet inspection and intrusion detection technologies

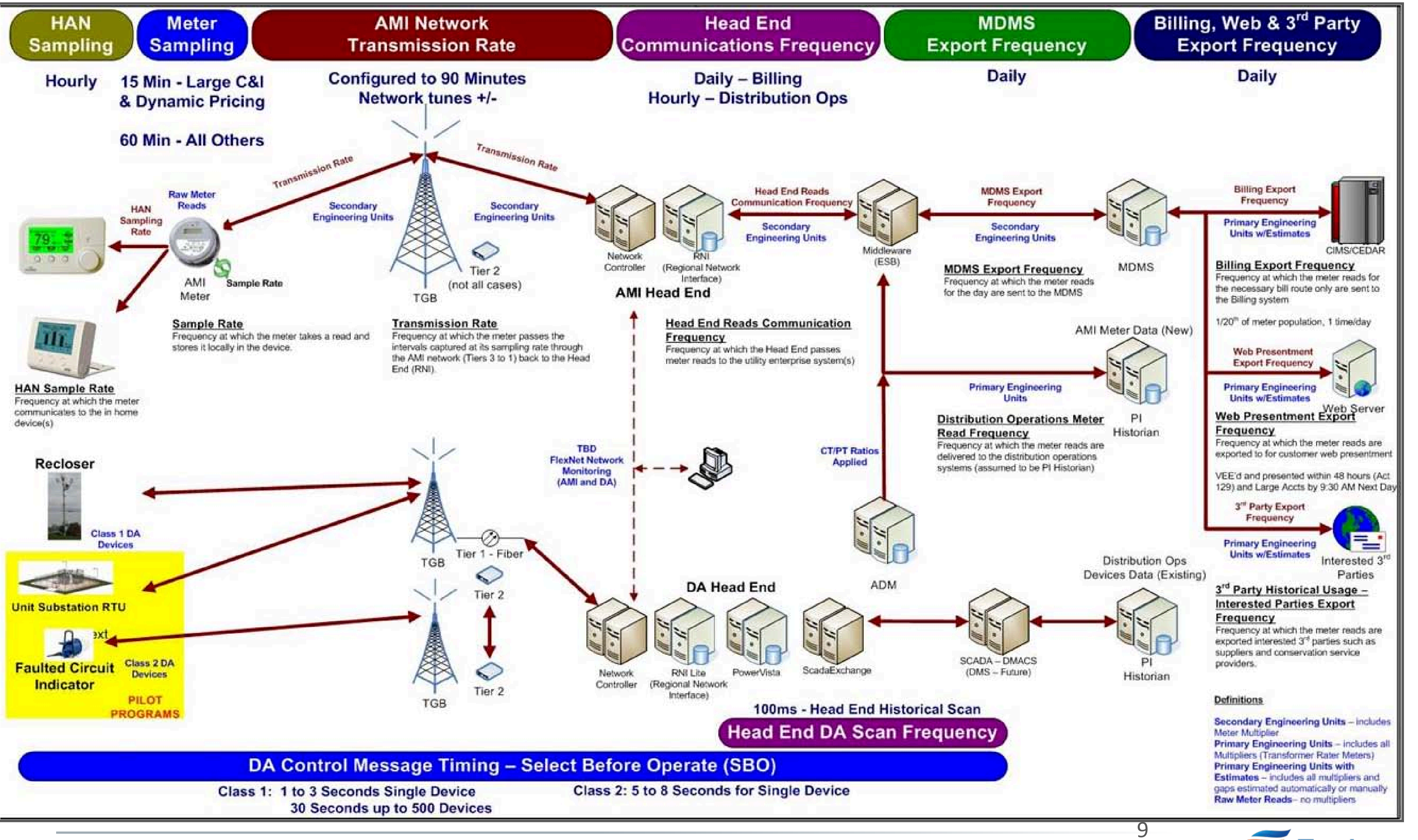
Implement encryption throughout the network to ensure confidentiality and integrity

Multi-service architecture consisting of multiple application and network-layer services utilizing a common transport medium while maintaining appropriate separation within common communications backhaul elements (e.g., frequency and physical separation of AMI & DA transceivers, self-healing network elements, etc.)

