COMPILED INDUSTRY COMMENTS RESPONDING TO DOE REQUEST SUBMITTED 7/15/09

Q 1 – Can vendors build products around these specs? p. 2
Q 2 – will these specs meet NASPI's goals? p. 4
Q 3 – will the specs produce interoperable and testable products? p. 6
Q 4 – will the specs produce clear products that work between different builders? p. 8
Q 5 – do the specs incorporate appropriate standards? p. 11
Q 6 – security and cyber-security p. 12

Other – Before you build NASPInet, think about these things p. 17
Other – other p. 23

Attachment 1 – Paper from Dr. George Kusic, Univ. of Pittsburg p. 39
Attachment 2 – Material submitted by John A. Weyer, Cyber Security Subgroup p. 47

Commenters:

1. Sisco -- John Gillerman [johng@sisconet.com
2. SECS -- Stanley A. Klein [stan@osecs.com],
3. Consumers Energy -- Jianmei Chai [jchai@cmsenergy.com]
4. Mason, Michael R [michael.r.mason@xcelenergy.com]
5. Luo, Xiaochuan [xluo@iso-ne.com]
6. Alan Roth [aroth@advfusion.com]
7. George Sidman [gsidman@webloq.com]
8. Dr. George Kusic [gkusic@pitt.edu]
9. Hydro One -- John.Ciufo@HydroOne.com
10. ABB, Inc. -- Reynaldo Nuqui [reynaldo.nuqui@us.abb.com]
11. Duke Energy -- Lee, Laura [Laura.Lee@duke-energy.com]
12. EEI – Jim Fama Dworzak
13. GE Energy -- Fan, Jiyuan [jiyuan.fan@ge.com
14. SCE -- Anthony.Johnson@sce.com
15. Southern Co. – Clifton Black [CRBLACK@southernco.com]
16. Entergy – Edward Davis [EDAVIS@entergy.com]
17. RTI -- Joe Schlesselman [joe@rti.com]
18. BBN -- Rick Schantz [schantz@bbn.com]
19. AEP -- Sanjoy K. Sarawgi sksarawgi@aep.com
20. BPA -- Denise E Koehn [dekoehn@bpa.gov]
21. PJM -- Chantal Hendrzak hendrc@pjm.com,
22. Open Geospatial Consortium -- Louis Hecht, Jr. [lhecht@opengeospatial.org]
23. Ameren -- Shah, Kirit S [KShah@ameren.com]
24. Southwest Power Pool -- Mark Rogers [mrogers@SPP.ORG]
25. WAPA -- Dan Hamai [aHamai@wapa.gov]
26. OPT Online -- John Weyer [jaweyer@optonline.net]
27. CAT-1 -- Ron Stelmak [ron.stelmak@cat-1.com]
28. Manitoba Hydro – Tony Weekes [maweekes@hydro.mb.ca]
29. FPJohn Chung Huei Hsu/FTUTSF [JohnCHsu@ftpc.fpcusa.com], no comment at this time

1) Is this specification something that vendors can build products around, to provide needed services and middleware? If not, what changes are needed to these specifications to attain these outcomes?

PJM -- A vendor may be able to build various components and services of the system; however, if multiple vendors are involved, system integration and interoperability could be extremely difficult to ensure.

Entergy -- Procurement of both the pilot prototype and the eventual production environment should be divided into two discretely separate and independent parts – a) the NASPInet WAN, and, b) the PG DMZ. This approach creates no constraints on vendors in terms of bidding on one or both, or teaming with another organization(s) to propose an entire solution. If done this way, network carriers can focus on what they do well – but not be required to do something that is not their core competency. On the other hand, a software house or even a university could bid the PG software development and continuing maintenance work, without having to worry about the wide area network aspects. What's more, a system integrator could bid both parts using subcontractors, carriers, and/or internal resources as it sees fit. Finally, this approach permits a larger subscriber organization to contract for network service, and build and integrate the PG on its own. This flexibility is important.

BPA -- In general BPA believes they are. However, particular care must be taken to insure the APIs and other aspects are well documented and publicly available without license fees. We have some preference for moving as much of these specifications as possible into publicly available standards as experience with them reveals additional standards values.

RTI -- RTI has reviewed the proposed Statement of Work and Specification. In the opinion of RTI, the current Specification is adequate for vendors to provide necessary products and services that meet Specification requirements.

Ameren -- Because of the extent and level of functional detail specified in the Phasor Gateway and Data Bus specifications, it appears a successful vendor(s) will require a large degree of partnerships to provide the desire functionality. This, in itself, may require a high degree of integration and interoperability with each PG and DB integration and deployment.

Duke Energy -- The specifications provide adequate information for vendors to build the necessary products.

Open Geospatial Consortium -- The words "geospatial" and "ogc standards" do not appear in the NASPI databus and phasor gateway specifications, though every Phasor has a location and every line phenomenon has a linear and perhaps area-wide region of effect. Without standards, geospatial capabilities will be expensive to implement and non-interoperable.

ABB Inc. -- It does not seem clear from the documents as to how these devices and systems will be interoperable, i.e., no middleware or interoperability standard was proposed (just APIs).

BBN -- The documents still heavily and confusingly mixes up specification and requirements. To wit, titles of sections 3,4,5,6 and 7 of the Data Bus Spec bear "Requirement". These sections account for the bulk of the document and the nearly 1000 variously numbered "requirements" are often too detailed for requirements. It is going to be extremely difficult to validate whether a design or implementation satisfies all these requirements. Suggest having a small number of requirements that are high level and can be verified. Then have separate sections about "specification" that define interfaces, algorithms, scheme, data types, protocols, services etc that may be needed to meet the requirements.

ISO-NE -- Both of the specifications are well written and contain large amounts of information. There seems to be considerable overlap between the two. It may be beneficial to eliminate this overlap by combining the common sections into one document, which both procurement documents could reference. There is a very lengthy, but high-level, description under the functional specification sections. However, several technical details, which are needed to ensure interoperability are missing or insufficiently explained. For example, a message exchange facility requires a very detailed protocol description that contains data models, message layouts, format descriptions, validation logic and application behavior (e.g. how to report errors). Neither document contains the type of in-depth technical detail that is expected. The IEC/TR 62325-ISO 15000 series of documents provide a good example of the type of detailed technical information that is required for a reliable messaging system, which the authors of NASPInet may find useful as a model.

2) Given the NASPInet concept and goals, will the Phasor Gateway and Data Bus elements as specified in these documents effectively meet those goals? If not, what changes are needed to these specifications to attain these outcomes?

PJM -- Though it is mentioned that the proposed system needs to be able to handle data other than streaming phasor data using IEEE 37.118, the specifications sees to be geared toward what is an evolving and somewhat narrow standard. It would be desirable to build a high speed, trustworthy and secured data exchange network for several different types of measurements as well as control signals that can support a variety of grid monitoring and control applications.

Class A service with guaranteed delivery of phasor measurements and other control signals under the proposed architecture would be difficult to achieve and ensure. Additionally, the system needs to provide signal level granularity.

It has been mentioned that the system capabilities will be upgraded as needed. However it is hard to envision, short of replacing many of the components of the system, how the system capabilities can be upgraded. It would be desirable to do it right from the beginning.

If the goal is to facilitate Synchrophasor data exchange the system specified can meet that goal (if integration and interoperability can be assured).

BPA -- Yes, with caveats around the exceptions taken in our answers to #1 and #3. The data bus and gateway architecture is a better approach than the super PDC hub-spoke architecture, leaves more potential for diverse participation, and makes it easier to appropriately share data, while preserving necessary security.

WebLOQ, Inc. -- These specs are much more the 'what', and will need additional technical design fleshing out to arrive at the 'how.' The specs, as they are, are very detailed and completely explain what the project is out to accomplish as a set of overall functional goals. The next step is discover and analyze what technologies are available off-the-shelf to support the overall solution. Then, what Technical Specification needs to be developed to target the specifics of Phasor equipment interfacing and backend database development to deliver the overall solution?

1. Operational questions need addressing, such as who owns and operates the overall network and server infrastructure.
2. If the overarching solution operates as a quasi-public body, what is the governing entity and the management decision structure?
3. What is the cost participation model under which the services are established and maintained?

4. Is this an amalgamation of existing energy company networks with open Internet transport, routed through distributed servers under the control of a private or public entity?
5. If a pilot project is anticipated, prior to letting the project development contract, the Pilot project specs will need scoping in the light of components not yet developed, and with an eye towards a rough proof-of-concept and discovery of COTS technologies that might contribute to the final solution.
6. A complete Technical Specification will be required. This could be developed by a lead vendor and partially sub-contracted to participating developers, or carried entirely by a developing prime contractor.
7. The high performance requirements of this spec, given the packet transmission rates described, will require the least imposition of encryption overhead and very high network performance. A study of real-world connectivity available at Phasor equipment locations and robustness of network connections might well drive data aggregation techniques that will be required to achieve project goals.

RTI -- Concerning the network middleware components of the specification, in the opinion of RTI the elements as specified will adequately meet NASPInet goals. Note that this view is limited to network software aspects of the specification

Duke Energy -- The specified Phasor Gateway and Data Bus meet NASPINet's current goals. It seems the software/hardware plan has been thought out and is adequate for its 10 year lifetime. However, there is a lack of information addressing how increased deployment and communications will be handled over the proposed 30 year lifetime of the entire NASPINet. Additional considerations should include communications medium upgrades (potentially to a medium we do not currently use), necessary bandwidth availability (especially if the phasor system reaches the potential to eliminate the existing SCADA system), how unexpected applications of phasor measurements will be integrated, potential storage requirements, etc.

Open Geospatial Consortium -- No. See comment above and other comments.

ABB Inc. -- NASPINet/Phasor Gateway should be able to identify and correct for time synchronization errors in PMUs and PDCs before communicating synchrophasors from these devices.

BBN -- The current version is (but) one way to realize the desired NASPInet capabilities. Certainly not the only way, and likely not the best way.

ISO-NE -- The NASPInet approach, utilizing a phasor gateway and data bus, appears to be a good first step toward standardization of phasor data on a broad scale, using a distributed design. However, in order to fully respond ISONE would require more information about the analysis and monitoring tools that will be made available on top of the PG and DB facilities. In addition, as indicated in the specifications, the NASPInet solution may be challenged to meet the scalability requirements that may be imposed as the number of PMU's and PDC's continue to grow.

