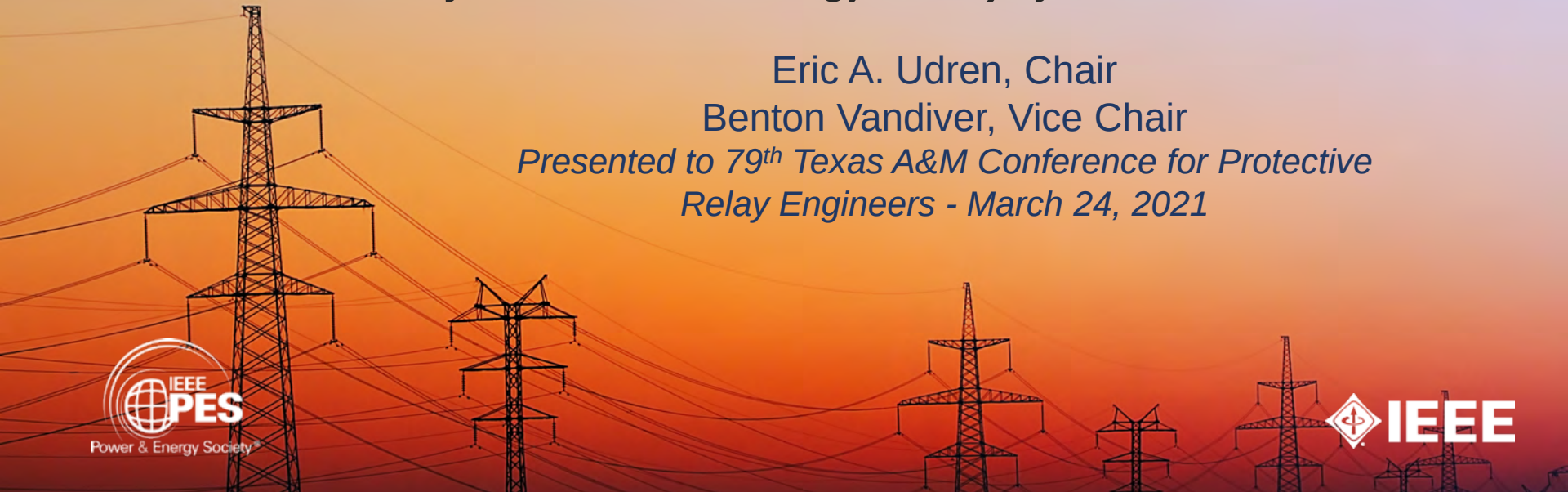
Application of Ethernet Networking Devices Used for Protection and Control Applications in Electric Power Substations

Report of Working Group P6 of the Power System Communications and Cybersecurity Committee of the Power and Energy Society of IEEE

Eric A. Udren, Chair
Benton Vandiver, Vice Chair

Presented to 79th Texas A&M Conference for Protective Relay Engineers - March 24, 2021



WG membership

PSRC WG H12 moved to PSCC P6 in PES Reorg. Membership of H12 & P6 when report was approved:

Eric A. Udren, Chair

Benton Vandiver, Vice Chair

Jay Anderson
Philip Beaumont
Fernando Calero
Bill Dickerson
Didier Giarratano
Anthony Johnson
Aaron Martin
Charles Sufana
Galina Antonova
Robert Beresh
Christopher Chelmecki
Michael Dood
Roman Graf
Marc LaCroix
Roger E. Ray
John T. Tengdin
Alex Apostolov
Christoph Brunner
Thomas Dahlin
Herbert Falk
Christopher Huntley
Deepak Maragal
Veselin Skendzic

Report Table of Contents

Introduction - Purpose

Section 1 - The report describes engineering of Ethernet for use in protection and control:

- The basic purposes, functionality, and application guidelines for Ethernet communications devices in substation local-area networks (LANs) and utility operational wide-area networks (WANs).
- Architecture and configuration of connections of the LAN for security, dependability, and maintainability.
- Settings or programmed configuration of switches and routers to control traffic flow to meet the required security and dependability.
    - Like setting relays - requires the same organizational control processes.
- *Key differences from IT networks – IT & PC experts need cross-training.*

Section 2 - Overview

- IEC 61850 GOOSE for high-speed tripping and status over network – example of wiring reduction use, but not the only one.
  - IEC 61850 MMS, Sampled Values, DNP3, C37.118.2 synchrophasors, vendor specific protocols in packet format.
- Optical links carry almost unlimited signals and messaging in flexible dynamic mix of packets.
- Role of *Ethernet switches* in directing traffic around LAN
- Role of *Ethernet routers* for interfacing LAN with enterprise operational or integrated WAN, with isolation and security.
  - Connect to SONET TDM or to wide-area all-Ethernet (WAN).