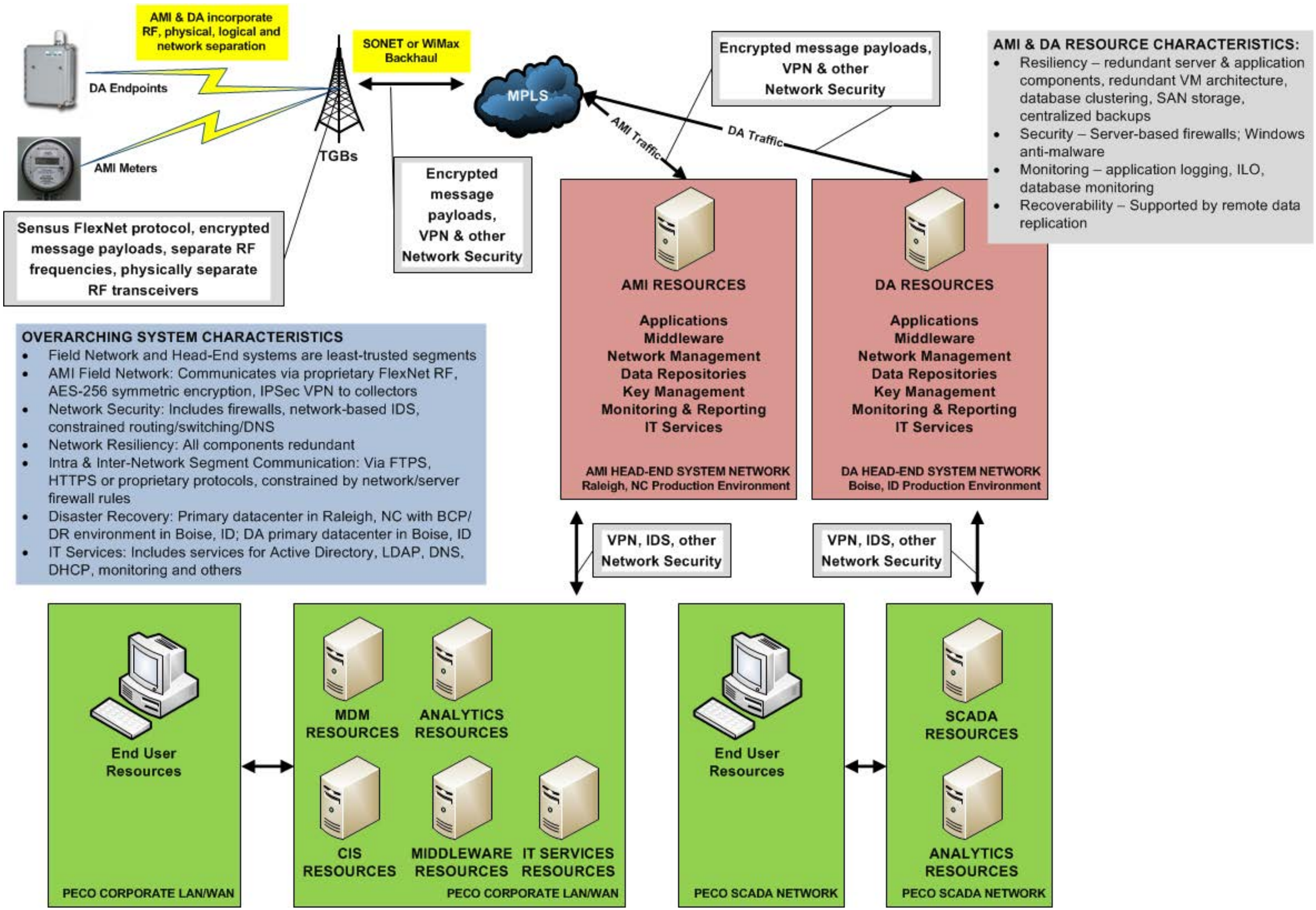
Risk Management

- Activities to direct and control security risk management within the SGSM Program. Security control selection is dependent upon organizational decisions based on criteria for risk acceptance, treatment options, and the general risk management approach applied throughout the CSMS
- Performed initial security assessments and risk-based go/no-go decisions prior to large scale deployments.
- Common business and IT-based controls analyzed, gaps identified and corrective actions taken:
  - Gaps were identified in areas including vendor management, security monitoring, incident management, field network OTA firmware update, and encryption management
  - Issues/Risks have been analyzed for root-cause, remediation plans developed, and corrective actions implemented. SGSM risks and issues are tracked to closure via HPQC
- Implemented Intrusion Detection System (IDS) in accordance with original design specifications
- Established the SGSM Security Council (SSC), integrated within the broader SGSM Program risk management model, to assess security risks and render decisions based on the cyber security plan, relevant standards and best practices, and business/operational priorities

Functional AMI & DA Architecture



Defense-in-Depth - Architecture



Multi-Service Communications Architecture Emerges

Requirements

- Examining Business & Application Requirements
- Substation communications architecture must consider the Smart Grid and map to the Smart Grid strategy and associated application portfolio
- The architecture must enable the elimination of legacy communications infrastructure and be scalable to accommodate future growth

Convergence & Alignment

- Emerging Smart Grid applications will share a common transport
- Current architecture relies on legacy communications infrastructure that performs poorly, is not monitored and lacks Carrier SLA's

Architecture Framework

- Multi-service communication infrastructure aligned with current technology offerings