3) Are these specifications adequately designed to be interoperable, enabling the use of diverse applications, data collection devices, and hardware at both ends of the data collection and data use efforts, to make sure that all elements work together effectively? If not, what changes are needed to these specifications to ensure we can build an interoperability testing regime upon these specifications?

Advanced Fusion Systems -- The main weakness is that there are no requirements that the communications network be built to withstand a major electromagnetic pulse (EMP) from nuclear or solar sources. If there is damage to the electrical grid, there will also be damage to the communications network so that information about the EMP-caused grid outages cannot be reported and dealt with. Protection against EMP needs to be a high priority for NASPInet.

PJM -- In general the specifications list all these functional requirements, however without testing at component and device levels, and at an end-to-end system level on a prototype installation, it will be difficult to verify.

BPA -- No. Although there are many references to interoperability, device exchangeability, multi-vendor development of diverse applications, there is still room in these specifications for a very few vendors to essentially lock in a preferential role. There are many potential solutions, including our suggestion in response to question #1. We believe additional effort should be made to insure this effort does not result in vendor lock-in.

WebLOQ, Inc. -- These specs discuss at length the need for high degrees of interoperability, but do not yet get to the level of technical detail such that the broad goals of interoperability can be baked into the planned solution. It is probably most critical that the application, security and transport layers of NASPInet be abstracted from the data collection, applications and other end-point equipment. This can be accomplished through Application Program Interfaces (APIs) that enable simple data handoffs through XML type conversations. Furthermore, abstracting the handoff in this fashion will allow vendors of new equipment to easily create compatible **interfaces without compromising the security of the basic network.**

RTI -- Concerning interoperability, RTI notes that middleware standards, specifically the Object Management Group (OMG) Data Distribution Service (DDS) for Real-Time Systems specification, provide most of the attributes sought. There are multiple DDS implementations by commercial vendors available.

Ameren Services -- Based upon the item above and because of the criticality of this defined initiative we challenge whether the procurement of the PG and DB (and NAPSInet WAN) should be decentralized and allocated to the respective utility (or other NAPSInet participating entity) as the documents specify. To ensure maximum interoperability, it appears it would be in this initiatives' best interest for a central governmental agency maintain primary responsibility for the Data Bus and PG technology evaluations and solution selection processes and allow utilities to acquire these solutions through a common procurement vehicle managed by this central agency. Under this approach, the DOE's NETL and/or NERC (or other appropriate government entities) would be considered the 'PD_REQUESTER' and "DB_REQUESTER' as

referred to throughout the documents to ensure the solution selected is consistent and therefore caters to the highest level of interoperability. Individual utilities (or other NAPSInet participating entities) would still need the Implementation and Sustainment services to integrate these solutions into their respective enterprises).

Should the DOE/NERC consider an RFI process with these specifications to determine the amount of functionality identified within these specifications that exists in the current market vs. needing to be developed? This may provide a validation check to see what degree of functionality exists and identify whether major gaps exist between vendor solutions that could impeded the desired level of interoperability.

Duke Energy -- The specifications adequately address interoperability.

Open Geospatial Consortium -- No, not with respect to geospatial services and encodings. See comments following the questions. (**Others** Section below).

ABB Inc. -- The Phasor Gateway should have a phasor user management system that controls access to synchrophasors. This is similar to users access rights. This ensures that only authorized parties can gain access to controlled set of synchrophasors such as for example those use for wide area control.

BBN -- The APIs are not really APIs at all. For example it does not show function signatures that one application can use to engage another. Everything is stated as "will include the following information for example..". This leaves many things unspecified; and the implementors will make different assumptions leading to integration nightmare, defeating the purpose of having the API.

ISO-NE -- No (see answer to question 1)

4) Are the NASPInet Data Bus and Phasor Gateway specifications sufficiently detailed to ensure that when different organizations and entities build regional phasor communications infrastructure using these specifications, the resulting regional demonstrations will be able to integrate and interoperate effectively without substantive revision or redesign? Are the interfaces and means for information exchange sufficiently clear that critical data and reliability information can flow effectively between regional and individual company NASPInet implementations? If not, what changes are needed to these specifications to attain these outcomes?

PJM -- If the network is to support only streaming Synchrophasor data, the specifications are sufficient provided integration/interoperability is ensured. If the system is to support a variety of wide area monitoring and control capabilities as well as exchange of historical data, it is less certain as to whether or not the specifications are sufficiently detailed.

BPA -- Yes, provided that the APIs are developed and available quickly.

WebLOQ, Inc. -- These functional specs describe the areas and varied situations where interoperability between existing and newly built networks must be easy to achieve. It would be unrealistic to expect all companies and networks to modify existing applications and protocols to conform to NASPInet requirements. These specs should be extended into a Technical Specification that details the neutral handoff data formats such that disparate networks and equipment can interface with minimal effort through local API processes. At the handoff point, which is presumed to be behind a firewall, the reformatted data would drop into and out of the NASPInet fully secured environment and move to and from servers and other networks independent of the local processes.

This API technology should be a well designed GUI-based application that permits the definition of equipment, applications, processes and data exchange tables without direct programming. By providing neutral beachhead facilities at all the edges, NASPInet participants should be able to seamlessly accommodate any external connectivity and data exchange.

RTI -- RTI has concerns regarding the maturity of the interface specifications for NASPInet. In our experience, no specification is complete and inevitably revisions to the specification will be required unless a mature, data-centric foundational middleware specification is selected.

Duke Energy -- The specifications should allow regional phasor systems to communicate effectively with the gateway and receive data from other systems.

Open Geospatial Consortium, Inc. -- No, not with respect to geospatial services and encodings. See comments following the questions. (**Others** Section below).

BBN -- As stated above, many aspects are left unspecified. Control of realtime behavior across entities is suspect.

ISO-NE -- If the specifications are augmented with adequate technical details, as indicated in the answer to 1, then there would be a high probability of interoperability between implementations.

5) Do these specifications draw upon all relevant, existing national or international standards for communications, data, hardware or software? Given NASPInet's goals and functions, what, if any, relevant standards from other industries that perform parallel services can or should be incorporated into the NASPInet design or specifications?

PJM -- The system should draw upon several IEC (61850, 61970) standards.

WAPA -- Our primary observation is that the NASPInet as described in the specifications is a huge leap from the current WECC synchronized phasor network. Although we understand the key design principles stated in the specifications, the Phasor Gateway and Data Bus concepts seem so complex and sophisticated given today's technology as to be nearly unattainable. The NASPInet appears to incorporate services that have not been tested and implemented by end-users.

BPA -- These specifications should be compared with Internet2 specifications and standards.

WebLOQ, Inc. -- The broad realm of international standards applies to this project. There may be data exchange standards specific to the industry that will directly affect design considerations. All international encryption standards apply directly, but advanced security solutions may bring added capabilities that improve overall functionality and usability.

RTI -- As noted, the Object Management Group (OMG) Data Distribution Service (DDS) for Real-Time Systems specification should be investigated and incorporated. The related OMG Real-Time Publish-Subscribe (RTPS) interoperability wire protocol should likewise be investigated and incorporated.

Duke Energy -- Duke is unaware of additional standards that need to be included in these specifications.

Open Geospatial Consortium -- No, not with respect to geospatial services and encodings. Open geospatial standards from OGC and ISO TC/211 (and a few other organizations) really need to be incorporated. See comments following the questions (**Others** Section below).

ABB, Inc. -- NASPINet should make reference to all applicable standards cited by NIST in its Smart Grid Interoperability Standards Framework. The devices and systems proposed must be capable of being upward compatible with respect to the future communication systems.

BBN -- It uses all the current buzzwords (SOA, Web Service, pub-sub etc etc), but this is going to be a long lived infrastructure-- we should not be tieing ourselves too closely with standards that may be transient or still undergoing debate and change and become obsolete in 2 years (vs tieing to an abstract interface representing the important concept),. NASPInet should be designed for change-- evolution/easy upgradability and maintenance is an aspect that has not had much consideration in this document.

ISO-NE -- The specifications do not appear to leverage existing reliable messaging standards for the Energy industry, such as those described in IEC/TR 62325 (aka, ISO 15000-2:2004)

6) Since NASPInet constitutes both a communications and data exchange service, what security and cyber security measures need to be built into NASPInet to assure the crucial reliability of the bulk electric system? Do the Phasor Gateway and Data Bus specifications contain adequate, integrated cyber security provisions? What, if any, additional cyber security measures or considerations should be added?

Advanced Fusion Systems -- You list many requirements for cyber security but nothing for EMP security. If it is not specified, your proposals will not include it. The only item that I found that even reflects a broader need is:
"Fault Tolerance - The ability of a component, service, or system to operate satisfactorily under anomalous conditions such as traffic flow degradation, equipment failure, configuration management errors, and other errors that could affect overall system availability. [4]"
There should be as much about EMP protection as there is about cyber security as the threat is just as great if not more so.

PJM -- The functional specifications adequately address integration of the cyber security provisions. Efficient implementation of those provisions will be a challenge. Also, because there will be multiple architectural options to achieve these cyber security measures, it would be important to agree on and adopt a design to facilitate more detailed specifications for the system.

Entergy -- Entergy submits that when in eventual production operation NASPInet will have direct salience for national and economic security. In other words, should this network infrastructure be manipulated or cyber-crippled by unfriendly forces, dire consequences for the nation are entirely possible. Accordingly, Entergy suggests that NASPInet WAN requirements should not be specified entirely in “functional” terms, i.e., go beyond just ‘what’ and go a bit more into the ‘how.’ Specifically, we recommend consideration of a hybrid functional/technical specification that dictates:

- NASPInet WAN should not be fielded using a shared or public “value added” commercial “network service.” At scale, this network will require very high capacity bandwidth to support steady state operations. If NASPInet traffic is mixed with other carrier customer traffic in a “cloud” competing for internal bandwidth and switching/routing cycles it will be very difficult to do proper trending, tuning, and predictive network enhancement necessary to attend stated throughput and latency performance requirements in any way approaching a “deterministic” data transmission system. There are also security issues...