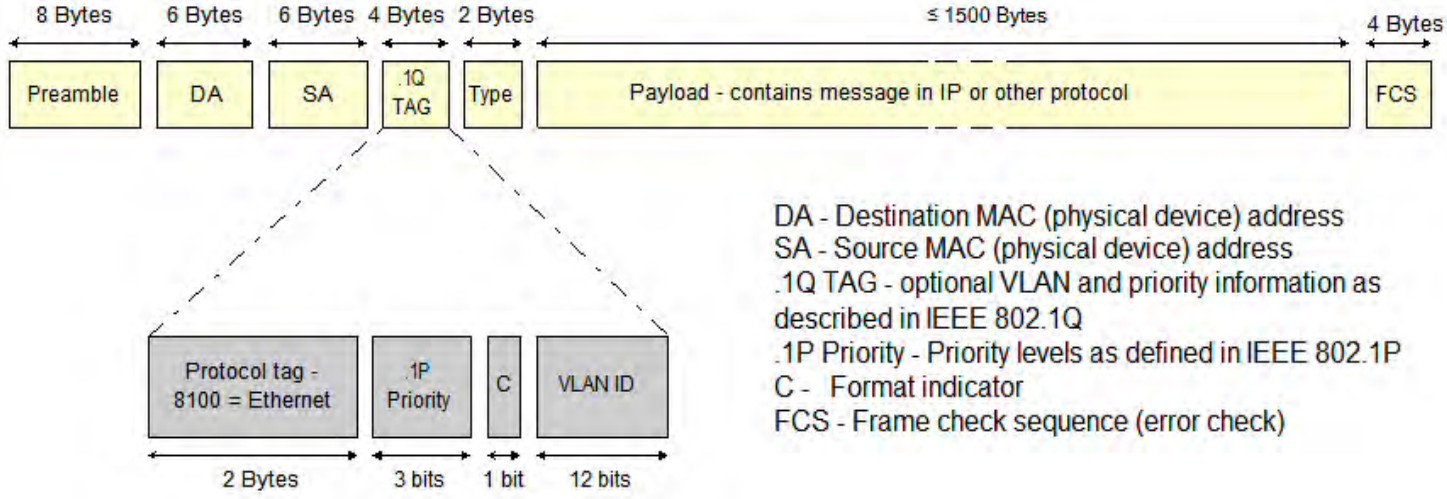
OSI 7-layer communications model

Data fields in packets tell switches and routers how to handle them

Layer	Name	Function	Typical Usage (Device or Software)	Examples
7	Application	Meaning of the data (utility user specifics)	Application Programs	HTTP, FTP, NTP, PTP, SNMP, MMS
6	Presentation	Building blocks of data and encryption for security	O/S Ethernet Stack	JPEG, ASCII, HTML, Encryption
5	Session	Opening and closing specific communications paths	O/S Ethernet Stack	RPC, NETBIOS
4	Transport	Error checking	O/S Ethernet Stack	TCP, UDP
3	Network	Determining the data paths within the network	Router, L3 Switch	IP
2	Data Link	Data transmission, source & destination, checksum	Switch	Ethernet, ATM, PPP, Token Ring
1	Physical	Signal levels, connections, wires, fiber, wireless	Media Access Controller, Repeater	10Base-T, 100Base-FX

Ethernet message frames or packets – Section 3

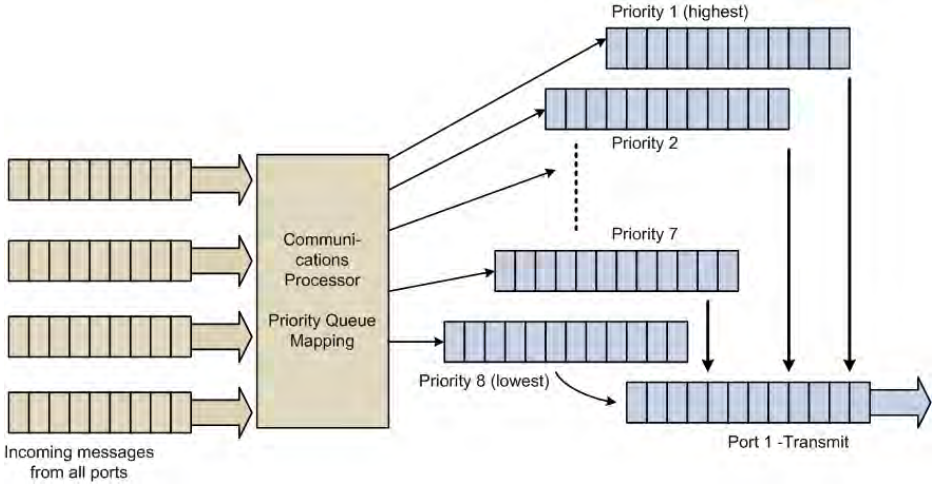
- Media access control (MAC) addresses are for networked devices in Layer 2.
- IP address is in Layer 3 IP payload (IPv4; or IPv6 has a lot more addresses).



Priority tag

Tells switches & IEDs which packets are most urgent – 8 levels

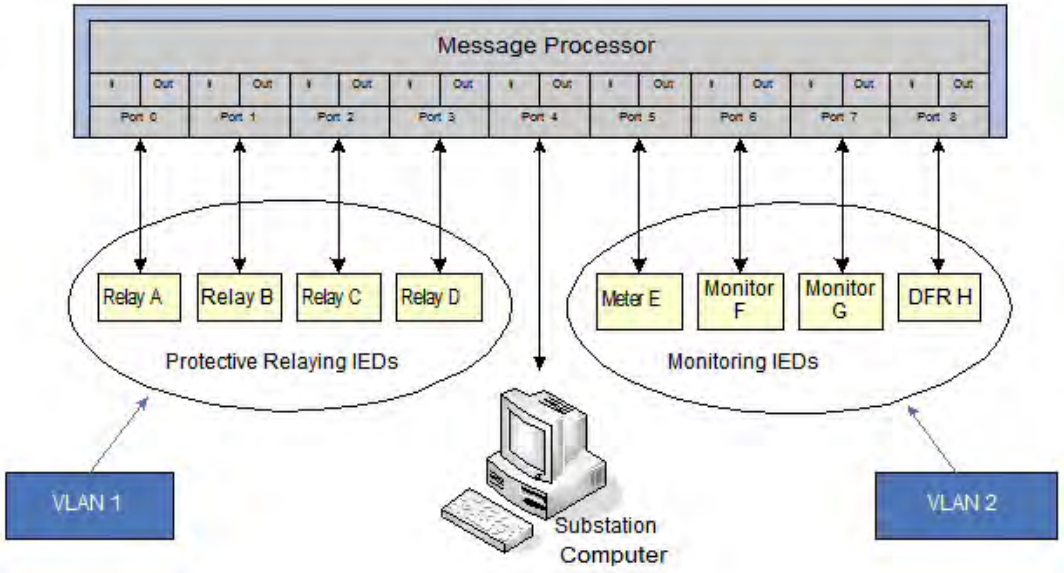
- Highest priority goes into queue next.
  - Note that big outgoing packet must finish first.
- Top priority – critical network management and timing.
- Next priority – IEC 61850 GOOSE or Sampled Values
- Remainder sorted at lower levels.



