IEC 61850 P&C Architecture - Impact on NERC Standards and Definitions

Eric A. Udren, Member NERC SPCWG
Quanta Technology LLC

WECC Protection & Control Subcommittee Meeting

June 5, 2025

Eric A. Udren

Industry Advisor
Quanta Technology, LLC
1395 Terrace Drive
Pittsburgh, PA 15228 USA
Mobile +1 412-596-6959
eudren@quanta-technology.com

SPCWG project - Ethernet-based Protection and Control Technical Reference

Project team:

Eric Udren (SME - Quanta Technology LLC), Lynn Schroeder (SPCWG Chair; Sunflower Coop), Davis Erwin (PG&E), Jeff Iler (AEP), George Wegh (Eversource), Michael Thompson (SME – SEL); Brian Kasmarzik (monitoring as Chair of PRC-005 SDT)

Theme:

Give recommendations - which NERC standards and definitions need clarification or adjustments when the P&C system is based on:

1. Ethernet network or data communications paths among relays or protective computing elements, carrying data or control signals used in fault protection.
2. Switchyard data acquisition or I/O - merging units (MUs) or remote I/O units (RIOs) with fiber data communications in place of switchyard or panel dedicated wires.
3. Wide-area system protection functions using inter-site communications, such as PMU-based backup fault or swing protection.

SPCWG project - Ethernet-based Protection and Control Technical Reference

Looking even further forward with caution – in trial now or coming soon:

1. P&C performed on interconnected computing platforms supporting flexible combinations or allocations of protection functions.
    a) This includes 'centralized' (CPC) systems as in IEEE Guide C37.300 or distributed unified protection systems like the unified grid control platform (UGCP) concept (EPRI).
    b) Includes virtualized protection functions like vPAC on IT server platforms and standard-platform relays with function-enabling menus and operating systems.
2. Electronic instrument transformers or binary state sensors with analog, binary, or data message outputs (*not much new on which to focus*).
3. Power apparatus with computer-based control interfaces and fiber data communications messaging used for fault protection (*covered by 1. and 2. of prior slide*)

Related or impacted NERC standards & definitions

1. NERC Glossary Definition of *Protection System (Protective relays, associated communication systems, voltage and current sensing devices, station dc supply, and control circuitry)*
2. PRC-004-6 - Protection System Misoperation Identification and Correction.
3. PRC-005-6 – Protection System Maintenance (*including Condition-Based Maintenance PSMP*).
4. TPL-001-4/5 - Transmission System Planning Performance Requirements (*has component definitions*)
5. PRC-012-2 – RASs (design & review, testing, op/misop reporting & actions, databases, review)
6. FAC-008 – Facility Ratings (*e.g., as applied to MUs, EITs*)

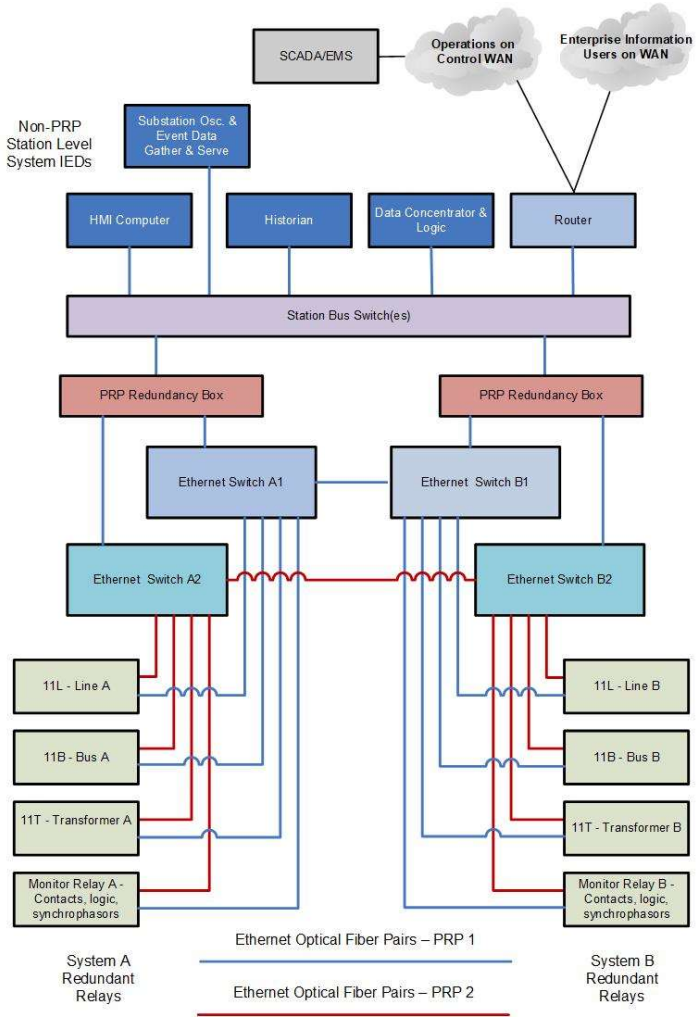
- What interpretations are required?
- Are changes needed?
- How does the industry deal with these systems going forward with respect to NERC reliability standards?

Conclusions are to be *functional* and not focused on a specific technologies, designs, or protocols.

Tech Reference development is still in progress – we can explore and review issues here .

Emerging technologies for P&C

Recent P&C design technologies calling for interpretation



IEC 61850 communications services replace single-function wires with interleaved Ethernet packet messaging services over optical fibers – *thousands of functional connections on one fiber:*

- *GOOSE service* – high-speed tripping, control, and status reporting messages exchanged among relays, and between relays and MUs, for protection.
- *Routable GOOSE or R-GOOSE services* – wide-area network (WAN) GOOSE with automated routing configuration and authentication security – used for wide-area protection & control, like RAS, CPC, UGCP.
- *Sampled Values (SV) service* – streaming packages of point-on-wave sampled data and status points – e.g., from switchyard MUs to networked control house relays sharing measurements.
- *Routable Sampled Values or R-SV service* – WAN SV with automated routing configuration and authentication security – - synchrophasor streaming and wide-area P&C like RAS, CPC, UGCP.
- *Redundancy arrangements* – duplicate relays versus network redundancy methods like Ethernet rapid spanning tree protocol (RSTP), IEC parallel redundancy protocol (PRP) or HSR.