- NASPInet procurement specifications should call out use of dedicated circuits between at least core NASPInet routers, regardless of point-to-point mesh or SONET rings in manifestation (or both). The requirement for “dedicated” physical data network transmission circuits and associated networking equipment is very much necessary. [Note: Avoid use of the term “private” circuits, as this has different implications as commonly used in commercial network carrier service parlance.]

- National Communication Service (NCS) fiber optic cable plant should be used for core backbone NASPInet WAN network links as much as possible; use of other

federal, network carrier, and utility dedicated circuits should be carefully researched for potential use in NASPInet WAN build-out.

- Use of “virtual” logical overlays on the physical infrastructure should be avoided (or greatly minimized) to facilitate instantaneous and unambiguous operator awareness and understanding of the exact infrastructure assets in use and where, especially when experiencing a widespread ‘event’ regardless of cause (storm, hacker, etc.). It can be very hard to readily troubleshoot and recover ‘virtual networks’ when time is of the essence…

- Fully integrated and dedicated network (DB) and systems management (PG) systems and related tools, including security tools, should be built in at the onset of the pilot prototype implementation, and later production roll-out.

- If the proposition that NASPInet will one day have direct significance for national and economic security is conceded, then use of end-to-end reliable protocols (e.g., TCP) is critically necessary to assure data integrity.

BPA -- These seem sufficient. Additional considerations could include a formal risk based assessment using the Australia / New Zealand Risk Management Standard.

WebLOQ -- Within these specs, the security goals are broadly defined. We believe the security issues of this project are so pervasive and of such importance that they will dominate the overall application architecture design. Once security (encryption, authentication, key management, etc.) have been designed into the transport and database layers, the remaining issues are end-point device interfacing, database schema and operations policies. The extremely critical operations of the NASPInet layer will require that the security components operate at every level and interconnect across all end point devices, server-side operations and all transport in between.

The security of NASPInet must reach through the participating companies’ networks and attach to Phasor equipment while not impeding local operations. This imposes sophisticated security requirements that will be difficult to implement if not designed well enough to work seamlessly in heterogeneous environments and without extensive engineering efforts on the part of local IT management. The good news is that this is known science and there are solutions today that can meet this goal.

It will not be enough to simply encrypt packets in motion using a single layer solution, such as only content encryption or only a TLS transport wrapper, nor will central private/public key stores be the right model to withstand a determined cyber attack. This project will need a distributed and highly defensible key management structure that is transparent to end point devices and users, and will survive even a successful server-side or client-side key file compromise without damaging effect.

Given the wide reach and the many participants in this project it is most likely unrealistic and unwise to place key exchange or key management in the hands of the many individuals involved. We recommend a machine-based large key exchange mechanism that is session based within the application layer and operates independent of end-user involvement – only under the control of a central authority. (Most encryption projects fail

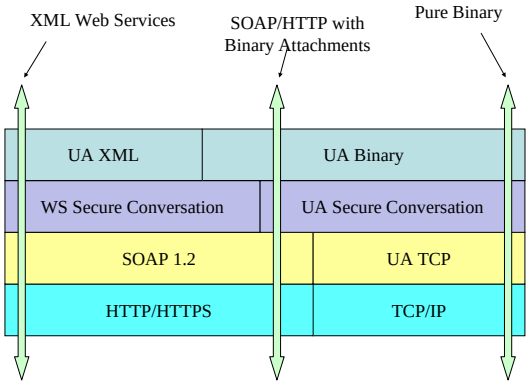
around this very sensitive key management issue – an exposure that NASPInet simply cannot afford.)

We also believe that the management of authentication and certificates should not be exposed to the many participants but should be provided internal to the NASPInet applications layer and be transparent to all operations – only under the control of a central authority.

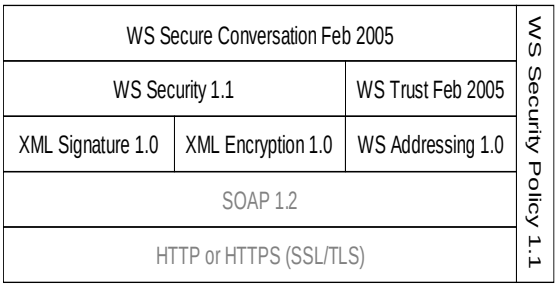
Additional considerations might be securing all email and other critical communications in a way that is integral to NASPInet, delivering to all participants a complete and secure ecosystem for protecting not only the operating data for the grid, but all communications associated with those operations. The logging and reporting of all transactions is another component that should be integral to the overall design. This will allow detailed tracking of all Phasor Gateway and Data Bus activity with report exporting for grid performance analysis and business intelligence reporting.

RTI -- Concerning Cyber Security, NASPInet should consider including DTLS (Datagram Transport Layer Security, IETF RFC 4347) along with the reference SSL/TLS specification (e.g. in Figure 2-12).

SISCO -- The document lacks specific requirements for security. While the document discusses security options, but no specific security technologies are required. Web Service Security provides a very large number of options. It is difficult to achieve interoperability without limiting the choices to those that are applicable to the utility operations environment. SISCO believes that specific requirements need to be created. Pending verification, SISCO experience in this area leads us to believe that IEC 62541 OPC UA may provide the needed security. IEC 62541 OPC UA includes a set of mandatory authentication profiles based on W3C Web Service standards. The IEC 62541 OPC UA Security profiles are illustrated below.



The IEC 62541 OPC UA Web Service security stack includes many of the WS Security specifications. A closer look of the IEC 62541 OPC UA Security stack is shown in the figure below:



John Weyer, Cyber Security Subgroup --
REGARDING HARDENING: The NASPInet should be hardened against electromagnetic disturbances (EMD) to include severe solar storms, and intentional electromagnetic interference (IEMI) such as electromagnetic pulse (EMP) from High-altitude EMP (HEMP) and locale facility EMP/microwave attacks.

- The Cold War standard used by the U.S. armed forces STRATEGIC UNITS of 50,000 volts-per-meter needs to be upgraded to the Russian/Chinese and possibly terrorist capability of 200,000 volts-per-meter at the center of the line-of-sight per the EMP Commission. The E3 effect in severe solar storms and HEMP is potentially the most destructive to long lines such as power lines (above and buried), pipelines, antennas, and so on.
- The IEC and IEEE are advancing on the commercial EMP standards; a team will be needed from the power industry to accelerate the EMP/Microware protection standards needed by this industry.

REGARDING THE DATA BUS: The power generation and transmission grid is the most critical national infrastructure for all other critical national infrastructures rely upon this system.

- (According to the EMP Commission, if the power grid goes out for a year or more 80% or more of the U.S. population expires. The critical path is the loss of the large transformers, which currently have a one to four year wait for new orders for only a few hundred units per year.)
- The power grid NASPInet needs a dedicated and secure data buss.
- During the Cold war AT&T and Western Union maintained dedicated and secure communication systems for the U.S. government / armed forces. They involved heavily redundant systems of microwave towers and buried coaxial cables that covered most of the U.S. (Map attached of AT&T long lines system.) Why not consider this abandoned system for the skeleton of a dedicated spine for the data buss? The redundancy of microwave towers and fibre-optic cable systems would allow rerouting traffic around compromised / damaged portions of the NASPInet. Local networks would feed into the national spine and a very high level of security would be applied at that entry points. Also, the local networks could transmit and receive information by both a fibre-optic cable system and microwave towers.

Duke Energy -- The specifications contain adequate security provisions for the way the data are currently planned to be used by Duke. Duke Energy currently does not consider the phasor data infrastructure to be critical to the operation of any critical assets, but this may very well change in the future. In light of this eventuality, Duke supports EEI's comments in regard to the recognition of the importance of data and data communication security.

Open Geospatial Consortium -- The OGC's main focus is not cyber security, though work is ongoing in the OGC on secure communications that involve geospatial data, and OGC testbeds have addressed critical infrastructure protection. Security of the bulk electric system involves knowledge about the locations of critical physical grid components (including Phasors), and security is one of many areas in which the heavily spatial world of the utilities intersects other heavily spatial worlds: emergency management, disaster management, civil engineering, weather, etc. All of these worlds are moving decisively in the direction of open geospatial standards.

ABB Inc. -- Overall it looks like security has been addressed well and maybe the goals are set a bit too high.

- Section 7.2.1 Access Control in the PG Spec states "access to PG shall provide authentication of valid users with encrypted passwords on the network and ...". This should be rephrased because encrypting the password only does not provide any security. It should read something like "access to PG shall provide authentication of valid users with passwords that are protected in transit using encrypted sessions". A better approach would be to use a challenge-response scheme where the password itself is never transmitted.
- Sections 7.2.2 and 7.2.3 talk about performance impact of Malware scanners and integrity verification. The wording used is "without significantly impacting". There must be a definition of what a significant impact is.

BBN -- It starts to cover some of the basics and essential aspects, but doesn't go nearly far enough either now or to enable a happy future, for something which is destined to become part of critical national infrastructure. As a critical infrastructure with national footprint, we really should be thinking about "survivability" not just security and cyber-security and network-level security. For example, a key aspect may be to design the system in such a way that it can still continue to function with backup, and/or to provide useful service even if cyber-attacks or other failures cripple or compromise parts of it Timely recovery from failure and the idea of constantly improving defenses over time are key elements that are missing.

SCE -- In general, security in these specifications seems to be relegated to a strong focus on confidentiality (encryption), with moderate thought put into access control and auditing. Many of the other aspects of security seem to have received lesser priority. Specifically, the highest levels of security abstraction are widely regarded as confidentiality, integrity, and availability (sometimes called the "CIA" or "AIC" triad). Most Everything else (e.g., access control and auditing) can be viewed as services or functions that support the AIC triad. This specification does talk about security measures for availability and integrity in many places in the document, but they are not always cast as "security" issues. In some ways this point could be considered a petty "turf"

perspective, but when it comes to security one needs to be able to look at it from the top-down as well as the bottom-up and come to a level of confidence that all issues have been covered. I am not there yet with this document as it feels like security has been given consideration all over, but in varying levels of concentration and without a real cohesive and uniform plan.

ISO-NE -- NASPInet may contain critical energy infrastructure information (CEII) and therefore could be subject to NERC and FERC security requirements for CEII.