VLAN (Virtual LAN) tag

Tells switches & IEDs how to segregate groups of packets on a LAN

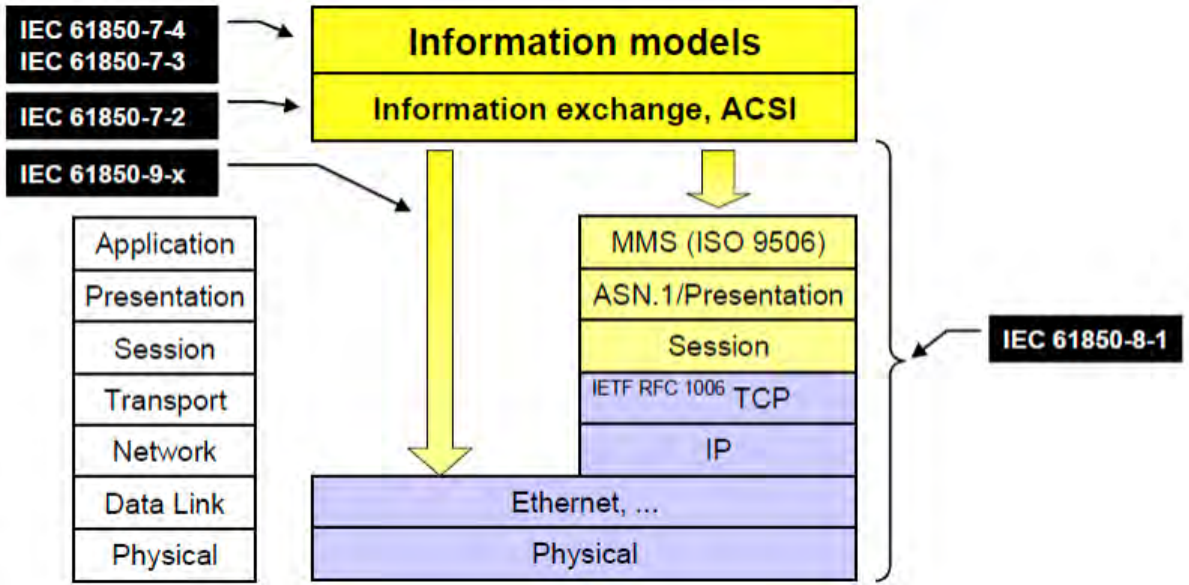
- Tool to isolate some types of traffic to certain regions of the substation LAN.
- Control traffic volume on each link.
- Any shared paths among VLAN packets are subject to traffic volume of all VLANs; failure impacts all VLANs.
- Up to 2^{12} VLANs available.
- Check handling of VLAN 1.



IEC 61850 service mappings to OSI layers

Need speed? Seven layers add processing delay.

- GOOSE – milliseconds or less – Packets on a LAN – Layers 1 & 2 only.
- More layers - TCP/IP (Layers 3 & 4) and above – slower.



TCP versus UDP

TCP

- Requests retransmission for errors.
- Only for a single receiving application.
- Slows down exchange by repetition to ensure accuracy.

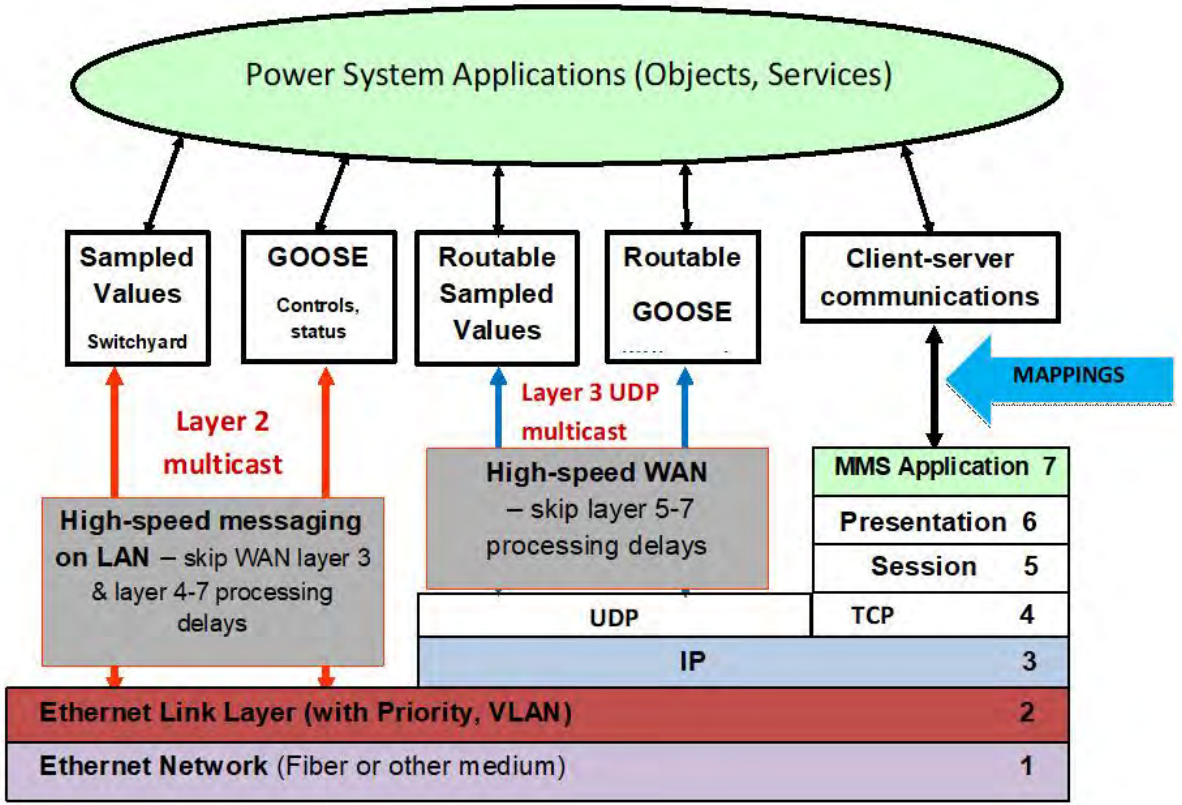
UDP

- Reception errors are flagged, but no way to request a resend.
- The only choice for multicast to multiple subscribers.
- Best fit for streaming data – keep it coming - the receiving application has to deal with missing data issues.
- Slightly smaller data overhead in packet.