Recent P&C design technologies calling for interpretation

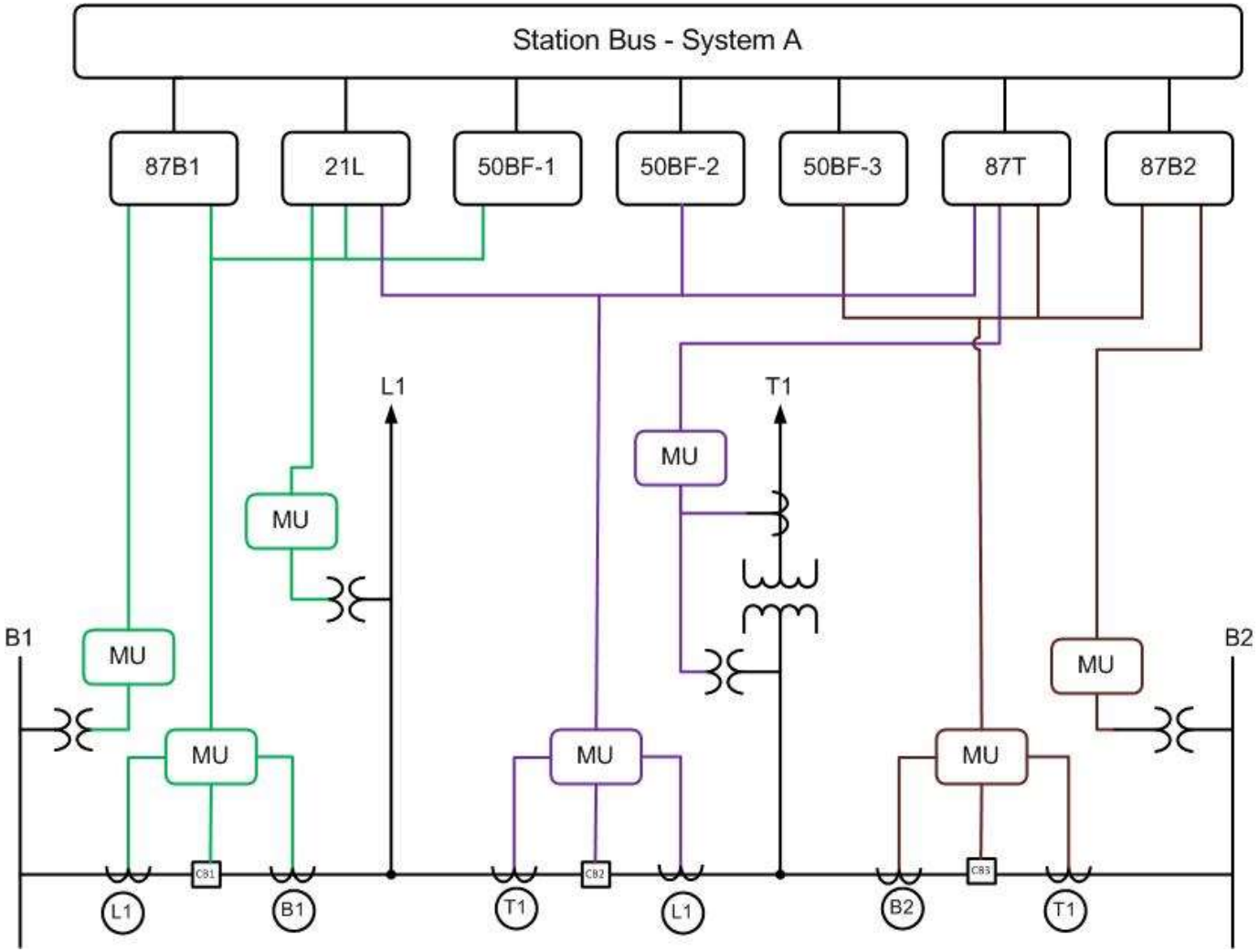
Tech reference will consider other protocols including proprietary choices used for protection.

- Examples – Mirrored Bits® or Direct I/O®; DNP3, Modbus, proprietary messaging *if used for protection or RAS*.
- Some non-protection protocols may be used to achieve *compliance* – e.g., SCADA monitoring and alarming via trip coil circuit monitor; heartbeat monitoring per PRC-005-2/6/7 CBM PSMP.