7) Other Comments

i) Comments on steps needs prior to implementing NASPInet:

PJM -- Several of the concepts, proposed as well as desired for the smart grid technologies, need to be explored in a pilot installation before adopting them for the industry.

ENTERGY -- We do not perceive that certain important and valuable sources of ancillary assistance and collaboration have been utilized to the best extent possible. Examples include:

- DOE Roadmap to Secure Control Systems Program and DOE Lab R&D projects, e.g., OPSAID, Hallmark, HMI/visualization, wireless research; encryption and digital certificate management; implementation conventions for IPSEC and IPv6;

- Related DOD, DHS, and NSF-sponsored research in progress and planned, such as the emergent DARPA "National Cyber Range" test bed initiative;

- Internet Engineering Task Force (IETF) guidance on most-current DOD Protocol Suite ("TCP/IP") stacks and relevant emerging draft standards on the near horizon, especially in the area of high-volume data streaming protocols.

Several recent technology developments associated with the above activities appear to have direct salience for application in design and implementation of NASPInet. All of the above sources of assistance should be considered prior to fielding even a live pilot prototype implementation, discussed next.

Prior to attempting full scale production procurement and roll-out of NASPInet, a limited but fully-functional prototype pilot project should be specified, procured, implemented, and live-operated for some period of time, analogously equivalent to the ARPAnet project of the early 1970s as antecedent to the Internet. We believe it essential to test, tune, and further adjust the refined specifications for application functionality, technical integration methods, services, and administrative and managerial ways and means based upon real world experience. Many important lessons will be learned in so doing. Additionally:

- The prototype pilot sites should be carefully chosen for immediate leveragability value that can be realized from real time wide area phase angle measurement capability, and execution of related PMU applications;

- Only C and D Classes of Service as defined in the specifications should be fielded in the pilot prototype, at least at the outset. Doing just this will provide much improved wide area real time grid situational awareness, as well as deliver richer data sets needed for better post event forensic analyses as called for in the recommendations subsequent to the August, 2003 NE Blackout. If all goes well in the pilot concerning Classes C & D Service, experimentation with Class B Service then could be undertaken as well.

- Class A Service is beyond the state of current commercial-off-the-shelf (COTS) wide area network technology to deliver in real world application, given the tolerance limits stipulated for latency and throughput. An entirely separate wave of longer term basic academic and DOE lab R&D well may be necessary to one day realize Class A service in practice – this should be undertaken separately.

- We further submit that serious reconsideration be given to whether or not to support Class E service within the same network infrastructure expected to deliver performance levels needed to support at least B and C Classes of Service (to say nothing of Class A). Use of the Internet or even off-line physical shipment (e.g., on hard disk drives) of the huge data volumes associated with Class E Service should be considered.

Entergy submits that the subject specifications are good and necessary work, but are not yet adequately refined for direct use in a procurement action aimed at practical widespread near term instantiation of NASPInet.

We submit that the NASPInet specification development process has been "overcome by events" to such a degree that another phase of more wide ranging, coordinated, requirements assessment and specification refinement is necessary. Specifically:

- NIST Smart Grid work is rapidly progressing in parallel with the NASPInet project, and it is generally expected (e.g., in the FERC Smart Grid Policy statement of earlier this year) that NASPInet is logically the next generation situational awareness and controls fabric for Transmission (and to some degree Distribution) at the core of Smart Grid. How do NASPInet specifications dovetail with Smart Grid thinking and standards being adopted for it?

- Similarly, NERC has issued a Standards Authorization Request (SAR) to create a drafting team to establish standards for next generation operational "real time situational awareness tools" for the bulk electric system. This activity and NASPInet certainly appear to have similar if not entirely in-common objectives. Are there conflicts?

- The NERC "CS_706_SDT" standards drafting team currently re-crafting the NERC CIP Standards certainly has an interest in how NASPInet is conceived and implemented. This drafting team has a level of maturity in thinking in these technical areas that can constructively contribute in refinement of the PG and DB specifications.

Based upon the findings and results of the suggested live pilot prototype exercise, formal procurement instruments can then be prepared in confidence that hidden challenges of production roll-out have been uncovered and adequately embraced.

Vernacular confusion: Current NASPInet PG and DB logical constructs within the specification documents are not necessarily "wrong," but they are arbitrary and conceived from a language frame of reference apart from mainstream networked-computing engineering. As presented, these logical constructs will be confusing to mainstream networked-computing subject matter experts and products and service providers alike, because they are contrary to long established generally accepted linguistic conventions, design concepts, system-building, and procurement practices

long predicated on the International Standards Organization's (ISO) Reference Model for Open Systems Interconnection, first embraced world-wide in the late 1970's.

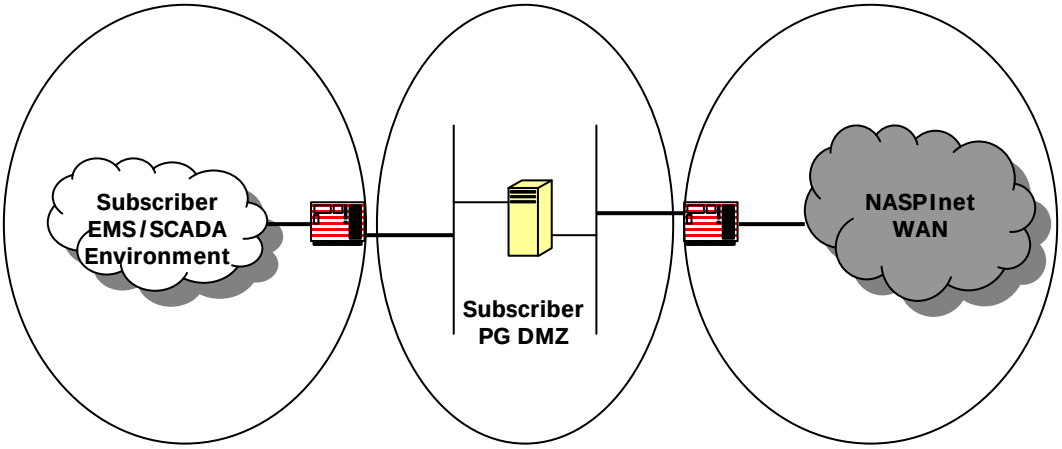
The NASPInet design concept should uncouple the PG and the DB. The NASPInet design concept depicted on the front cover of the design specifications shows both the PG and DB within the same logical conceptual box. At a high level of abstraction this may be fine, but the depiction is misleading in terms of the best way to actually define, procure, and implement the pieces of the overall solution set in practice.

The inter-network, data link, and physical layer protocols that will provide the NASPInet WAN data transport function of the system are technologically and commercially reduced to practice. Desired PG applications must be newly developed. This is one major reason why the NASPInet WAN can and should be procured, assembled, operated and managed independently of PG (host) applications, data, middleware, and related software.

Defining NASPInet to include "everything" – DB and PG alike – unnecessarily complicates things in a number of ways. 'Someone' will have to design, procure, install, operate and maintain "everything" as part of the backbone network service. Network service carriers know how to implement and operate backbones and access circuits as routine business – but not PG's and the ancillary things that will go along with it. They will be "$pecials" with special operating and maintenance logistics for the carrier that accordingly will have special pricing. What's more, allowing subscriber organizations to build their own PGs will not be a notion easily entertained by the network service provider. DOE/NERC will want service level agreements (SLA) with the carrier, and the carrier will only enter into those if it has complete and total control of "everything" as the specifications currently define them. A la carte "roll your own" PGs do not fit that bill. As currently conceived, DOE/NERC (or its agent) will have to manage "everything" as part of the greater service, or pay the carrier to do so at significant mark-up. This interjects unnecessary complexity (and/or cost) for the program on an ongoing basis – not just at service establishment. Break-fix maintenance of the entire assembly would be "the program's problem," necessitating additional resources and manpower (and/or cost) to facilitate. An important objective should be to minimize administrative burden for DOE/NERC to a small staff vs. a small horde.

We suggest that the current two-part concept of NASPInet (PG+DB as one part) plus subscriber private systems (as the second part) should be broken up into effectively three components: 1) NASPInet WAN; 2) Subscriber PG DMZ; and, 3) Subscriber EMS/SCADA Environment, as depicted below.

Recommended 3-Part NASPInet Conceptualization



- NASPInet WAN – NASPInet subscribers will want (and/or need) varying levels of performance and capability. Key subscribers (e.g., large IOUs) will need higher throughput and availability, and low latency service performance characteristics. This will require more robust network interconnections (e.g. multiple local loop access circuits, higher bandwidth, and bigger routers), and this will and rightly should cost more to implement and operate on an ongoing basis. This cost should be directly borne by the subscriber, according to need.

  In RFP specifications, require the carrier to propose:
  - Network service access circuit options differentiated by a variety of sustained throughput (not "port speed") bandwidth options DS1 and above
  - A suite of small-to-large IP routers for use at the customer sites;
  - A flat rate per mile for access circuits, regardless of locale (if you can get away with it – they may not bite – new construction is often necessary).

The point of demarcation between the customer premises and the NASPInet WAN would be the Ethernet/IP port on the subscriber side of the network carrier- provided site router. The network provider's router is itself connected to the NASPInet WAN by one or more local "access circuits" or "tails circuits" customized for the specific customer site scenario. Subscribers would order and coordinate installation of the access circuit(s) and router(s) directly from the provider of the network service backbone – ordering from a "contract menu" offering different gradations of bandwidth/routers. Installation of the access circuit is always a custom affair, entirely dependent upon the specific unique situation at each subscriber site. Accordingly the subscriber would engage the carrier organization directly to work out implementation logistics and details. Approached this way, both initial installation and ongoing monthly service costs can be direct-billed to the subscriber, and DOE/NERC can avoid being in the middle of these administrative transactions. This is the exact carrier-customer paradigm routinely employed today throughout the world, and variance from this well established practice for NASPInet should be avoided.

- The Subscriber PG DMZ should be owned and operated by individual subscriber organizations. The PG box(es) itself would be attached to two small subnetworks, one on either side as depicted. Each subnet would actually be instantiated by LAN switches (in place of the vertical lines above), and each subnet could have various other (e.g., security) devices attached. On the Subscriber EMS/SCADA Environment side, either discrete router/firewall devices would be implemented, or a router with a firewall feature set installed. Given that NASPInet will be a "closed user group" community, it may be advantageous to simply employ access control lists (ACL) on the carrier- provided router in place of a full-blown firewall. With more details in hand, further consideration and pilot activity would identify the best approach.