IEC 61850 service mappings to OSI layers

New - growing importance of fast WAN services using Layer 3

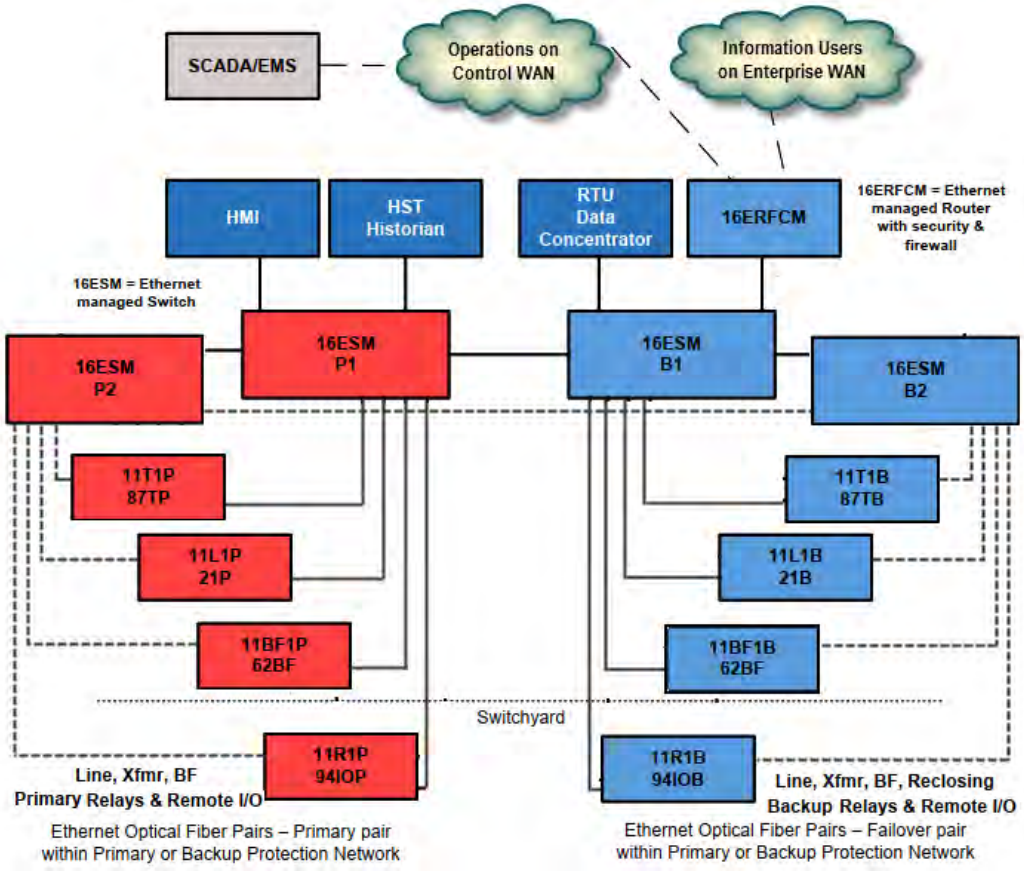
- Wide-area R-GOOSE and R-SV add layer 3 UDP – tens of ms and getting better.
- IEC 61850 high-security synchrophasor transport to supersede IEEE C37.118.2.
- R-GOOSE for wide area tripping or control.



Substation Ethernet configuration for redundancy – Section 4

As shown in report, with:

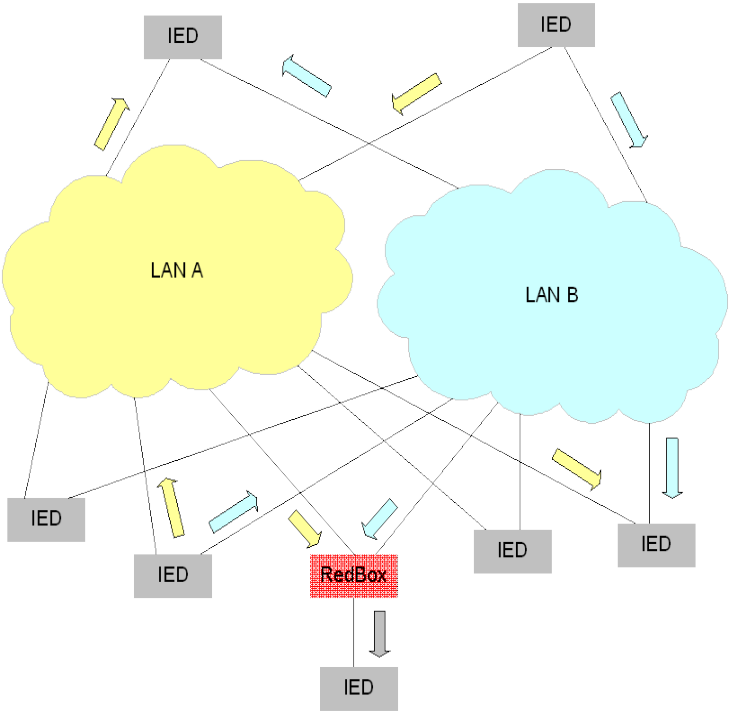
- IEEE C37.2 Device 16 and acronyms.
- Two isolated redundant protection systems P & B
- Backup or failover relay optical Ethernet paths for comms failures within redundant system.
- RSTP failover link between redundant systems.