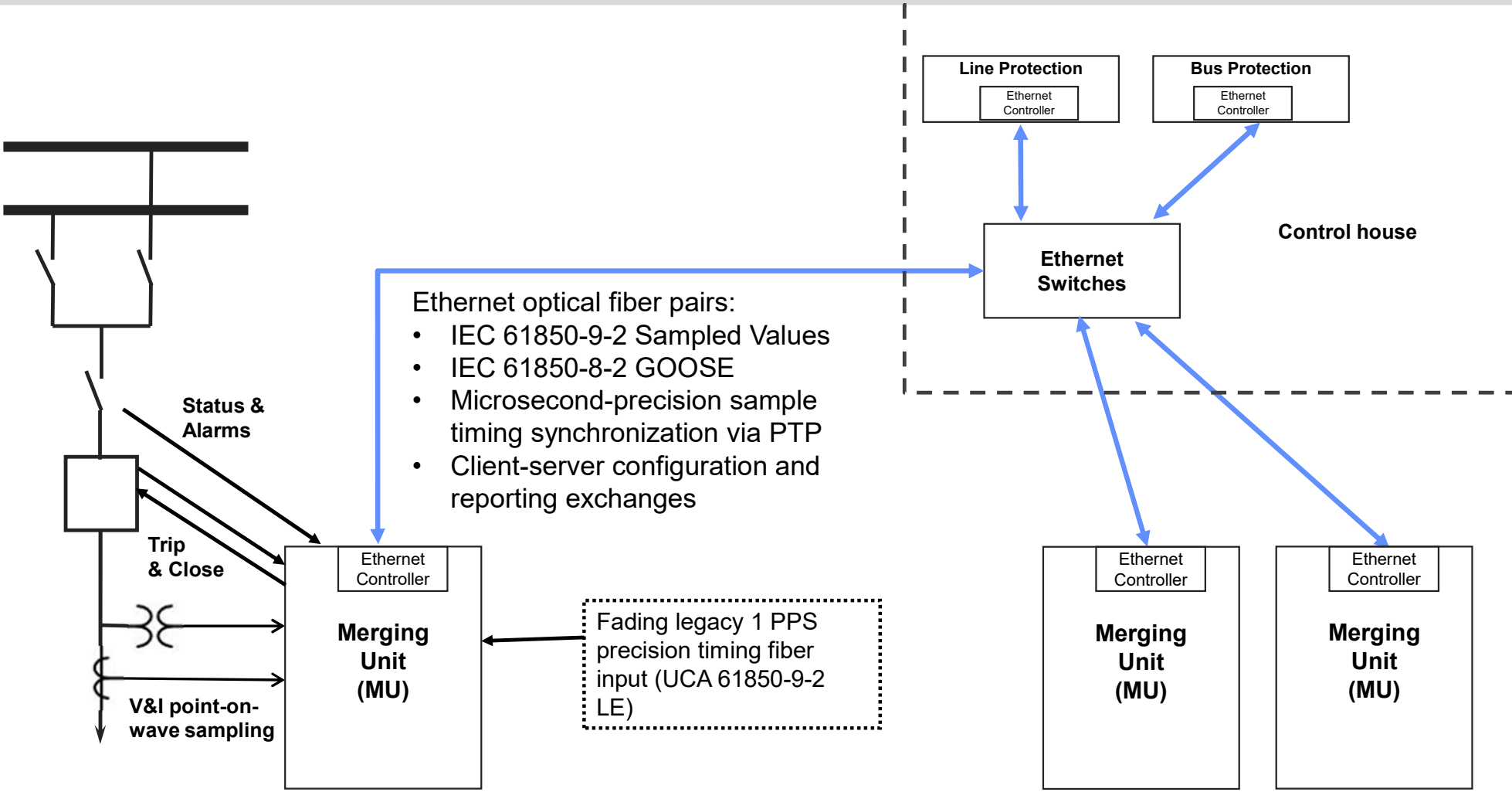
IEC 61850 background - drivers and absorption

- IEC 61850 comprises:
  - List of standard communications services – GOOSE, SV, client-server and configuration exchanges (*works like DNP3 with automatic associations in lieu of point list mapping*), time synchronization, more…
  - Standardized data exchange interfaces for each function ('logical nodes') – PDIS, PIOC, XCBR, etc.
  - Substation Configuration Language (SCL) project or P&C system engineering process based on automation tools to save time and money – interconnect the *functions* to fit the substation or project topology and forget about *mapping points*.
- Products available from relay and other vendors for two decades.
  - Most projects were turnkey international jobs by relay vendors until last decade.
  - 2010 to 2025 – increasing NA utility adoption of IEC 61850 based P&C standards.
- *Organizational education and adaptation are needed for success* – this is **not** just the next generation of P&C boxes to adapt to the design and maintenance standards we have.
  - Affects the whole organization and processes – business cases, deployment project management, standards management, engineering processes, documentation and databases, configuration management systems, maintenance programs, maintenance procedures and skills, operator knowledge, asset management, supply chain.

Typical IEC 61850 substation P&C system with process bus



Merging units in switchyard

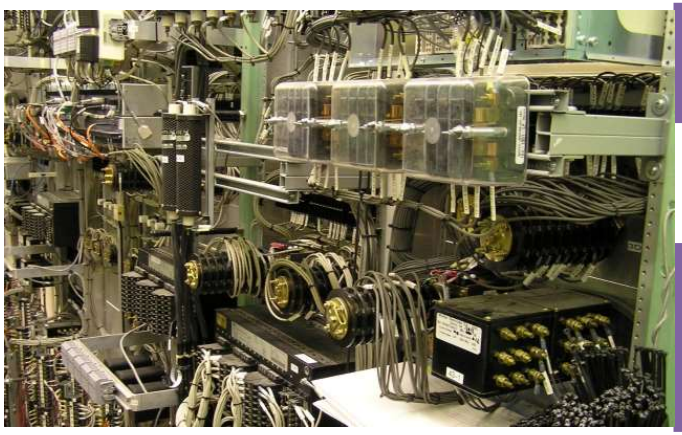


IEC 61850 drivers and absorption

- Ethernet networking components from the IT world combine with substation-grade processing to utilize the world's supply chain of latest electronic systems.
  - P&C teams learn fundamental Ethernet network engineering and IT-OT principles.
  - Make friends and collaborate with your utility IT/Telecoms team.
- Vendors are focusing on IEC 61850 based products.
- Most wiring eliminated – replaced by *configured* Ethernet messaging (i.e., settings)
  - Among relays, IEDs, functions in control building, and switchyard MUs or RIOs.
- IEC 61850-6 functional system or substation configuration language (SCL) - automated system engineering process & tools save time & work (once user process is running).
- Secure wide-area communications and management *can & must* be built in.
  - Tacked-on boundary security solutions will be tough to manage.
- 61850 logical node (LN) modeling determines interconnection mapping.
  - serves generic-platform and digital-twin models of protection, monitoring, control, management.

Wiring reduction – Ethernet & fibers

IEC 61850 and Ethernet P&C eliminate almost all wiring for protection, control, automation, and data gathering.