Exelon

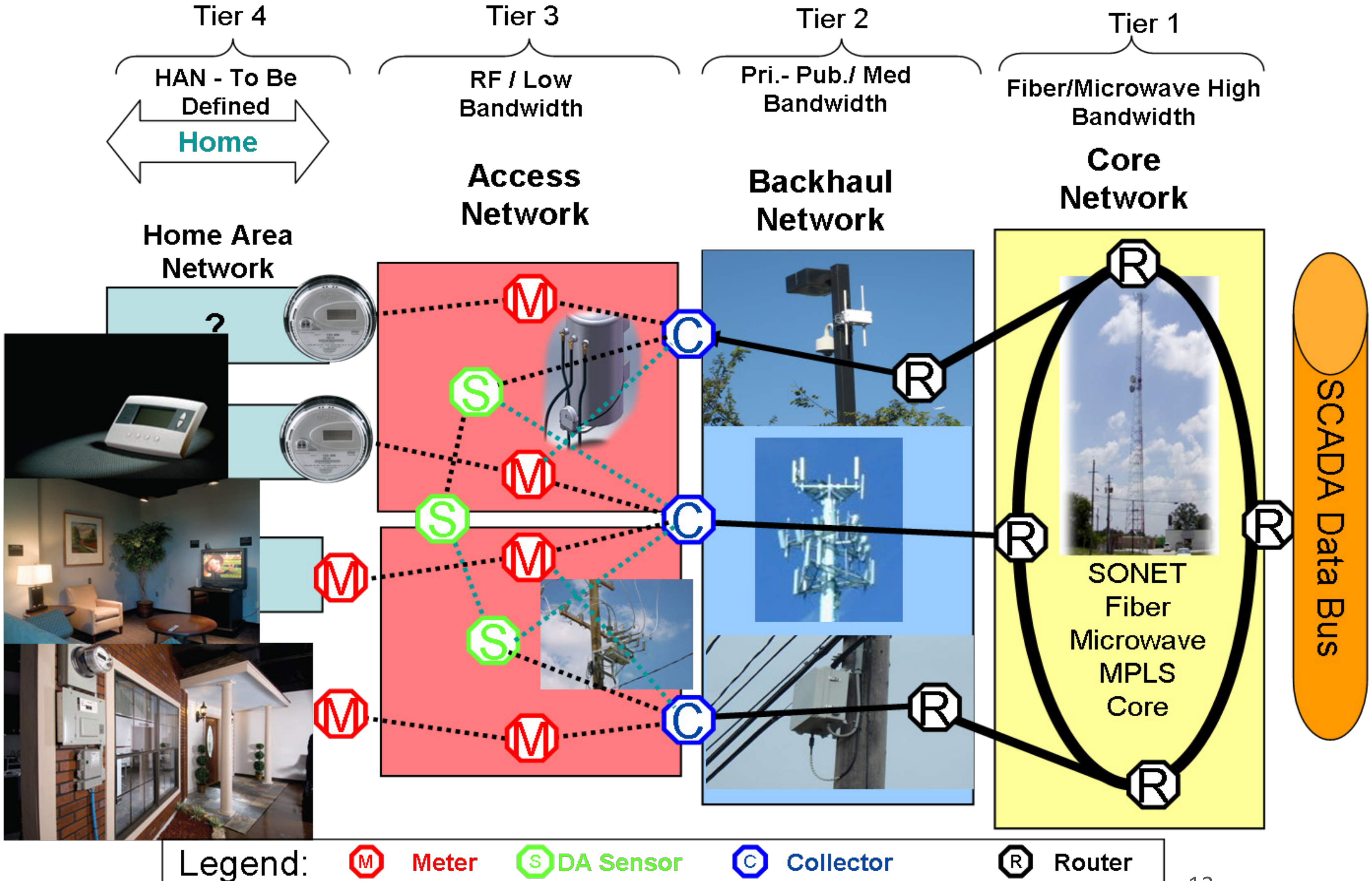
Multi-Tiered Transport Technologies

Tier 3
- Field Area Network
- Low Bandwidth RF
- End Point Device Communication

Tier 2
- Backhaul
- Medium Bandwidth
- WiMax/LTE

Tier 1
- Core Network Backbone
- High Bandwidth
- Fiber/SONET

Smart Grid Communication Tiers



Exelon.

Architectural Multiservice Framework

Substation Service Portfolio – 7 application groups have been identified

- Telemetry – RTU/IED communications
- NERC CIP Telemetry – Telemetry from CCA devices
- Distribution Automation Telemetry
- Enterprise – Business applications (email, VoIP, video)
- Security – Surveillance Video & card readers
- AMI Tier 2 interface to Core Backbone PoP
- Management – Network Management traffic

1 to 5 MB/Sec (depending video rates)

Substation Communications Architecture

Substation LAN

- Access switch built into the 7705 – VLAN mapped to individual LSP
- No inter-application or inter-service routing is permitted
- RTU access/authentication will be through SCADA core (hairpin over enterprise service)
- AMI & DA AP's and other substation IP devices will be partitioned in their respective VLAN's