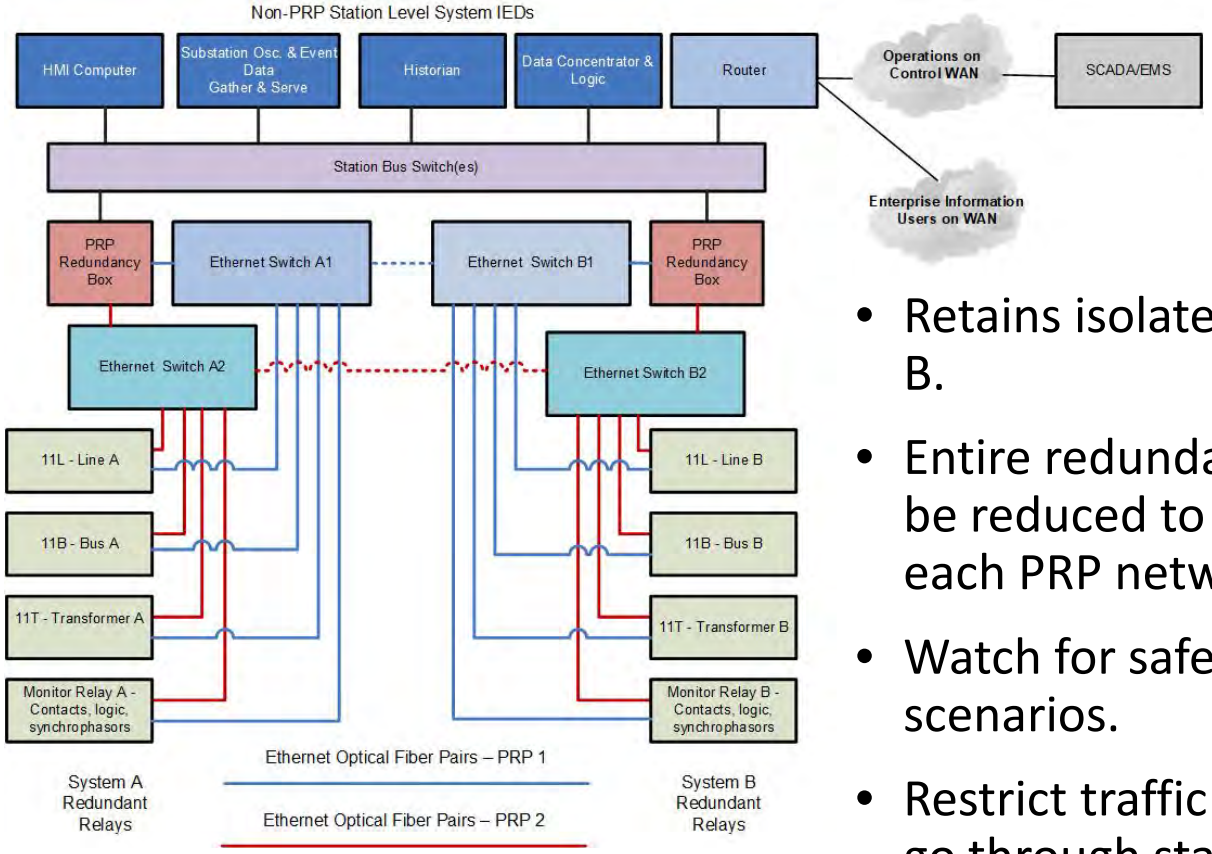
Bumpless network redundancy

Parallel Redundancy Protocol (PRP)

- Message content is tagged & sent into 2 networks.
- Only first received message is passed.
- No delay for first failure.
  - RSTP can lose 5-20 ms.
- *Note*: PRP covers only link, switch, port failures.
  - Improves *network availability* with each of Redundant System A and System B.
  - Doesn't help single IEDs that can still fail.
  - Does not replace dual isolated relay IEDs.



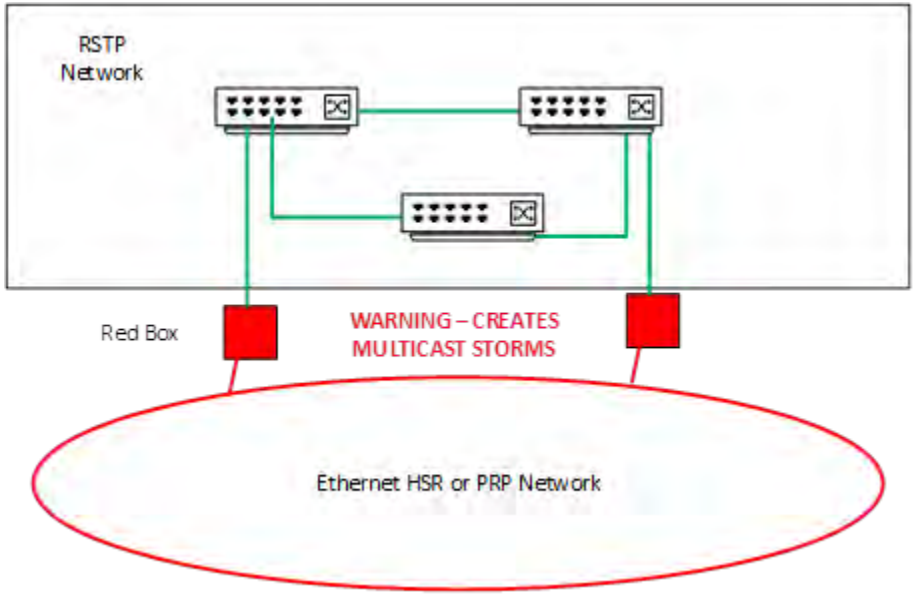
Redundant substation network with PRP

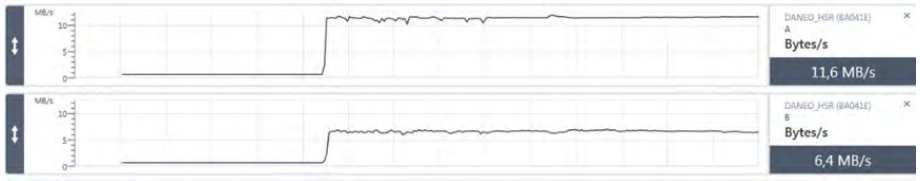


- Retains isolated System A & System B.
- Entire redundant protection could be reduced to 2 switches – one for each PRP network, but…
- Watch for safe maintenance scenarios.
- Restrict traffic on dotted cross links, go through station bus, or else…

Dual RedBoxes cause data storm

- Discovered in UCA IOP test.
- With redundant RedBoxes between shared networks.
- Each RedBox replicates traffic in both directions.
- They circulate each other's packets until networks are maxed out.
- Avoid redundant RedBoxes on the same LANs or get a RedBox with a vendor mechanism to block effect.