Conventional point to point wiring

Ethernet on optical fibers

Standardized object models, point descriptions

Integrated P&C system using fiber optic network cables

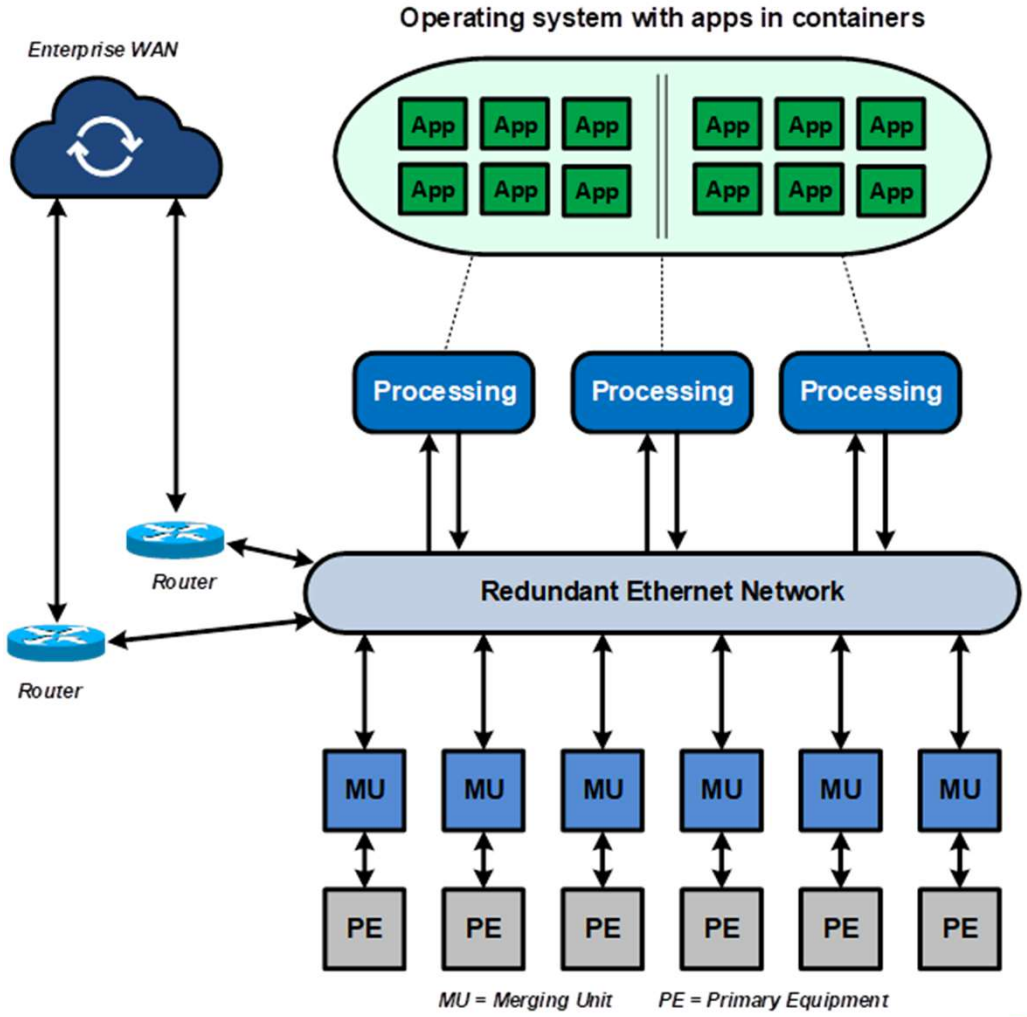
The wiring is gone, but what happened to the complex functionality?

It is embedded in settings or configuration throughout the system

- Where are the test switches and maintenance check points?
- How does utility update firmware or settings in this interactive array?
- What maintenance requirements minimize risk of setting errors (‘moving wires’)?

CPC and Unified Grid Control Platform (UGCP) *substation* architecture

- Builds on IEC 61850 digital substation design and networks.
- Generic processing platforms – standard relay boxes or IT server platforms.
- Multiple redundant processing platforms and networking.
- Many P&C functions in a standard box (apps) with logical node (LN) interfaces.
- Hypervisor operating system spins off P&C functions as virtual machines running in isolation.
  - Are they all there and running?
- Centrally managed configuration and modeling.
  - More layers and counts of settings than ever before.