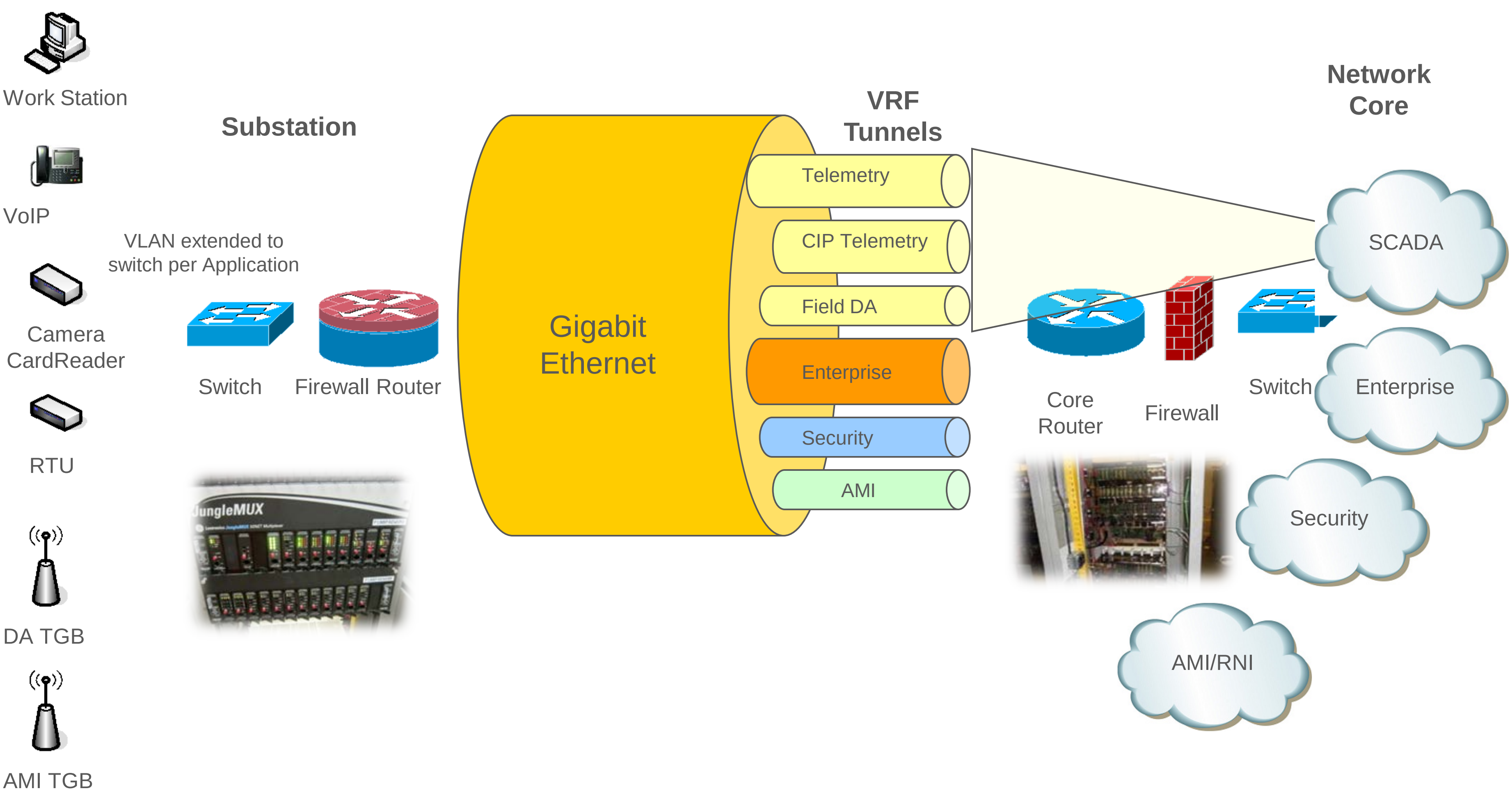
Substation WAN

- Router (layer 3) will interface with MPLS Label Switched Path (LSP)
- 7 LSP VPRN tunnels will be created for logical separation
- RTU telemetry will be encrypted end-to-end
- IP addressing schema will be defined for entire substation population

Relay Protection Teleprotection

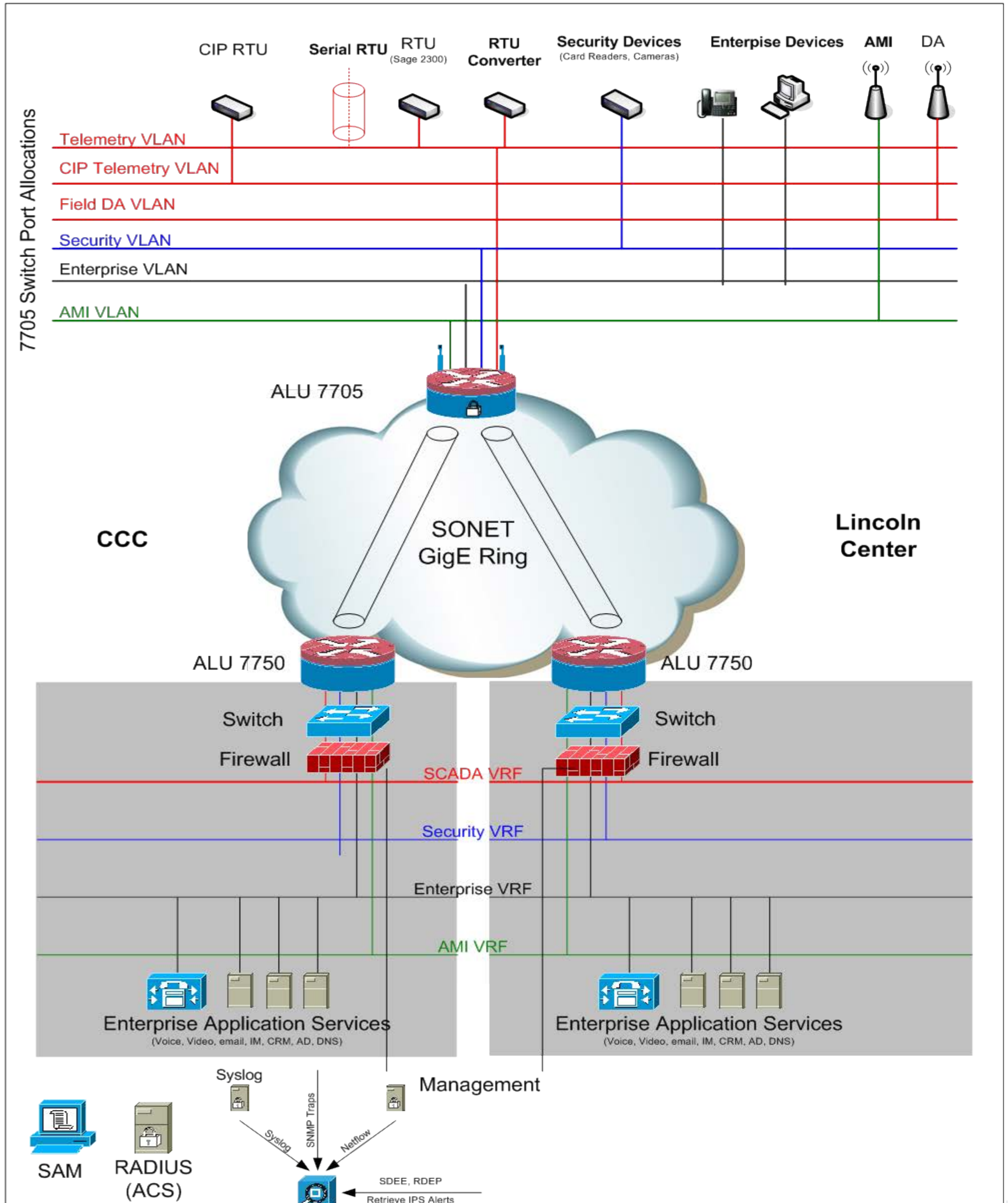
- Will not interact with Ethernet Services (no IP)
- Prefer fiber based communications
- Combination of direct on fiber relay channels & SONET based communications
- Dual counter rotating SONET loops