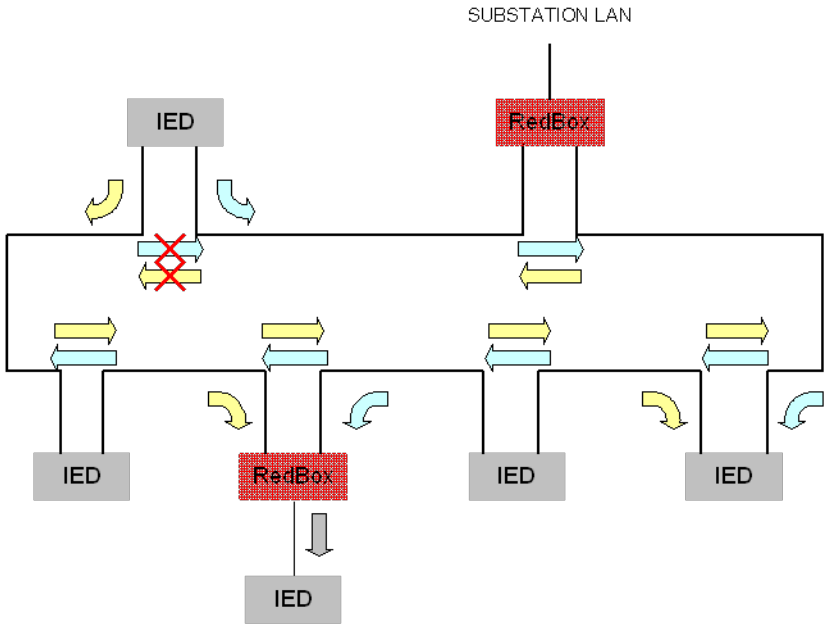




Bumpless network redundancy

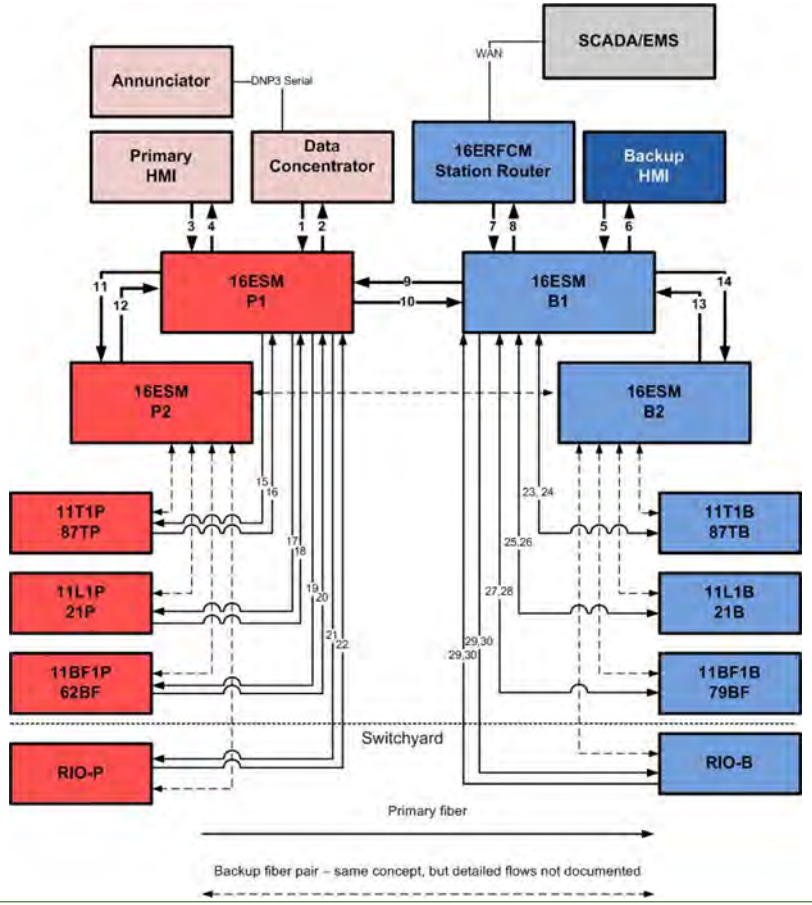
High availability Seamless Redundancy (HSR)

- Ring network architecture.
- Dual-port IED circulates packets in both directions.
- Circulation stops when packet in either direction gets back to sender.
- No single failure impacts reception success.
- Requires no Ethernet switches – save cost & complexity.
- Doubles traffic – use for simple or distribution applications.



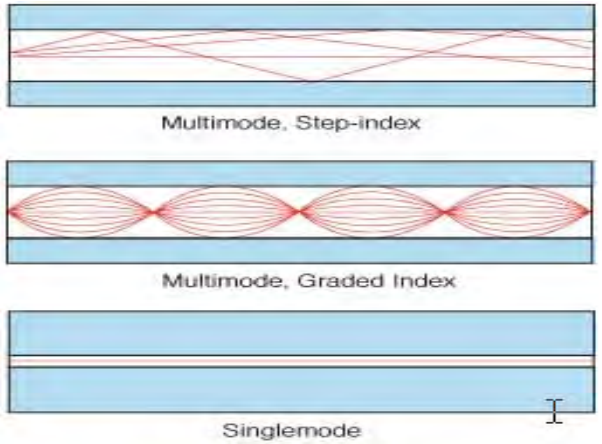
Functional data flows – Section 5

- Data signals are not single point-to-point as with wiring.
- Each path carries many signals.
- Paths can pick up new signals.
- In and out of multiple switches & IEDs.
- Flows altered by redundancy.
- GOOSE multicast throughout LAN.
- Document specific data flows for:
  - Traffic analysis.
  - Troubleshooting.



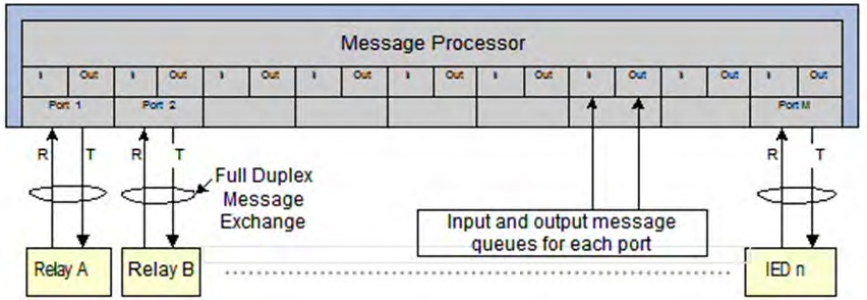
Fibers and wires – Section 6

- Use copper & RJ-45 in substations only for short runs in a rack – EMI vulnerability.
- Multimode fiber for short runs in substation.
- Single mode for long distance with laser or may be used in substation with LED emitters as offered.
- ST connectors being overtaken by LC.