  Center stage in the Subscriber PG DMZ is of course the application software, middleware, and all other NASPI-specific software services and utilities. The procurement instrument would focus on these items, and the ancillary COTS hardware needed to physically instantiate the DMZ could simply be listed as things the bidding vendor is required to include in the package (if a "bundle" is desired). For a subscriber wishing to develop code itself, the COTS hardware simply becomes a 'grocery list' of things to independently acquire.

  The procurement specification guidelines originally initiated by the State of NY and SANS, and later fully fleshed-out at Idaho National Labs, should be relied upon heavily to guide procurement specification of the Subscriber PG DMZ.

- The Subscriber EMS/SCADA Environment would technically be beyond the scope of the NASPInet initiative being undertaken by DOE/NERC. While the subscriber would acquire and operate PMU/PDC independently, certainly cooperative coordinated configurations and parameter-settings are essential.

The requirement for a PG-to-DB "Application Programming Interfaces" (API) is at cross purposes with stated Objectives and Principles. The current NASPInet design concept must better adhere to generally accepted networked-computing concepts and conventions, and in so doing well-established commercial network service vending practices, in order to attain the Objectives and Principles described in the Architectural Foundations section of the specifications. The current design concept is at cross purposes with hard won practical lessons about protocol layering, open systems, clean demarcation of ownership, operational management responsibilities, and security best practices; and also the stated objectives to use COTS technology, provision of a build-your-own PG option for subscribers, ease of entry both technically and cost-wise, and the ability to customize network interfaces appropriate to end user size and need.

At the heart of the incongruity with stated goals is the use of API between the PG and the DB in the specification design concept. In essence, the specifications call for a merging of network, transport, and session protocol layer functionalities into the interface between the PG and DB. While this may be attractive for a future academic basic R&D project, we do not feel this is a practical approach to fielding NASPInet in the near term within the confines of the stated Objectives and Principles. There should be no API between a PG – a host computer – at the interface with the DB, which is a router (intervening firewall notwithstanding). The interoperable interface between the PG and the subscriber's NASPInet interface router should simply be Internet Protocol (IP) datagrams (and associated IP layer service protocols). The PG is a "host" computer, and

any/all application and middleware interactions should be between end points – end-PG-to-end-PG, i.e., "host-to-host" – independent of the wide area data transmission system (NASPInet WAN) used to shuttle application semaphores and data between them. Doing otherwise, such as adoption of "distributed real-time embedded"(DRE) concepts, literally requires either invention of a brand new part-host/part-network device, or two completely new devices speaking some to-date nonexistent API protocol or suite of protocols. This is what the current specifications dictate, and this flies squarely in the face of the stated Architectural Foundation Objectives and Principles. All PG-to-PG middleware data streaming management software, service utility applications (e.g., security, name resolution services, etc.), and NASPI application suites should be resident and execute on PG and PG alone. PG should be described in the specification, procured, and implemented simply as "host" computers that attach in common to the NASPInet WAN, and inter-process across it with peer utility PG. This is by far the more generally accepted best practice than the approach taken in the specifications.

Little needs to be invented from scratch. By following the recommendation to steer away from use of custom APIs between PG and DB as the design concept is now conceived, at a high level of abstraction only three (major) things have to be originally developed: a) the PG application software and service-request management middleware; b) API code that PMU (and PDC and/or commercial historian products) will be required to employ to 'talk to' the PG host applications; and, 3) end user visualization software (which already may be well along in development in DOE labs). The PG itself can be fielded using a properly configured COTS "quad-core PC"/server (or less, probably), and all other ancillary network/security/utility hardware devices would also be readily acquired COTS products. The more COTS technology employed, the greater the minimization of risk to the initiative overall. Consequently, the hard parts of this initiative are significantly reduced, makes contracting for and development of the PG software more compartmentalized, and facilitates the desired option of letting subscribers acquire their own PG hardware and develop the code in-house. But mixing PG middleware with network transmission equipment software is a horse of another color altogether.

SISCO -- Inclusion of Class A traffic for protection in requirements: Figure 2-5, 2-8, and 2-9 show Utility Operations Components connected to Utility Substation Components via Phasor Gateways. Section 3.1.1 includes a discussion of Class A (protection) traffic. Both of these aspects of the documents imply that NASPINet is to be used for protection and control. SISCO believes that it is unlikely utilities will want to use the same network to exchange data with utilities/ISO's/RTO's for near real time control over the same network to exchange data with external entities for non critical non real time exchange such as historical queries. SISCO's experience with NercNet (SISCO acted as coordinator during that rollout), leads us to believe that there will need to be multiple networks of some sort. While one could prioritize traffic based on who is asking for it and what they are asking for, the way the system is currently described, a utility Phasor Gateway only has one connection to NASPINet. This can mean that a connection may become loaded up with non-critical requests and be slow to respond to critical more real time requests.

SISCO believes that protection should be handled in a way that extends the existing standard ways of today. For example, IEC 61850 provides networking technology that can be used for Wide Area Protection and Control (WAMPAC) and is supported by virtually all major protection equipment supplies including SEL, GE, ABB, Siemens, and

Areva. If protection is done using this industry accepted way, there is no requirement for NASPINet to handle Class A traffic for protection. While NASPINet may convey the Class A traffic, it should not be used for protection, but rather for monitoring.

If NASPINet only handles Class A traffic for monitoring, the requirements for NASPINet can be significantly relaxed. In this case, NASPINet can be created largely using off the shelf software currently available from multiple utility software vendors.

SISCO strongly recommends the use of a Service Oriented Architecture (SOA) that leverages W3C Web Service technology. This is accepted industry best practice and can be used to successfully construct NASPINet. For instance IEC 61970 Part 502-8 specifies Web Service based technology that could be used.

ii) Others

Southern -- Southern Company believes the NASPInet Phasor Gateway and Data Bus Specifications offer adequate detail, specificity and flexibility to meet the intended purpose.

We see potential value in the Phasor Gateway being used as a central hub for all phasor data, both internal and external. This will provide a clean data interface for phasor applications and possibly historians. Is it intended that the owner of the Phasor Gateway be allowed to subscribe to the owner's data?

If so, should this be identified as a requirement in the spec? Internal data subscription should not introduce additional data bus traffic if properly implemented.

WAPA -- Western Area Power Administration (Western) has reviewed the two NASPInet specifications primarily to understand the NASPI effort. We have the following general comments.

We agree with the concept of creating “a robust, widely available and secure synchronized data (synchrophasor) measurement infrastructure for the interconnected North American electric power system with associated analysis, monitoring tools for better planning and operation, and with improved reliability” (NASPI mission). Western has been involved with the Wide Area Measurements effort for over 15 years. We purchased and installed the BPA Phasor Data Concentrator (PDC) in November 1998. Western and BPA set up a communication channel to exchange real-time PDC data in 2005. Today, the WECC synchronized phasor network includes BPA, Western, CAISO, PG&E, and SCE. Western currently has 5 PMUs installed in its service territory.

The NASPInet specifications as distributed would serve well as a road map for an advanced synchrophasor data network. Use of standards such as IEEE C37.118-2005 "IEEE Standard for Synchrophasors for Power Systems" would allow building from the synchrophasor data infrastructure already in place. From a utility perspective, we would want to see a series of assessment tests for technical feasibility and estimates of NASPInet costs before adopting such a complex data network.

Entergy -- I don’t think the specs are ready for prime time as they are. We had too many power system engineers and ivory tower academics involved in this networked-computing design conceptualization, and far too few seasoned large scale data network

engineers and users. In my comments I've proposed an intermediary (to production procurement and roll-out) "live pilot prototype" project analogous to what ARPAnet was to the Internet. The first phase of that work would be to "refine" the specs by involving a wider community of expertise... I see this initiative as mondo important in the grand scheme of things – as in "Smart Grid Backbone"… If we don't screw it up…

EEI -- EEI relies on its member companies to provide detailed responses to the questions in the June 15 letter, and provides three general comments here:
First, a detailed management and business plan is needed for the synchrophasor initiative. The electric industry needs focused discussion and decisions on a sustainable long-term business platform. EEI understands that some DOE and NERC personnel and budget resources have been available over the past year and various planning and implementation issues are being addressed. This is important and useful work, however, the complexity of both the data collection and management, and technical specifications of this project, and the critical electric system functions that synchrophasor data will support, indicate a strong need for a clear long-term business plan.

Second, in conjunction with the development of a business plan, the ongoing funding of this initiative needs to be settled. To ensure a sustainable funding source, EEI believes that the electric industry should consider an independent entity for managing and funding the synchrophasor initiative. This suggests to EEI that NERC and the electric industry should explicitly address NERC corporate policy on the nature of NERC's role in this specific initiative, as well as for other technical programs and activities that support BPS planning and operations. The electric industry should make clear decisions that ensure sustainable methods are in place for both the necessary funding and administrative support.

Third, EEI strongly recommends that the synchrophasor initiative recognize the importance of cyber security for data and data communication. As you know, these data will be used in the future by realtime system operations functions, which will rely on very high levels of data and communications integrity. Especially during challenging system events and disturbances, operations personnel will increasingly rely on highly detailed visibility and diagnostic tools based on these data. Cyber security and communications systems require strong levels of protection.

BPA -- BPA wishes to reinforce there should be no "fee-based components" required to interface with or use the data bus. Also, all needed documentation must be publicly available and (nominally) free.

We were struck that no reference in either document was made to energy efficiency. While performance must trump energy efficiency, the physical equipment selection must include a requirement for energy efficiency considerations.

In the data bus specification:
Section 8.2.1.1 "Steady State" - We suggest that steady state include a substantial amount of 60 phasor per second traffic. BPA plans to move to a 60 phasor per second rate as our default. We want the additional measurement bandwidth for control and disturbance analysis. Our specific test suggestions are:
item 3: 70% at 60 phasors per second
15% at 30

15% at 10
item 4: 70% at 60 phasors per second
15% at 30
15% at 10

Section 8.2.1.1 "High Activity State" - Ditto for the high activity state; a much higher rate of all registered analog and digital streaming data signals. Our specific test suggestions are:
item 3: 100% at 60 phasors per second
item 4: 100% at 60 phasors per second

Section 8.2.3 "System Latency" - Change the historical data transfer size from 30 minutes to one hour.