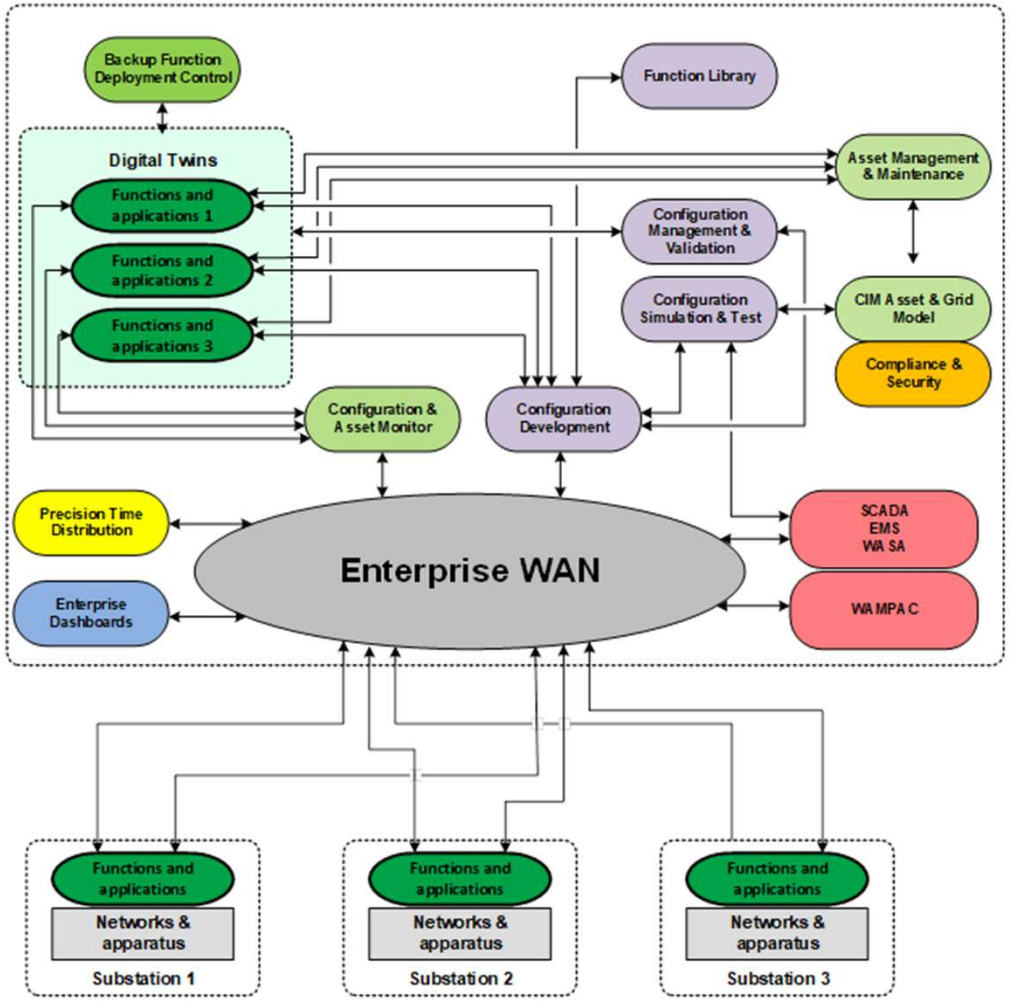


UGCP – P&C expands across the regional grid

- Distributed array of redundant standardized data sensing, processing, and storage resources interconnected with redundant high-reliability cybersecure data communications.
- Inherits IEC 61850 digital substation elements.
- Redundant processing platforms and networks.
- Floating protection apps with Logical Node (LNs) standard interfaces and virtual processing compartments..
- Centrally managed configuration & modeling.

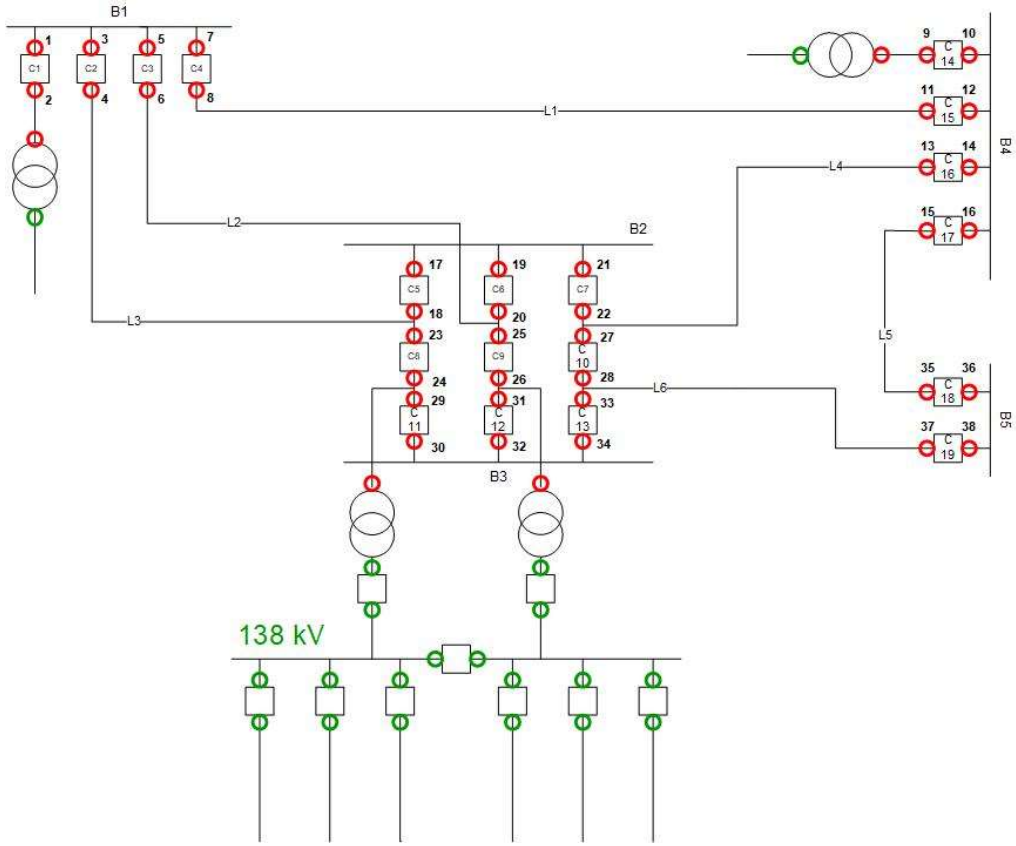
*Includes substation and **wide-area protection and RAS** functions.*

UGCP papers given at WPRC 2023, Texas A&M 2023, Georgia Tech 2024



Example relaying – Wide Area System Protection (WASP)

- *Assured* backup (& slow primary) protection with IBR penetration up to 100% varying during the day.
- Now under development with DOE support.
- Utility demos in 2026 – ConEd, Dominion, SCE, SDG&E – includes field demos in hi-IBR areas.
- Gather PMU currents (and voltages) for a zone-by-zone holistic grid 87 fault protection.
- Faster and more surgical than Zone 2, which may not work (but leave Z2 as slower overreaching safety net).
- Wide-area relaying system works through substation relays, is self-monitoring across the grid.
- Components are PMUs, secure Ethernet WAN R-GOOSE and R-SV comms, time synch (GPS -> PTP).
- *RAS will go down the same technical path.*