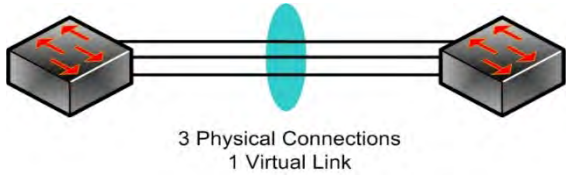
Message processing computer connects all LAN devices

- No packet collisions or losses up to data rate capacity.
- Checks each incoming frame and resends via configured outgoing port queues.
- Priority, VLAN, Layer 2 address, multicasting, speed.
- Optical and/or electrical ports.
- Full duplex operation on every port via message queues.



Switch services beyond VLAN and priority tagging

- Simple Network Management Protocol (SNMP) – configuration, reporting, alarming.
- Internet Group Management Protocol (IGMP) – dynamically adjust routing of multicast messages to VLANs or ports.
- Generic attribute Multicast Registration Protocol (GMRP) – filters multicast messages to devices that should get them (useful with GOOSE).
- Rapid Spanning Tree Protocol (RSTP) – ping network for loops, disable redundant paths; detect link failures and quickly enable backup path.
- Automated port configuration negotiations like speed – might want to turn off for stable P&C substation networks.
- Class of Service (CoS) queuing based on tag; Quality of Service (QoS) management based on traffic type identified by type of service bits in TCP/IP packets.
- Link Aggregation Control Protocol (LACP) for speed and redundancy between switches.

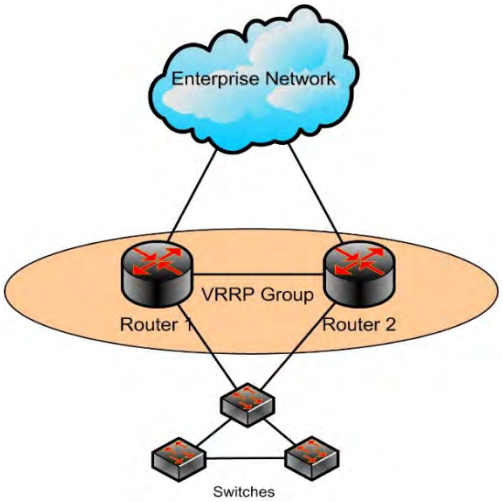


Switch selection and configuration

- A switch can have thousands of settings:
  - For each port – name, enable/disable, medium, speed, duplex mode, auto-negotiate, flow control, link fault indication, alarms, ingress limit, ingress filtering, egress limit, egress filtering, ingress and egress VLANs, untagged message handling, tag add/remove, extract priority from IP, port mirroring, power over Ethernet, more.
  - Overall settings for the switch.
- One error can cause failure – manage settings like a multifunction relay.
- Develop replacement configuration strategy – SNMP or other.
- Switch selection guidance – see Annex B, draft UCA Product Implementation Conformance Statement (PICS) for IEC 61850 [*and other*] applications.

Ethernet router functions – Section 8

- Ability to discover remote servers on WAN - including domain name to IP address conversion (DNS).
- Static WAN configuration or dynamic primary-backup-alternate path selection.
- Translate LAN addresses to WAN or Internet addresses for routing and cybersecurity.
- Firewall blocks unauthorized access.
- Virtual Private Networking (VPN) - isolated secure communications tunnel to remote device/server.
- Processing all he LAN messages and selecting packets intended for external communications; routing and prioritization in both directions.
- Routing of multicast messages to LANs or VLANs at remote sites – Generic Routing Encapsulation, GRE.
- Assign and manage LAN IP addresses – Dynamic Host Control Protocol (DHCP).
    - In substations the IP addresses of relays and IEDs are usually fixed as settings in those units.
- Detect external path failures and reroute traffic - Virtual Router Redundancy Protocol (VRRP).



Ethernet router functions continued

- Reformatting of messages for compatibility with a variety of external communications channel types, for example:
  - Multi-protocol label switching (MPLS) - common carrier or utility-owned
  - Ethernet connection to WAN
  - T3/E3/DS3 (e.g. utility owned SONET)
  - T1/E1 (e.g. utility owned fiber ring or microwave)
  - Frame Relay or DSL (common carrier; obsolete protocols)
  - Serial RS-232 and RS-485 (e.g. to old SCADA master); modems
- Monitoring, alarming, and logging of traffic behavior and diagnostics.
- Network management protocol (SNMP) or Secure Shell (SSH) communications for configuration.
- Receiving and serving date/time to LAN - network time protocol (NTP); simple NTP or SNTP; IEEE 1588 Precision Time Protocol (PTP).
- Backup and restoration of the full configuration or setting data base.
- Functions of switches with multiple LAN ports.

Network addressing with IP – Section 9

- In long-standing IP version 4 (IPv4) – 32-bit address in IP payload packet.
- Displayed as four bytes, each 0-255, e.g. 192.168.1.152.
- The world is running out of IP addresses.
- Specific bit-wise sub-allocation of addresses in private networks.
- Temporary allocation on Internet or on private subnetworks – Distributed Host Control Protocol (DHCP) of router.
- *Details – IP ports, etc. – Annex A*

IANA-reserved private IPv4 network ranges			
	Start	End	No. of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16,777,216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1,048,576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65,536

Internet Protocol version 6 (IPv6)

"Coming soon…" since 1998.

- 128-bit address resolves shortage issues.
- Security incorporated in protocol.
- Quality of Service (QoS) management incorporated.
- Packet prioritization incorporated.

Causes of delay in implementation:

- Availability of compliant products.
- Lack of diagnostic tools & training.
- Massive change cost for huge legacy networks working as they are.
- Migration and dual-scheme solutions.
- Lack of regulatory requirement.