Section 9.10.2 "System Noise" - Is it realistic? Our understanding of server class hardware makes us doubt, but do support it if it's realistic.

For the gateway specification:
We also noticed the same noise spec in section 9.10.2 as for the DB an have the same reservations.

If we really wanted to cover the future (and stress the NASPInet systems), we should include traffic at 120 phasors per second for both the DB and the PG.

The PG spec spells out the functional requirements in great detail. It does not spell out the PG to PG data format (including security). This opens a risk that a specific manufacture's PG will (likely) only communicate with other PGs built by the same manufacturer and this is not tenable. Multiple manufacturers' phasor gateways must fit into the bus - gateway architecture.

Dr. George Kusic -- Include data snapshots of the power system around each PMU. This snapshot should be comprised of line flows (MW,MVARs) on the lines near the PMU's as well as injections (MW,MVAR) near the PMU's. This will enable State Estimation calculations to determine bus voltages and phase angles. In the event there is a blackout, this data will provide faster re-connection of islanded power systems.

Data snapshots plus phasor information can also be used to determine transmission line parameters. There are many IEEE transaction papers on parameter determination with phasor measurements.

WebLOQ -- The current state of increasing cyber warfare makes the success of this grid management project extremely critical to national security. To protect the national grid from a potentially disastrous penetration will require that the security components of the project achieve the highest level of protection possible, and that the protection extend to all aspects, companies and equipment that might be attacked. Even though many portions of the NASPInet network may be on dedicated circuits, recent experience has taught that any TCP/IP network has open Internet exposure at some point, and is therefore potentially vulnerable.
Our primary observation about this project is that to build a complete application solution from scratch that is largely about the security system - bringing in the enabling

technologies such as encryption, authentication, key management, certificates, the database, etc. and paying for the extensive project development schedule to create a totally secure platform that meets the complex needs of this project – would be a large, complicated and risky venture. The foundation technology to deliver a powerful solution in much less time, with a much higher probability of success, already exists.

We hope that our observations and answers are helpful. As this project comes together, WebLOQ would welcome the opportunity to present in detail how its highly advanced and high-performance security ecosystem could dramatically collapse time to significant results, greatly reduce the risks inherent in any complex software project, meet and exceed presently declared project goals, and deliver a robust and flexible solution that can be rapidly deployed and easily plugged into any existing or planned network.

Consumers Energy -- In addition to ensuring cyber security issues, we feel access to the information must also be addressed. The information could be misused to gain market power.

GE Energy T&D --

1. It is specifically defined a base sampling rate of 30 times/sec will be used in NASPInet (Ref. Section B, Project Background, in Quanta's document of Statement of Work). It means that the actual sampling rate in the PMUs and PDCs of individual utilities can only be one or multiples of the base rate. However, NASPInet is required to support other real time data from IEDs that generally do not have such high sampling rate, how should those data be aligned with the phasor data?

2. Keep consistency on naming convention for the Data Bus. It is better to call it Phasor Data Bus (PB) or Phasor Bus (PB), rather than the general term of Data Bus (DB), being consistent with the Phasor Gateway (PG), Phasor Data Concentrator (PDC), etc.

3. The Data classes/priority numbers should be able to be redefined by users.

4. The two SPECs only talk about the phasor gateway and data bus architecture to deal with the phasor data, without addressing how these data will refer to the corresponding network models. Moreover, the phasor data are closely coupled with the network topology driven by the switch statuses. Without correct mapping the topology to the requesters, the phasor data are not useful at all.

Hydro One Networks Inc. -- Reviewed from the point of view of the system working in the Ontario environment and not whether the NASPInet product is good or not. I assume it will work and do its job. The Ontario situation is different from the US, where there are many small utilities in each reliability region. This system is described to fit the US model.

Hydro One Background understanding:

1. The NASPInet is just the mechanism for exchanging PMU data between utilities and the ISO/RTOs (similar to ICCP for the exchange of existing data). It does not affect the PMU data within a utility. HONI would acquire all PMU data within Ontario from its own PDC. HONI would only need the NASPInet if to acquire PMU data from outside Ontario, and for its obligation to supply others with the PMU data.

2. The Areva State Estimator (SE) at OGCC (A control Centre) that would use the PMU data, would still converge without the PMU data, at least for the foreseeable future.

3. The Areva e-terraVision product could be used to visualize the PMU data. It would acquire the Ontario PMU data from the PDC.

4. NASPInet will be needed to send the PMU data from HONI to the IESO.

5. NASPInet would be needed to see the big picture affecting Ontario (e.g. flow around lake Erie), and for utilities in US to see into Ontario

Hydro One Comments on Tendering documents:

1. Not clear that the tendering documents requires redundant PGs to be capable of operating in separate computer rooms. OGCC has the requirement that the NMS continue to function with the loss of 1 computer room. The tendering specification states that the redundant PGs should have no common components, but that does not mean that they can operate in different computer rooms. Also, the entire system must be set up to operate in separate computer rooms, that includes the switches, routers as well as the PGs. The tendering document should state that the NASPI net should be designed to operate in redundant computer rooms separated by more than 300m, and have no loss of function if one computer room is lost. (this should also apply to the Data Bus (DB components). I know this is not a unique requirement to HONI (e.g. PJM operates similarly).

2. It is not clear from the tendering documents that the backup centre would function. The backup centre operates completely separately from the main control centre . That would require the PG at backup centre to be separate from the PG at the main control centre. I am not sure that two independent PGs can be registered. The PG registration ID for the main centre could not be passed to the backup centre, similarly all the PMU and data stream registration and encryption codes could not be passed between the 2 control centres. That tendering documentation should clearly require that a second independently registered PG can re-register PMU data and terminate the registrations that are already in progress. This needs to be done in a secure manner.

3. There is no statement about regional self sufficiency in the tendering document, e.g. Ontario should be able to function even if communication is lost with facilities outside Ontario, that is PMU data exchanged between HONI and the IESO. This should be added to the Data Bus specification.

SISCO -- While the document says that NASPINet should be able to carry data other than phasor data, the document does not describe what other data needs to be included

sufficiently. SISCO believes that at least two other types of data should be considered early in the deployment of NASPINet.

a) Power system modeling data – Phasor data is of very limited usefulness without a network model. IEC 61970 provides several ways for utilities to share model data. The use of IEC 61970 should be required included.
b) Alarming and Eventing – In order to attain Wide Area Situational Awareness (WASA), it is helpful to exchange alarms. This does not mean that Utility A gets all Utility B's alarms. Rather, Utility B should be able to act as a smart alarm processor for Uitlity A by only providing Utility A the alarms it needs to know about. IEC 61970 related technology provides a way for utilities to share alarm data.

There is a lack of references to standards. The document should reference:

c) IEC 61850 for protection and control as well as other standards as shown below:

IEC	57	10	61850-3	General requirements
IEC	57	10	61850-4	System and project management
IEC	57	10	61850-5	Communication requirements for functions and device models
IEC	57	10	61850-6	Configuration description language for communication in electrical substations related to IEDs
IEC	57	10	61850-7-1	Basic communication structure – Principles and models
IEC	57	10	61850-7-2	Basic communication structure – Abstract communication service interface (ACSI)
IEC	57	10	61850-7-3	Basic communication – Common data classes
IEC	57	10	61850-7-4	Basic communication structure for power utility automation – Compatible logical node classes and data object classes
IEC	57	10	61850-7-410	Hydroelectric power plants - Communication for monitoring and control
IEC	57	10	61850-7-420	Basic communication structure - Distributed energy resources logical nodes
IEC	57	10	61850-8-1	Specific communication service mapping (SCSM) – Mappings to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
IEC	57	10	61850-9-2	Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3
IEC	57	10	61850-10	Conformance testing
IEC	57	10	61850-90-1	Using IEC 61850 for the communication between substations
IEC	57	19	61850-90-2	Using IEC 61850 for the communication between substations and control centers
IEC	38	37	61869-9-2	Digital interface for instrument transformers
IEC	17C	11	62271-3	High-voltage switchgear and control gear - Part 3: Digital interfaces based on IEC 61850

d) IEC 61970 for network model sharing and web service based technology to be used as the NASPINet services, as well as other standards as shown below. Note that IEC 61970 Part 502-8 includes IEC 62541 as a normative reference:

IEC	65E	8	IEC 62541-1	OPC Unified Architecture Specification - Part 1: Overview and Concepts
IEC	65E	8	IEC 62541-2	OPC Unified Architecture Specification - Part 2: Security Model
IEC	65E	8	IEC 62541-3	OPC Unified Architecture Specification - Part 3: Address Space Model
IEC	65E	8	IEC 62541-4	OPC Unified Architecture Specification - Part 4: Services
IEC	65E	8	IEC 62541-5	OPC Unified Architecture Specification - Part 5: Information Model
IEC	65E	8	IEC 62541-6	OPC Unified Architecture Specification - Part 6: Mappings
IEC	65E	8	IEC 62541-7	OPC Unified Architecture Specification - Part 7: Profiles
IEC	65E	8	IEC 62541-8	OPC Unified Architecture Specification - Part 8: Data Access
IEC	65E	8	IEC 62541-9	OPC Unified Architecture Specification - Part 9: Alarms
IEC	65E	8	IEC 62541-10	OPC Unified Architecture Specification - Part 10: Programs
IEC	57	13	61970-1	EMSAPI – Part 1: Guidelines and General Requirements
IEC	57	13	61970-2	EMSAPI – Part 2: Glossary
IEC	57	13	61970-301	EMSAPI – Part 301: Common Information Model (CIM) Base
IEC	57	13	61850-90-1	Using IEC 61850 for the communication between substations
IEC	57	13	61970-502-8	CIM Data Services
IEC	57	13	61970-454	Naming Service