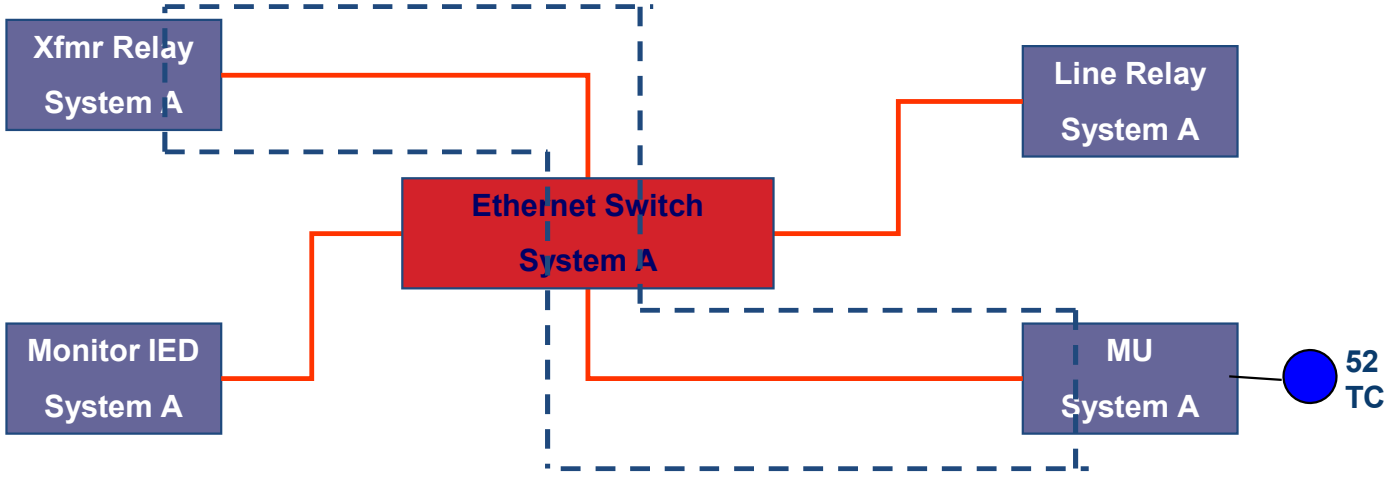


NERC standards and definitions examples

Continuous end-to-end monitoring serves PRC-005-2/6/7 CBM - 1

End-to-end check of IEC 61850 tripping or protection-critical communications:

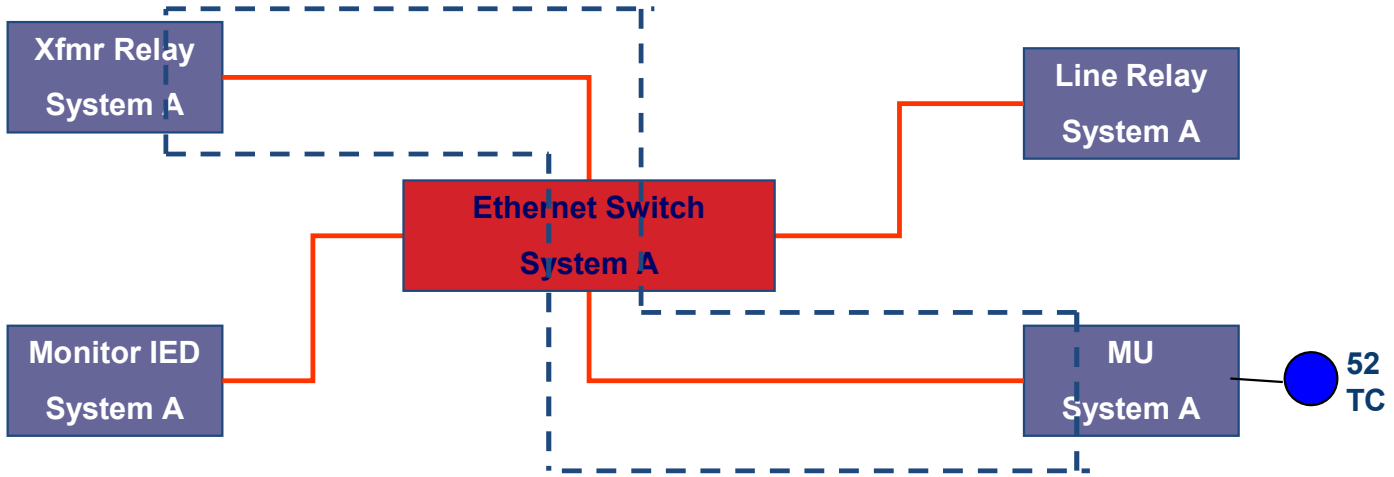
- All processors are monitoring themselves continuously.
- *Example*: transformer relay publishes a GOOSE message including a specific breaker trip bit.
- Normal-state message (*do not trip*) is generated *every second* by DSP in transformer relay.
- Passed to the communications processor in transformer relay
- GOOSE message passes through relay Ethernet controller to fiber, then to Ethernet switch.



Continuous end-to-end monitoring serves PRC-005-2/6/7 CBM - 2

- Ethernet switch passes GOOSE message to subscriber MU incoming control Ethernet port.
- Communications processor of MU passes *no-action* message to MU processor every second.
- MU processor alarms if *no-action* subscribed GOOSE isn't received every second.
- MU sends alarm back to substation relays or concentrator via GOOSE or MMS with the same type of heartbeat (subscriber to alarm message will raise a different alarm if this path is lost).
- We always know that when we finally send a *trip-action* bit, it will be received and acted on.

Not all wires can check themselves continuously like this. This monitoring alarms for configuration/setting errors as well as optical path, processor interface, or switch failures.



NERC PRC Topic 2 – Practical auditable CBM programs

- Documentation of how condition is monitored in a P&C system replaces extensive TBM work and records
  - No hidden failures – failures reported when they happen, not when found years later in a test or when a misoperation exposes it.
- Design standardization helps – document once to support all standard installations
- Some records of alarms and failure mitigation could help demonstrate that CBM program is effective
- Give hard guidance on audit-acceptable documentation for a CBM PSMP based on IEC 61850 or other communications services to drive use of CBM
- TBM will be impractical in new substation and wide area designs.
- CBM can be easier, practical, and effective.
- A chapter of Tech Ref will push for practical CBM.