Substation LAN – WAN Architecture

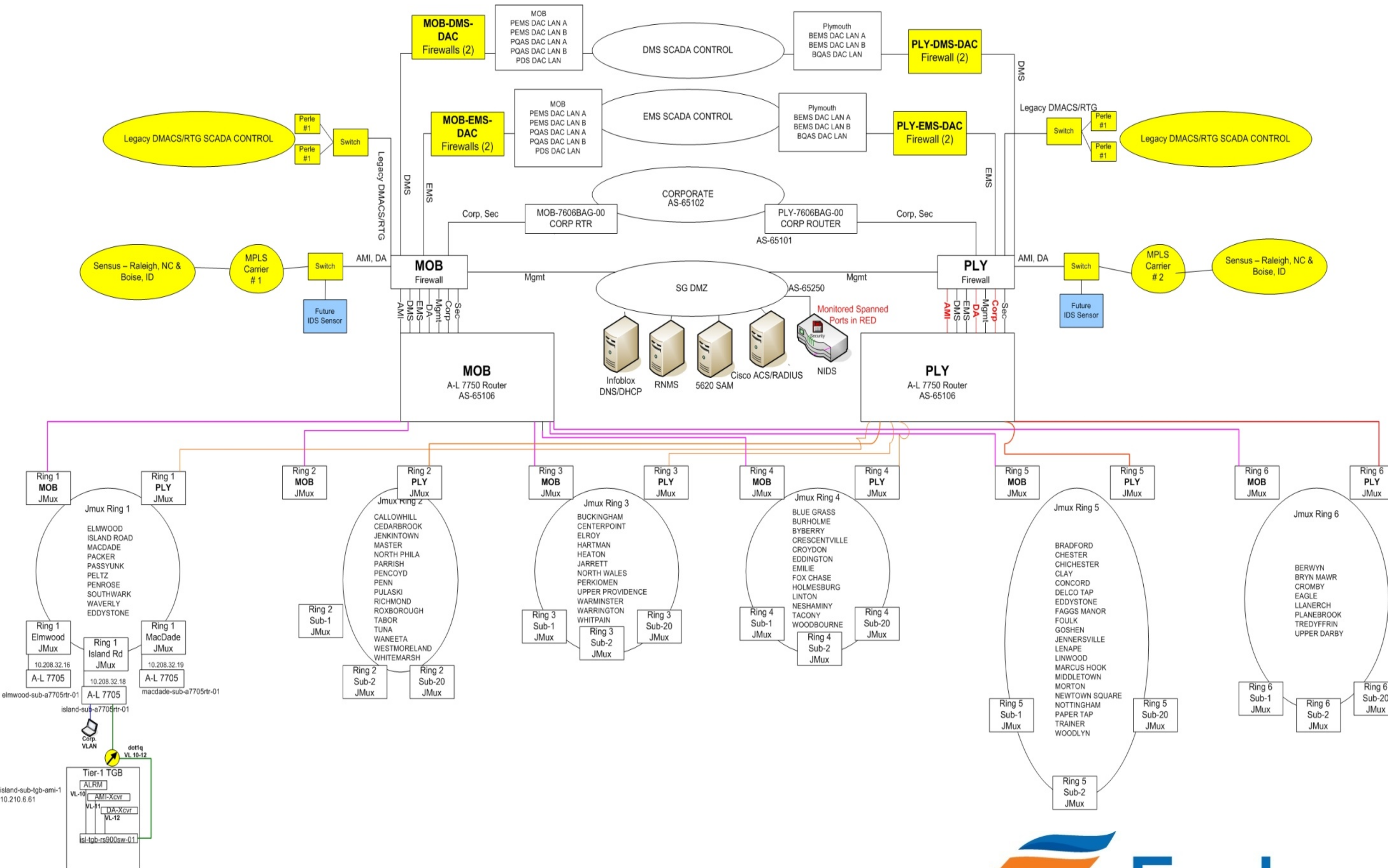


Ethernet based devices

Substation Logical Architecture

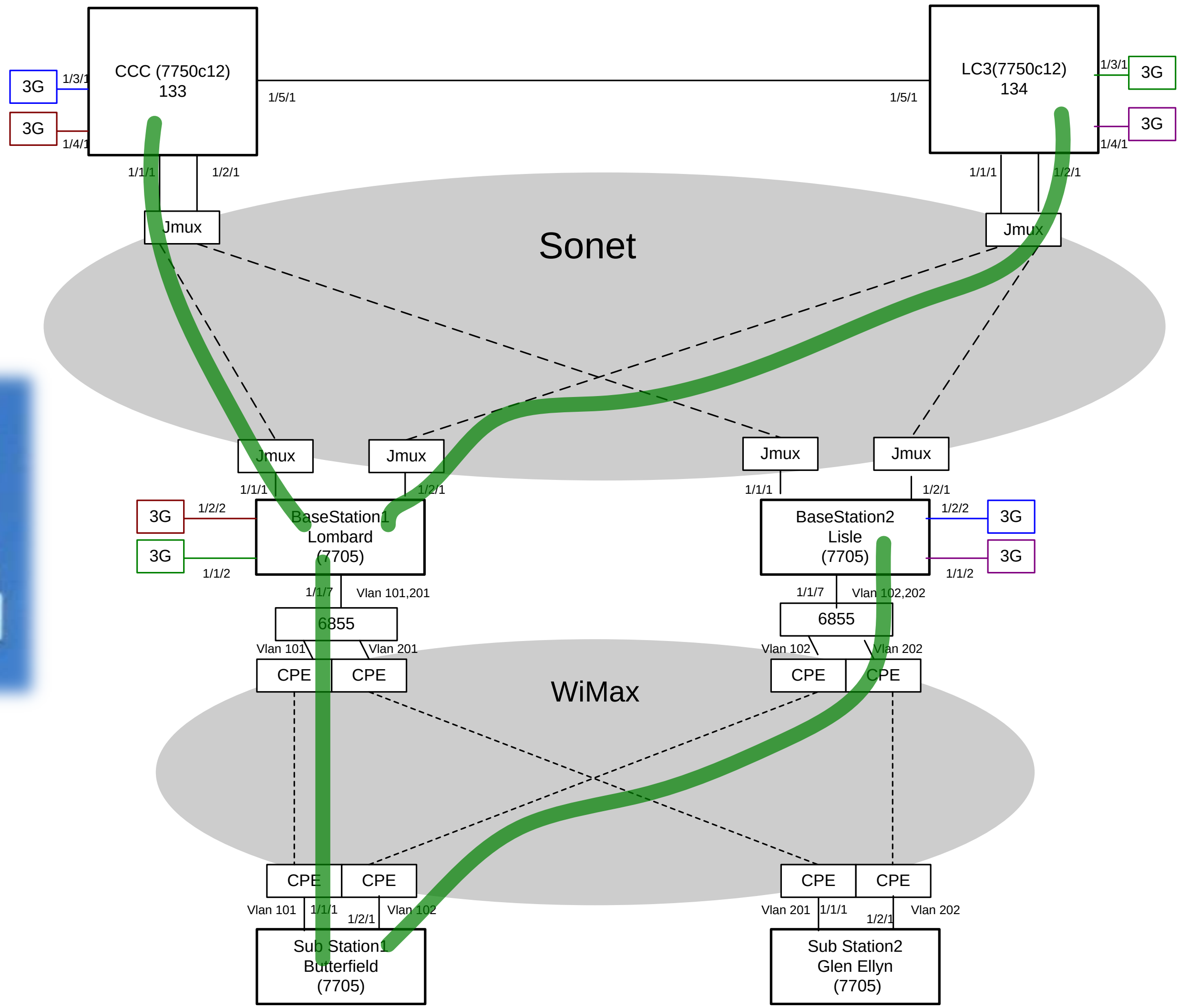


PECO High level Network Design

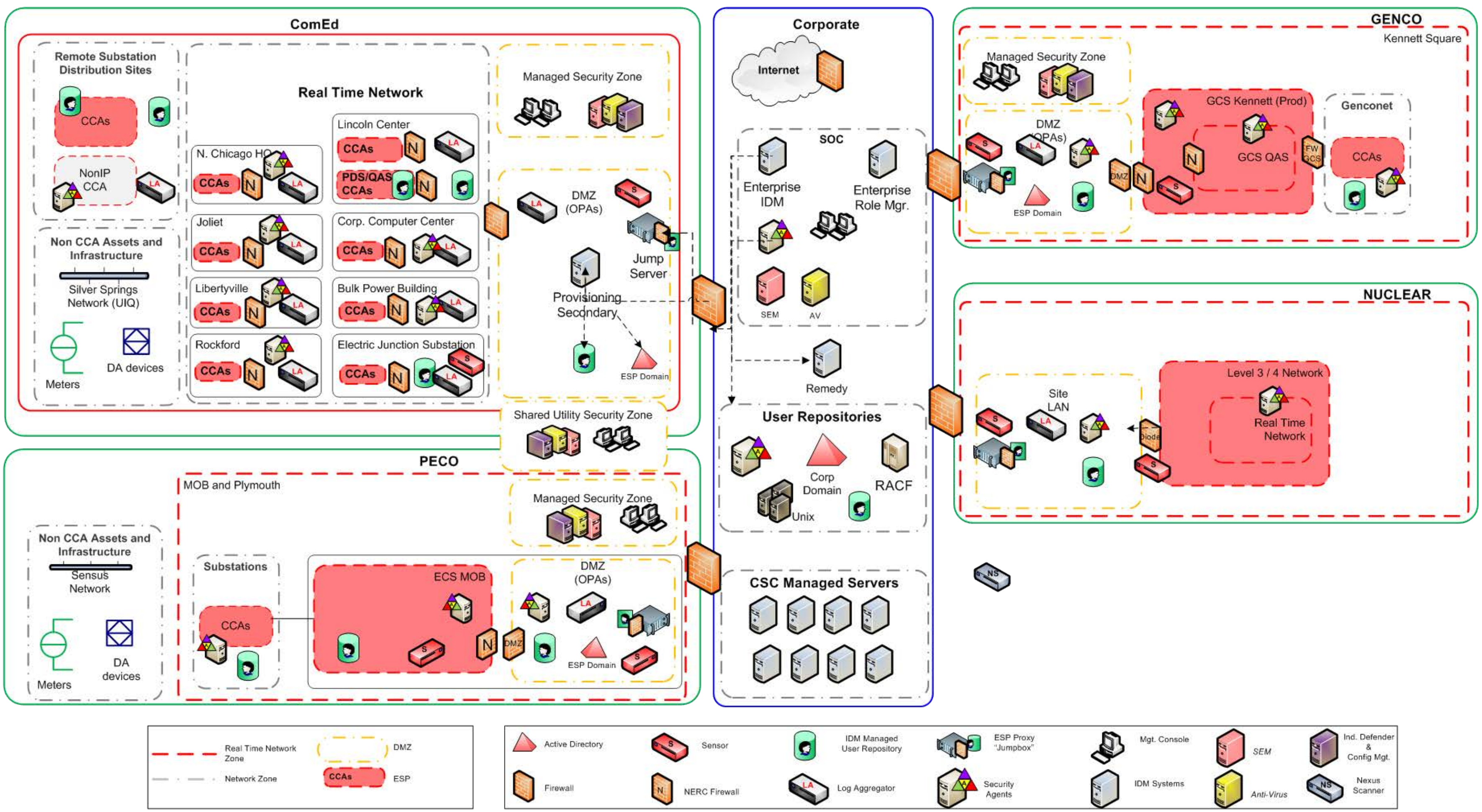


Exelon®

WiMax Failover Redundancy



Security Architecture



Tier 2 Backhaul Architecture

Bridge the FAN with Tier 1

- AMI backhaul
- Distribution Automation – Field Devices
- Substation Telemetry – Eliminate Public Carrier circuits
- Voice/Video (~1Mbps per video stream)