IEC 61970 SISCO believes that IEC TC 57 standards should be used if they meet the stated requirements. SISCO believes that exchange of current and historical phasor data can be exchanged using existing IEC 61970 standard services as well as the new web service versions. The existing OPC COM base services are supported by major utility software vendors including: Siemens, ABB, Areva, GE, OSIsoft, and SEL. For NASPINet, the new IEC 61970 Part 502-8 Web Services (IEC 502-8 applies IEC 62541 OPC UA to the exchange of utility data) should be used so that other non PMU data such as COMTRADE may also be exchanged. SISCO believes IEC 62541 OPC Unified Architecture and IEC 61970 Part 502-8 CIM Data Services meet all the stated requirements. IEC 62541 OPC UA employs W3C SOA standards and can provide the following functionality:

(1) Role based access control to the signal (variable) level.
(2) Publish/Subscribe

(3) Current and historical data access
(4) Performance optimizations required for utility operations
(5) High availability and reliability
(6) Naming Services. It should be noted that the document discusses naming services but does not mention an IEC 61970 draft standard that matches up with the stated requirements very well. SISCO recommends that a reference to draft IEC 61970 Part 454 Naming Service be added to the specification. Significantly, IEC 61970 Part 454 enables integration of NASPINet with other national initiatives such as NercNet (ICCP data exchange) and the Common Power System Model (CPSM) exchange (CIM model exchange between regions). SISCO believes it does not make sense to employ entirely different technology, tools, and methods for NASPINet. Instead, NASPINet can be positioned as being complementary and easily integrated with the other initiatives. It should noted that a network based on IEC 61970 can support NercNet, CPSM exchange, and NASPINet.Data Bus

While C37.118 should be used to covey phasor data from PMU's or PDC's to the Phasor Gateway, the use of C37.118 should not be used as the protocol for NASPINet Data Bus. C37.118 does not support

(7) Role based access control to the signal (variable) level.
(8) Publish/Subscribe
(9) Current and historical data access
(10) High availability and reliability
(11) Service Oriented Architecture

Section 2.3 suggests that the use of C37.118 on the wire is preferred for phasor data exchange on the NASPINet Data Bus because the not using C37.118 could break existing NASPI applications. This suggests that existing NASPI applications have been written directly over C37.118 instead of over a network neutral API. This architecture should be avoided as it goes against commonly accepted programming practices for the following reasons:

ii) Applications will need to change when ever the network protocol changes. C37.118 is a relatively new protocol that is subject to revision. For example, SISCO has identified several issues with C37.118 error handling. SISCO believes C37.118 is a useful protocol for PMU data monitoring, but that the protocol needs revision. Issues with C37.118 include:
   (1) Not readily integrated with substation protection, automation, and engineering
      (a) Protection – C37.118 only specifies the use of TCP or UDP protocols. Without access to lower layers of the communication protocol stack, it is difficult to reserve communication path bandwidth and set the data delivery priority. Consequently, phasor data transmitted using C37.118 cannot be used for reliable system protection.
      (b) Automation - C37.118 doesn't reuse IEC 61850 data semantics or the communication protocol. Existing substation automation equipment cannot receive C37.118. This greatly increases the cost of using PMU data in substations.
      (c) Engineering – There is no standard way to describe a PMU in IEC 61850 Substation Configuration Language (SCL). Consequently there is no way to configure a PMU off line.
   (2) C37.118 only supports continuous streaming of data

(a) Support for event driven exchange is needed where PMU data is only sent upon the occurrence of an event.

(3) Miscellaneous protocol issues

(a) There are numerous C37.118 error handling issues that need to be resolved. Consequently, C37.118 cannot be described as a highly reliable protocol.

(4) No context to data on the wire. Having a larger device context would allow phasor data to be more easily integrated into the larger substation architecture

iii) The documents suggest that Web Services and SOA are a preferred integration technique, but since C37.118 complies with neither Web Services or SOA, recoding of the applications will be required if Web Services and/or SOA is used in the future.

iv) Continuing to directly code to C37.118 will mean an unstable and bifurcated development environment for applications. It will cost a significantly more money to maintain applications coded directly to C37.118.

Section 3.1.1 lacks specific requirements for the different classes of traffic. SISCO SISCO recommends that NASPI use the message performance classes defined in IEC 61850-5. The Clause 13.7 Message types and performance classes include:

e) 13.7.1 Type 1 – Fast messages: This type of message typically contains a simple binary code containing data, command or simple message, for example “Trip”, “Close”, “Reclose order”, “Start”, “Stop”, “Block”, “Unblock”, “Trigger”, “Release”, “State change”, maybe also “State” for some functions. The receiving IED will normally act immediately in some way by the related function on receipt of this type of message since, otherwise, no fast messages are needed.

f) 13.7.1.1 Type 1A “Trip”: The trip is the most important fast message in the substation. Therefore, this message has more demanding requirements compared to all other fast messages. The same performance may be requested for interlocking, intertrips and logic discrimination between protection functions.

i) For Performance Class P1, the total transmission time shall be in the order of half a cycle. Therefore, 10 ms is defined.

ii) For Performance Class P2/3, the total transmission time shall be below the order of a quarter of a cycle. Therefore, 3 ms is defined.

g) 13.7.1.2 Type 1B “Others”: All other fast messages are important for the interaction of the automation system with the process but have less demanding requirements compared to the trip.

i) For Performance Class P1, the total transmission time shall be less than or equal to 100 ms.

ii) For Performance Class P2/3, the total transmission time shall be in the order of one cycle. Therefore, 20 ms is defined)

h) 13.7.2 Type 2 – Medium speed messages: These are messages, as defined in 13.7.1, where the time at which the message originated is important but where the transmission time is less critical. It is expected that IEDs will have their own clocks. The message shall include a time-tag set by the sender, and the receiver will normally react after an internal time delay, which then will be calculated from the time given in the time-tag. Normal “state” information also belongs to this type of message. This type may alternatively include a single measurand, such as a r.m.s. value calculated from type 4 signals. The total transmission time shall be less than 100 ms.

i) 13.7.3 Type 3 – Low speed messages: This type includes complex messages that may require being time-tagged. This type should be used for slow speed auto-control functions, transmission of event records, reading or changing set-point values and general presentation of system data. Whether a time-tag is required (normally) or not (exception) will be stated by the actual application. Time tagged alarms and events for normal alarm/event handling and non-electrical measurands such as temperature also belong to this type, but some automatic functions in general and some dedicated values (for example pressure) of generally slow-speed functions may request message type 2. The total transmission time shall be less than 500 ms.

j) 13.7.4 Type 4 – Raw data messages: This message type includes the output data from digitizing transducers and digital instrument transformers independent from the transducer technology (magnetic, optic, etc.). The data will consist of continuous streams of synchronized data from each IED, interleaved with data from other IED.

Table 1 – Raw data for protection and control

Data type	Class	Transmission time (ms) defined by trip time	Resolution (Bits) Amplitude	Rate (Samples/s) Frequency
Voltage	P1	10,0	13	480
Current			13	
Voltage	P2	3,0	16	960
Current			16	
Voltage	P3	3,0	16	1 920
Current			18	

For convenience, the resolution is given in bits.

Table 2 – Raw data for metering

Data type	Class	Accuracy classes and harmonics	Resolution (Bits) Amplitude	Rate (Samples/s) Frequency
Voltage	M1	Class 0.5 (IEC 62053-22) Class 0.2 (IEC 60044-8) Up to 5th harmonic	12	1 500
Current			14	
Voltage	M2	Class 0.2 (IEC 62053-22) Class 0.1 (IEC 60044-8) Up to 13th harmonic	14	4 000
Current			16	
Voltage	M3	Class 0.1 (not defined by IEC) Up to 40th harmonic	16	12 000
Current			18	

For convenience, the resolution is given in bits.

Formosa Utility Venture Ltd. -- Based on what has been reviewed of the documentation. Formosa Utility Venture Ltd has no comments based on infrastructure communications which would be on transmission provider side

Ameren -- Ameren endorses the comments and position submitted by Edison Electric Institute (EEI) and shares their concerns for the long term funding & sustainability of this project as well as the concerns regarding strong cyber security controls in the overall design.

The specifications appear to be very comprehensive and sufficiently scope the functional requirements of the stated NASPInet concepts and goals.

In some instances throughout the document several APIs are provide as 'an example'. I comment whether these references be made more absolute (and perhaps mandatory) to increase interoperability.

OGC -- Because all smart grid devices, including Phasor Measuring Units (PMUs), have geospatial parameters, and because geospatial parameters are critical in many or most smart grid use cases, the Open Geospatial Consortium, Inc. (OGC) has offered input into NIST's smart grid standards effort.

With respect to the North American SynchroPhasor Initiative (NASPI), our suggestion is that there be discussion between OGC participants and NASPI participants to ensure that NASPI participants make informed decisions about whether or not to take advantage of the OGC's open standards, standards expertise and consensus standards process. The paragraphs below point out some of the areas that might be discussed to determine whether the OGC can offer value to NASPI.

NASPInet's Class A and Class B data services require communication of geospatial data, but these services' performance requirements will undoubtedly exceed what is possible with OGC Web Services (OWS) because of current Web technologies' limitations with respect to managing low latency response and fast and uninterrupted data flow. However, work done in the OGC's Sensor Web Enablement (http://www.opengeospatial.org/ogc/markets-technologies/swe) activity has addressed real-time and data streaming requirements, and some of this work might be useful to NASPI. We recommend discussion between OWS/SWE experts and NASPI experts to determine the degree to which OGC's work in this area might serve the NASPI mission. The discussion should cover a number of topics, including transducer (phasor) management, data reduction/transformation, rights management, subscribe/unsubscribe, and data quality. Regarding data quality, developers of NASPInet may find value in a recent OGC Discussion Paper, UncertML, which provides a conceptual model and XML encoding designed for encapsulating probabilistic uncertainties, and it may be used to quantify and exchange complex uncertainties in data.

It is important to note that not all of the OGC's standards are Web service standards. For example, the OpenGIS(r) Geographic Objects Interface Standard (GOS) provides an open set of common, lightweight, language-independent abstractions for describing, managing, rendering, and manipulating geometric and geographic objects within an application programming environment. It provides both an abstract object standard (in UML) and a programming-language-specific profile (in Java). The language-specific bindings serve as an open Application Program Interface (API). GOS might be useful in the context of NASPInet Class A and Class B standards development work.