Component Attributes	Interval	Maintenance Activities
Unmonitored protective relay	6 years	Verify that settings are **as specified** *Non-microprocessor relays:* Test; and calibrate if needed *Microprocessor relays:* Test protection I/O Verify ac measurements.
Monitored microprocessor relay with alarming for failures	12 years	Verify settings are as specified. Test operation of protection I/O. Verify ac measurements.
Monitored microprocessor protective relay as above plus Auto comparison check of ac measurements Alarming for change of settings Some monitoring of protection I/O	12 years	Test operation of protection I/O that isn't monitored. *Remote SCADA trip test = never touch the relay until it alarms*

NERC PRC Topic – mapping Protection System definition to IEC 61850

- Protective relays, or components of control systems [SDT for PRC-005-7], which respond to measured electrical quantities and provide protective functions;
- Communications systems necessary for correct operation of protective functions;
- Voltage and current sensing devices providing inputs necessary for the correct operation of protective functions;
- Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply);
- Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

For IEC 61850 protection systems – Some discussions and proposals among Tech Reference team members:

Protective relays which respond to electrical quantities - Include **processors** programmed to respond to data representing electrical quantities; **operating or software systems** supporting the processing and response; auxiliary devices such as **merging units or RIO** which acquire and transmit data on electrical quantities or implement programmed responses to those quantities; if fault protection can be impacted.

Maintenance impacts – time-based functional testing versus CBM with platform monitoring. Special attention: virtualized operating systems or containers used for protective functions – shall we treat each as a relay and thus require monitoring of each?

▪

NERC PRC Topic – mapping Protection System definition to IEC 61850

Communications systems necessary for correct operation of protective functions –

Devices and interconnections within a substation assembled to communicate protection information among protective relays or processors and auxiliary devices or merging units. Equipment that can impact fault protection may include switches, routers, fibers, PRP redundancy interface boxes (redboxes), interconnections and junctions, and time synchronization components.

Ethernet componentry conveying Protection System Control Circuitry functions [switches, routers, and fibers];

Ethernet componentry delivering voltage and current sensing device information input to the relays [switches, routers, and fibers];

Componentry internal and external to the substation provisioned for communication aided, inter-substation, or wide-area Protection Systems (Ex: POTT, 87L, wide-area protection functions, RAS).

Can we absorb RAS into other protection systems as latter move to wide-area applications anyway?

Maintenance: frequent functional testing (*not practical at scale*) or functional/performance monitoring.

Note: In-substation communications network paths were characterized as 'control circuitry' in Technical Reference for PRC-005-2. This lowers monitoring and testing requirements – we think unwisely and unnecessarily.

NERC PRC Topic – mapping Protection System definition to IEC 61850

Voltage and current sensing devices providing inputs to protective relays -

This category is limited to the sensing device and the wiring from the sensing unit to the merging unit. No change of maintenance options.

Station dc supply associated with protective functions (including station batteries, battery chargers, and non-battery-based dc supply), and

Control circuitry associated with protective functions through the trip coil(s) of the circuit breakers or other interrupting devices.

Traditional substation protection wiring (wiring from merging unit to the breaker Trip Coil, breaker status, etc.) and wiring from the DC panels to Protection components (physical device power). No change of maintenance options.

Other discussions and proposals

- Add clarity regarding system timing functions like GPS and PTP messaging when they are critical to fault protection performance.
  - We can work with GPS but will eventually want wide-area redundant distribution of precision time over Ethernet networks. This can impact fault and swing protection functions.
- How can we assure auditor understanding of a compliant CBM design and program? Use *functional* language in definitions.
- Is there any action required to help ensure proper continuing design of redundant configurations? What functional rules are stated and where? This this to tie into TPL-001-5.
- There has been ongoing work by SPCWG members to get sensible language on protection system components into TPL-001-5 (Footnote 13 and efforts of Davis Erwin, PG&E).
- There is ongoing discussion of proposal to move RAS requirements under protection system requirements and to clarify role of PRC-012-2.
- Can a PSRC White Paper clarify requirements to help users, or to guide audit processes? Compliance guidance document?
- There are no plans to work on new CIP proposals. Solutions for wide-area cybersecurity (and related physical security) can fit within existing CIP requirements.

Conclusions

- SPCWG Technical Reference team is working to advise NERC and the industry in 2025 on impact of emerging P&C technologies on standards, definitions, and compliance.
- Focus on Ethernet IEC 61850 substations.
- Focus on newer emerging P&C technologies – CPC, vPAC, and WASP are coming and cannot be avoided over time – are they being developed for reliability and compliance?
- We look for designs and issues that are coming to substations and wide-area protection systems – with caution about scope of what we recommend.

First goal **– explain technical issues and interpretation topics to industry stakeholders.**

Second goal **– give interpretation advice wherever that is resolves clarity or enforcement issues.**

Third goal **– recommend changes to standards and definitions if that is the only path to clarity.**

Questions & Discussion

Eric A. Udren
Industry Advisor
Quanta Technology, LLC
1395 Terrace Drive
Pittsburgh, PA 15228 USA
Mobile +1 412-596-6959
eudren@quanta-technology.com
www.quanta-technology.com

Current outline of Tech Reference on following slides.