Application Traffic Considerations

- Bandwidth consumption (5-20Mbps)
- Latency sensitivity (QoS tagging)
- Security (PKI)
- Logical separation & provisioning of applications (VLAN tagging)

WiMax Technology – 3.65 GHz Spectrum (802.16.e)

- Multi-sectored base stations (10Mbps)
- Supports application provisioning – 802.1q tagging & QoS
- Good propagation distance 3-5 miles up to 10 miles

Substation IP Enablement

IP/Ethernet to support legacy & new technology for Smart Grid application protocols and

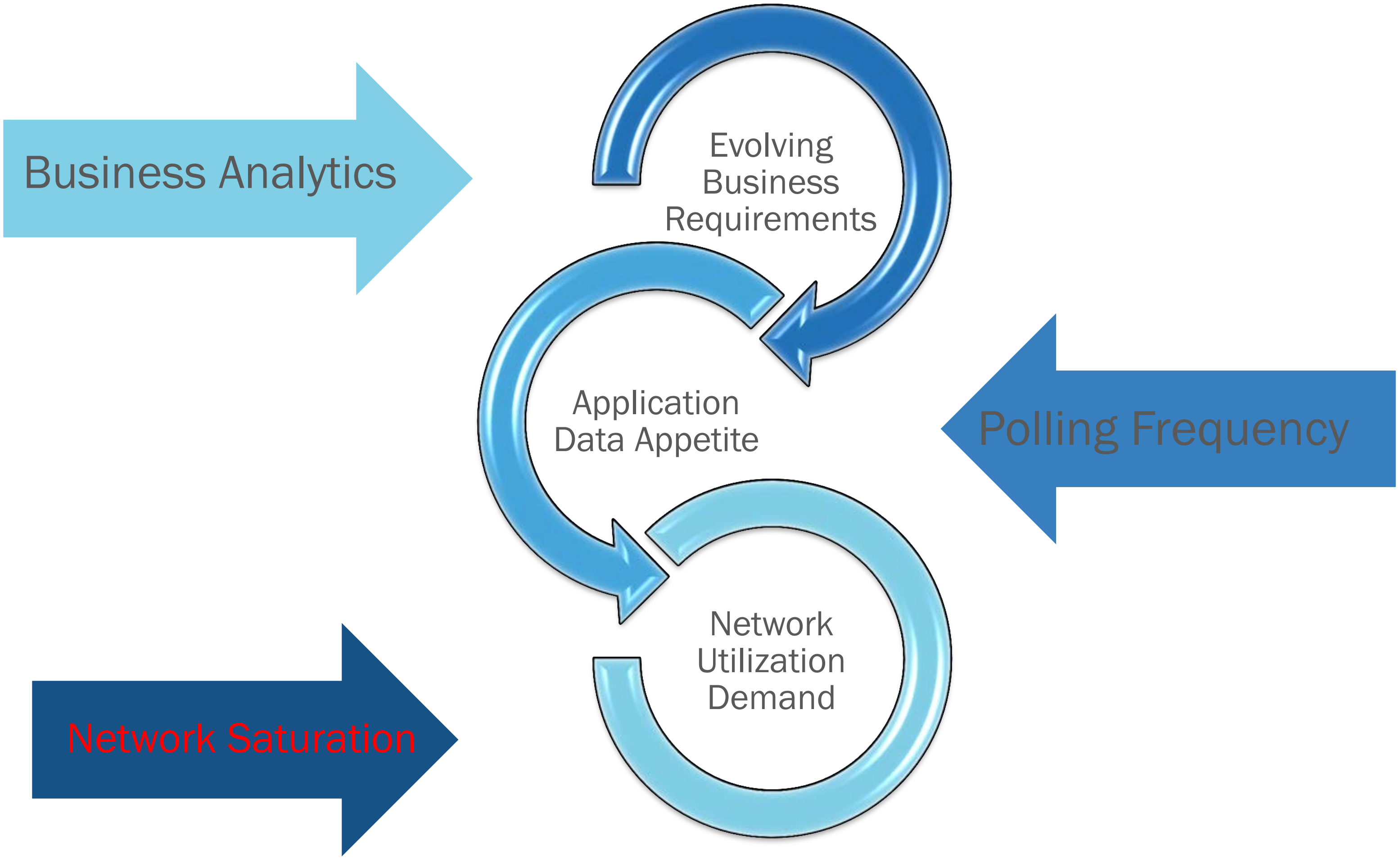
Migrate legacy serial based devices to IP/Ethernet

- IP emulate serial TDM communications
- Alternatively provision serial TDM circuits over new SONET infrastructure when IP/Ethernet not viable