Network security – Section 10

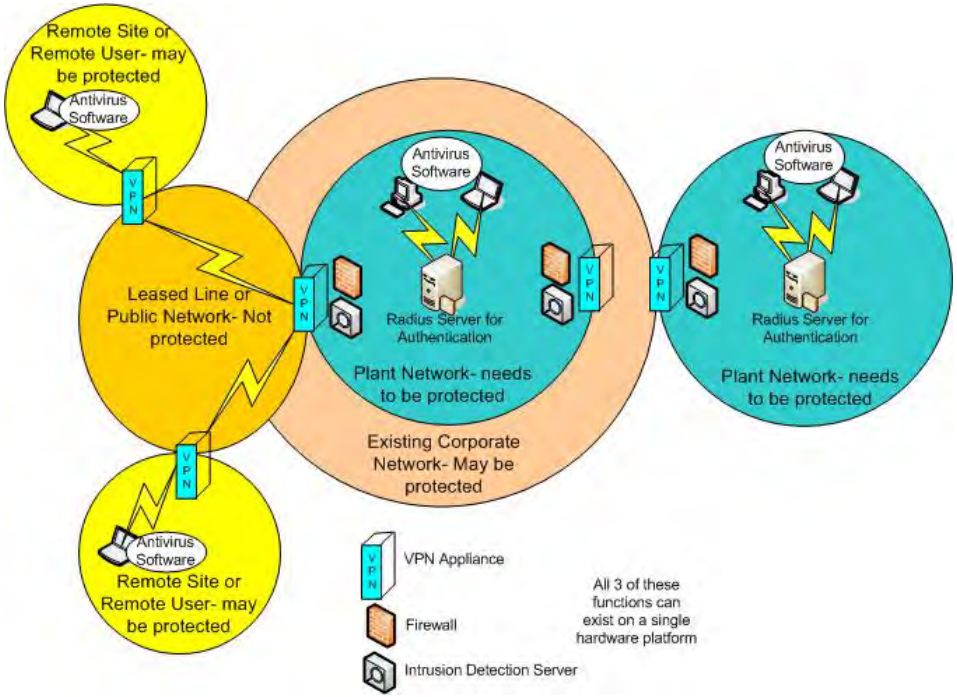
Vulnerabilities:

- Passwords
- Physical security boundaries.
- Device and user authentication.
- Remote access through physical security boundaries.
- Operational access across WAN.
- Local incidental access through network and device ports.
- Malware invasion through user device connections (including social engineering).
- Enterprise diverse role-based access control.
- Organizational control of personnel.
- Control and protection of security related information.
- Disclosure of security methods.
- Outright internal and external hacking.
- Security event detection.
- Event response capability.

Establishing physical and electronic security perimeters

Examples of tools:

- User role-based authentication & multi-factor authentication.
- Data packet authentication.
  - Challenging area of innovation for real-time systems.
- Encryption.
- LAN isolation & VLANs.
- VPN – secured tunnels.
- Firewalls & white-listing.
- New - Software Defined Network (SDN) traffic management.
- Electronic control of PSP.
- Video, thermal image, acoustic monitoring.
- Security monitoring organization.
- Training & procedures.
  - Work plans as for ac system.
- Intrusion protection service (IPS).
- Event recovery plans.



Network design steps – Section 11

- Use cases or applications listing.
- Security design concepts.
- Architecture for reliability and availability – impact of single points of failure.
- Backup or secondary operating modes for failures, and performance impact.
- Careful consideration of failure repair and safe maintenance procedures:
  - What does failure impact?
  - How does technician diagnose?
  - What needs to be turned off to repair?
  - How to reconfigure?
  - Backup or redundancy – can ac system be left energized?

Network design steps continued

- Ethernet mixes all types of messages and services
  - Model the worst case on each link, path, device.
  - Operational & non-operational traffic & priorities.
  - Traffic volume and mix analysis.
  - Use of priority and VLANs.
  - Traffic documentation and mapping.
  - Failure scenarios.
  - Security scenarios.
- Limit max traffic and plan for future (e.g. stay under 50% capacity).
- Check latency or packet delays, jitter, symmetry.
- Include performance and path failure monitoring (e.g. GOOSE time allowed to live or TAL alarm; DNP3 or heartbeat failure alarms; alarming path monitoring).

Intersubstation P&C applications – Section 12

How to send high-speed critical messaging over distances – pilot protection, transfer tripping, remote status reporting, remedial action schemes (RASs).

- LAN extension across large physical area/among sites.
  - Ethernet over SONET path.
    - VCAT (Virtual Concatenation).
    - LCAS (Link Capacity Adjustment Scheme).
    - GFP (Generic Framing Procedure).
  - GOOSE or SV tunneling.
  - *New* – MPLS Ethernet tunnel.
- Direct fiber ring or mesh.
- Routable GOOSE (R-GOOSE) and Routable Sampled Values (R-SV).
  - Includes authentication and external encryption for cybersecurity.
  - IEC 61850 synchrophasor streaming.

Standards for performance and environment – Sections 13 & 14

Performance

- IEC 60834-1 requirements for security and dependability of protection.
- CIGRE and IEC specific interpretations.

Environmental withstand capability

- IEEE 1613 physical and EMI environmental requirements for networking equipment & devices – living in substations with relays.
- IEC 61850-3 Edition 2 is parallel to IEEE 1613 plus other performance requirements.

Today's 'hot' topic – *cooling of networking equipment with high internal power consumption and heat generation for speed, e.g. MPLS routers.*

No fans? Living with fans?

Conclusions

- PSCC P6 report is broad introduction to networking basics for P&C
  - Sections adopted as basis by other IEEE PSRC/PSCC WGs to build detail areas.
- Reference and checklist for P&C network planning and design – from basics to practical considerations.
- Concise resource for P&C network terms and usage in IT context.

Section 15 – Network management – this section & whole report is a basis for IT and P&C experts to learn from each other and develop collaborative plans for network management, maintenance, sustainment.

- Report is supplied as WPRC paper and is published on IEEE PSRC and PSCC websites.

Communications evolve rapidly – watch relay conference papers each year for new developments.

Questions?

P6 Chair - Eric A. Udren, eudren@quanta-technology.com, (412) 596-6959

Vice Chair - Benton Vandiver, Benton.Vandiver@us.abb.com, (713)294-1535

IEEE Power System Communications and Cybersecurity Committee

https://site.ieee.org/pes-pscc/

IEEE Power System Relaying and Control Committee

https://www.pes-psrc.org/