Outline - Ethernet-based Protection and Control Technical Reference Document

V0.5 – August 23, 2023

1. Introduction – Statement of the purpose of the report and recommendations

2. Review of protection technologies in sequence, and key standard-related elements. R*eference designs* to support these explanations.

    a. Ethernet network or data communications path among relays or protective computing elements, carrying data or control signals used in fault protection.

        i. Features of redundancy and architecture that impact reliability.

    b. P&C systems with the above features may have protection functions based on IEC 61850 services on Ethernet such as GOOSE or Routable GOOSE (R-GOOSE) and Sampled Value (SV) or Routable SV (R-SV) messaging; but other protocols and services capable of control or data transfer for relaying by communications messaging are included, including proprietary methods.

    c. Switchyard data acquisition and binary I/O - merging units (MUs) or remote I/O (RIO) units.

        i. Data communications multiplexed on optical fibers in place of switchyard or interconnecting dedicated wires.

        ii. Switchyard protection system elements & enclosures.

        iii. Binary inputs and contact outputs.

    d. Wide-area system protection functions using inter-site communications of messaging services, such as PMU-based backup fault or swing protection.

        i. DOE development and a paper with the concept – only needs to be explained on the top level for this tech reference.

    e. P&C performed on interconnected or centralized standard computing platforms supporting flexible selections, combinations, or allocations of protection functions in operating system containers.

        i. This includes ‘centralized’ (CPC) or distributed unified protection systems coming to the industry - separate technical paper on Unified Grid Control Platform.

        ii. Present straw man is that this will have the same issues as a combo of IEC 61850 substations, teleprotection, and wide-area protection schemes.

        iii. Functions are mixed on platforms; need continuous monitoring.

    f. Electronic instrument transformers or state sensors with analog, binary, or data message outputs.

    g. Power apparatus with computer based control interfaces which are activated by communications messaging exchanges with protection functions.

    h. *Not in scope* - non-protection control communications, such as DNP3 or IEC 61850 non-protection control communications, even if these operate over the same data communications paths. These messages are present on the same data paths or networks; and they can be leveraged for PRC-005 CBM maintenance purposes. For example, a SCADA trip from a control center or HMI through a relay to a merging unit trip contact can demonstrate that that the protection trip path is functioning down through the trip coil.

3. Review of NERC reliability standards that need mapping, clarification, or expansion – for each of the following, what may be impacted? What change if any might be needed?
    a. PRC-004-6
    b. PRC-005-6/7 – a whole section below
    c. TPL-001-4/5
    d. PRC-012-2
    e. FAC-008 and merging unit interfaces
4. Relationship to NERC CIP standards and security methods or requirements for communications paths outside of PSP, such as teleprotection paths using What are the elements of a Protection System built from subject technologies?
    a. Goal is to evaluate the adequacy of the existing protection system definition and suggest options to address gaps or lack of clarity
    b. Current NERC Protection System definition
    c. For each protection system element, describe elements from each listed technology – conceptual table or mapping
    d. Discuss variations in the *definition* across NERC standards needing clarification – status of PRC-005-6/7 definitions, TPL-005 definition aberrations, RAS elements...any others?
    e. Ethernet routable protocols? This is out of scope – just point out CIP/security issue and compliance need.
5. PRC-005-6/7 CBM program impacts
    a. Report section explaining CBM approach of PRC-005-6 and practical application.
    b. Criticality of CBM for protection systems based on technologies in (2); challenges of applying TBM to these.
    c. Recommended direction of CBM programs
        i. Criticality of configuration and setting management.
        ii. Network components like switches and routers may be protection system components requiring monitoring and configuration management. Where in definitions and standards is this assured?
    d. Avoid technical prescription and stay functional.
    e. Help to guide future implementations of CBM.
6. Recommendations
    a. Recommendations for Protection System definition
        i. Changes or not to Protection System definition
        ii. Mapping or clarifications to Protection System elements where PS definition change is not required.
    b. Identified issues with NERC PRC or other standards listed above.
        i. Recommended revisions if any to above-cited standards.
7. Conclusion - Conclusions should be functional and not focused on a specific technology or protocol.
    a. Best practices

TPL-001-5.1 Definition of Protection System in Table 1 Footnote 13

13. For purposes of this standard, non-redundant components of a Protection System to consider are as follows:

a. A single protective relay which responds to electrical quantities, without an alternative (which may or may not respond to electrical quantities) that provides comparable Normal Clearing times;

b. A single communications system associated with protective functions, necessary for correct operation of a communication-aided protection scheme required for Normal Clearing (an exception is a single communications system that is both monitored and reported at a Control Center);

c. A single station dc supply associated with protective functions required for Normal Clearing (an exception is a single station dc supply that is both monitored and reported at a Control Center for both low voltage and open circuit);

d. A single control circuitry (including auxiliary relays and lockout relays) associated with protective functions, from the dc supply through and including the trip coil(s) of the circuit breakers or other interrupting devices, required for Normal Clearing (the trip coil may be excluded if it is both monitored and reported at a Control Center).

UGCP Specifications

UGCP adds requirements to our specs for the latest IEC 61850 P&C systems. Suggestions:

- Choice of Type 1 versus Type 2 hypervisor for containerization of applications.

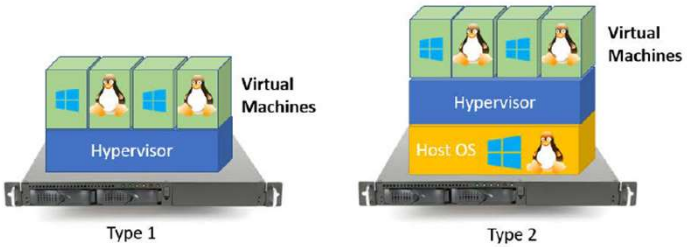


Figure courtesy of EPRI report and Herb Falk

- Condition based maintenance (CBM) maintenance program (PSMP) for Ethernet based system monitors processors, computations, communications heartbeats like GOOSE and DNP3 – *now add hypervisors, OS, virtual machines or containers, and comms among them. Monitor performance, not just presence. Add diagnostic filters for rapid remediation.*
- Add virtual and physical switches for isolating elements that may be upgraded or replaced. Monitor switch traffic for safe isolation and restoration. Traffic has time stamps and sequence numbers.
- Create strong configuration and settings management that *includes virtual machine deployment*.
- Hardware – all processors, memory, communications must stay under about 50% of capacity. Passive cooling without fans. Redundant power supplies. Redundant networking like PRP in addition to isolated redundant paths.