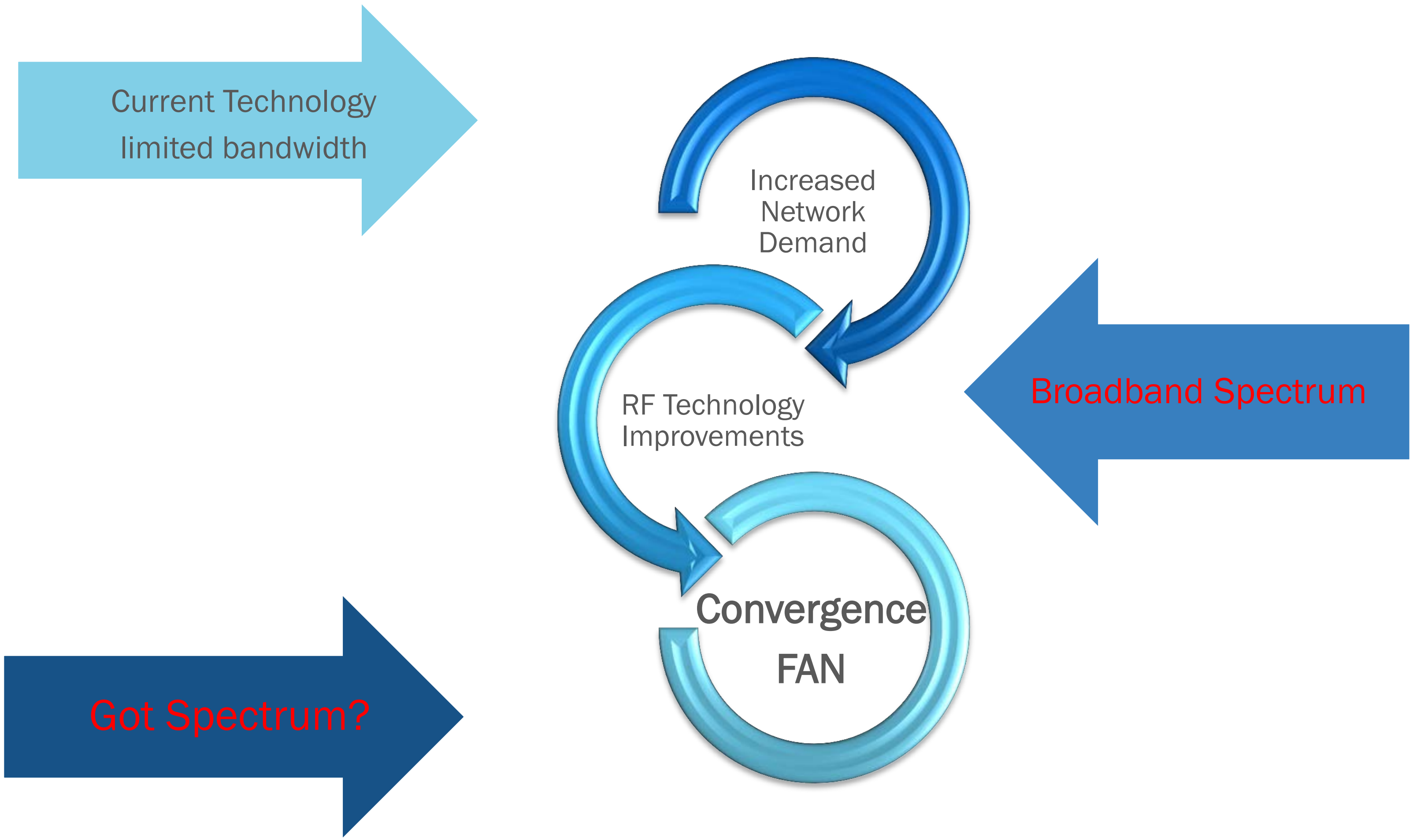
Remove legacy ATT & Verizon communications circuits

22

Smart Grid Evolution



Smart Grid G2



Spectrum

Broadband Spectrum critical to the future of the Smart Grid 10-20MHz would be nice

- Existing technology will saturate in time
- Impose application evolution limitations

Broadband not readily available to Utilities

- Competing with Carriers in auctions not likely
- Priced outside of Utility budgets

Creative Alignments – Assistance not likely from FCC/NTIA

- Public Safety 700MHz sharing arrangements
- Buying smaller blocks
- Sharing with government agencies (DOE/DOD under NTIA control)
- What else?

Questions?

Technology Details

Multi Protocol Label Switching (MPLS)

- The various types of MPLS-based VPNs can be classified in a number of ways. This is either a layer 2 or a layer 3 point-to-point service or multipoint service. This results in the following interesting VPN types:
  - Layer 3 multipoint VPNs; referred to as Virtual Private Routed Networks (VPRNs)
  - Layer 2 multipoint VPNs, or VPLSs is a layer 2 multipoint VPN that allows multiple sites to be connected in a single bridged domain over a managed IP/MPLS network. All substations in a VPLS instance appear to be on the same LAN network. VPLS uses an Ethernet interface and allows flexible service provisioning.
- Label Switched Paths (LSP); Tunnel defining the packet path over label switched routers
- Rsource Reservation Protocol (RSVP); is a Transport Layer protocol designed to reserve resources across a network to support integrated services

Spectrum Evaluation

	Frequencies					
Requirements	700Mhz	900Mhz	2.3Ghz	3.65GHZ	5.8Ghz	6-11Ghz
Risk	High	High	High	Medium	Low	Low
Cost	Low	Low	High	Low	Low	High
Coverage	Excellent	Adequate	Good	Good	Good	Excellent
Equipment Availability	Limited	Good	Growing	Growing	Good	Good
Licensed	√	√	√	No	No	√
Unlicensed	No	√	No	√	√	No
Lightly	No	No	No	√	No	No
Availability – PECO area	√	√	√	√	√	√
Point-to-Point	No	No	No	No	√	√
Point-to-Multi Point	√	√	√	√	No	No
Overall Ranking	**2**	**6**	**5**	**1**	**3**	**4**

Ranking: 1 high - 6 low