It would be good to think about the role that open standards for sensor communication might play in the future, in the event that PMUs and other NASPInet components will need to handle other sensor inputs. For example, the smart grid will likely be employed to provide unprecedented levels of power quality to support use of ever more sophisticated electronic devices that may be employed in grid management or in homes and businesses. This may involve new kinds of measurement. And the smart grid, and particularly smarter PMUs, will enable unprecedented maximization of grid resources, which will likely require more widespread and sophisticated measurement of line temperatures, weather, etc. Thus, because PMUs may, in the future, be extended to enable management of other kinds of sensors and controls, conformance with open sensor communication standards, including the OGC's SWE standards, should be considered.

NASPInet Class C, D, and E data services involve visualization, analysis, modeling, and research. Because all such activities (Figure 2-3 in the NASPInet Phasor Gateway Specification shows the scope) sometimes involve using geospatial tools and geospatial data not created specifically for power transmission monitoring and control applications, it appears to us that it would be highly desireable for NASPInet applications to implement geospatial service and encoding standards from OGC and other standards development organizations (ISO TC/211, in particular) that work on geospatial standards. OGC and ISO

TC/211 standards are widely implemented by software and data vendors and widely used by those vendors' customers.

NASPI should look at the OGC Web Service interface standards, but the one OGC standard that will almost certainly find a role is the OGC Geography Markup Language (GML) Encoding Standard, an XML extension that can be used to encode all types of geospatial data and can also be scaled down for lightweight applications such as the GML application schema in the Internet Engineering Task Force (IETF) Presence Information Data Format (PIDF-LO) standard for location payloads. PIDF-LO, designed for communicating privacy-sensitive presence information, is being incorporated into numerous other Internet standards. One such standard is the Session Initiation Protocol (SIP), currently documented as RFC 3261 from the IETF Network Working Group, which will likely play in important role as part of the smart grid standards framework. GML is already part of the International Electrotechnical Commission (IEC) Common Information Model (CIM) standard.

From the outset, one of the OGC's goals has been to develop and promote international open standards, and we have been successful in doing this. NASPI focuses on North America, but all major nations are beginning to look seriously at developing smarter grids, and what transpires in North America will surely influence other nations and world regions. One positive benefit of mandating international open standards will be increased industry innovation and trading opportunities, as well as a faster global progress away from dependence on problematic fuels.

Southwest Power Pool -- Southwest Power Pool is in full support of the NERC, NASPI initiative to network current and future Phasor Measurement Units. Southwest Power Pool values the advantage of the increased data stream for voltages, currents, and frequency data. Also, we see a strong value in the further enhancement of data exchange across all RTO’s and ISO’s nationwide. We also see this as a necessity

during the development of the Transmission Interstate-Highway backbone. Our strongest concern with the NASPInet project for SPP and our members is the Cyber Security Protection and the specifications from the vendor will ensure the highest possible protection for our members.

XCel Energy -- In general there were no specific concerns identified within the sections of the two technical specifications. General architecture, technical viability, and security are more than adequate for vendor use in the development effort. General comments were identified and are listed below:

- In section 7 of the Phasor Gateway and Databus document there is not sufficient detail on what the requirements are to meet CIP compliance, it is thought that section would contain specific detail on configuration of strong passwords, authentication at access points, reporting, etc. The only CIP requirements specifically mentioned are CIP 5 & 7, no where does it discuss physical security boundaries for entities (vendor or participant). All regulatory standards should be explicitly listed
- Many utilities are not on the IPv6 standard, if that's a prerequisite it may have significant impacts to participant systems.

CAT-1 -- While providing an excellent communication infrastructure for phasors, the NASPInet also has the potential to readily bring wide area situational awareness to other technologies essential to grid reliability. Given the intellectual capital, time, and money to be invested in the deployment of the NASPInet, we suggest that the specifications be expanded to specifically accommodate those technologies that complement phasors and synergistically enhance the grid's reliability and its ability to serve the electric consumer. For example, phasors manage the electrical aspects of the grid (voltage, stability) while dynamic line ratings manage the grid's capacity (amount of power that can be safely transferred within thermal design limits and while maintaining line to ground clearances). The two technologies are complementary, both vary in time, and both are essential to the reliability and efficiency of the grid. In fact, one might consider combining phasors and dynamic line ratings into one service to address all 3 of the key elements (voltage, stability, capacity) that govern grid performance and reliability.

In keeping with its intended mission, the NASPInet's specification necessarily focuses on the specialized transfer requirements of phasor data. That focus may or may not be well suited to accommodating the transfer of other types of data with differing underlying requirements. To that end, it may be advantageous to incorporate into the NASPInet specification an arbitration layer that provides for the integration of non-phasor data, such as dynamic ratings, in a standardized way. For example, the arbitration layer might consist of an OPC server interface. OPC is a very widely used non-proprietary technical specification that can provide interoperability between the NASPInet and virtually any type of data or device. The presence of an arbitration layer can greatly simplify interfacing both legacy and future devices to NASPInet.

We recognize that we have proposed an expansion of NASPInet's use that may go beyond its original scope and intent. However, we believe that the added capabilities and benefits to reliability are a natural extension of NASPInet and are consistent with the goals of the North American SynchroPhasor Initiative, the North American Electric Reliability Corporation, and the U.S. Department of Energy. We would welcome the

opportunity to answer any questions and to actively contribute to any evaluation you may choose to pursue.

AEP Transmission Asset Management -- Networking and Communication Requirements

1) Responsibilities

It is confusing on who provides what:

Under 1.5.1 (of Phasor Gateway Specification), the "PG_SUPPLIER" responsibilities shall include:

- Procure, design, build, integrate, test, ship, install and perform site acceptance test and commissioning of all components of the PG
- Supply PG communication links and interfaces needed to satisfy PG_REQUESTER's requirements

Under 1.5.2 (of Phasor Gateway Specification), the "PG_REQUESTER" responsibilities shall include:

Provide the necessary LAN/WAN infrastructure for connecting the PG to DB and PG_REQUESTER's information systems to the PG.
Seems unclear on the who is providing network infrastructure and circuits.

2) MPLS vs. Dedicated Pt to Pt circuits

MPLS is heavily promoted now by the telephone companies due to cost advantages and ability to support QoS (packets that have been marked and honored for prioritization). A company like AEP would have a circuit that connects into the MPLS cloud. It is not clear whether they are seeking to build out the network (connections from Data Bus to Phasor Gateway) using MPLS technology and leverage the major carriers (more than one will be required since redundancy is required) or establish point to point dedicated circuits from a utility to the Data Bus point of entry. It is not clear what the Data Bus network looks like and it's WAN points of entry for utilities.

3) Redundancy

There are several references to redundancy. Redundancy can be interpreted in many different ways. It needs to be very clear what is required concerning redundancy of network equipment, interfaces, circuits, physical layer (routes, fiber, conduits), power, etc.

4) Bandwidth

I understand the bandwidth requirements will be calculated based on the amount of data that is subscribed/published. The diagrams (maybe they just used these as examples) imply OC-12 (622 Mbps) or OC-48 (2.488 Gbps) which are extremely large pipes which could be VERY costly especially if redundant circuits are required. As a reference, AEP's entire Internet usage is around 200 Mbps. I don't have a feel for who is funding the various components.

Where possible, Ethernet circuits (anything from 5 Mbps to 1000 Mbps) are becoming more readily available and scale better (easier to increase bandwidth as needed) than the defined OC-3, OC-12 circuits, etc. Where available they should be optional vs. the fixed rate circuits. With the Ethernet circuits, the hardware interfaces are also less costly.

5) Latency

With the network infrastructure and communications circuits there will be a given latency depending on equipment, mileage of circuits and any congestion issues. The latency across AEP's network and likely across network to Data Bus will be greater than the frequency of messages (60 messages per second or one message every 16.66 mS). Therefore the data will need to be packaged; is there a common specification of how the data is packaged or will the PG_SUPPLIER provide this recommendation?

6) QoS

Five QoS classes (A-E) are spelled out. QoS is typically implemented if there is a chance of congestion (i.e. all bandwidth is utilized), which there may be if large files will be sent and received in ad hoc fashion. Someone will need to be very specific about TCP ports and IP addresses, etc. that will be associated with each of these classes if QoS is to be implemented. (Not sure if it is in this specification or PG_Supplier spells this out). BTW, are there any additional QoS requirements needed internally across AEP's SCADA network (PMU to PDC?).

Southern California Edison -- The document references NIST SP800-30 and FISMA. The document alludes to the NERC CIP's, although not as directly. This is are good references, but there are several more security documents out there that could also be referenced. The DHS Control Systems Catalog, The Common Criteria and NIST SP800-53 come to mind off the top of my head.

Traffic performance attributes (classes of data) are all defined relative to the first classification. No measurement/evaluation criteria are provided (that I found), which will make it very difficult to evaluate if they are being met appropriately as well as significantly complicating the task of evaluating security performance trade-offs.

The central access authority (7.1.7 Trust Management in Phasor Gateway spec) is a very significant requirement. I think it will work, but it very much surprised me to run across it this deep in the spec. It was kind of like turning the corner in a maze to find yourself face-to-face with an elephant. Everyone involved needs to understand the implications of this and be on-board. No real detail is given as to how all of this should be worked out.

The document contains a lot of very specific detail about encryption and key management. These are good things to cover in detail, but I am concerned this came at the expense of other aspects of security.

Manitoba Hydro -- The only feedback I can add is some have stated why not build on the existing SMP gateway for the NASPI gateway. In their opinion, it appears one is re-inventing the wheel with the NASPI gateway.

Attachment 1 – Paper submitted by Dr. George Kusic, University of Pittsburgh

USING PHASE MEASUREMENTS IN EXISTING STATE ESTIMATION PROGRAMS

George L. Kusic
Department of Electrical Engineering
University of Pittsburgh
Pittsburgh, PA 15261
kusic@engr.pitt.edu

Nermeen Talaat
Department of Power and Machines
University of Zagazig
Zagazig, Egypt
nermeen_talaat@hotmail.com

ABSTRACT
This paper utilizes phasor measurements at busses of the power network into State Estimation programs without extensive re-coding the software. The advent of the Global Positioning System (GPS) absolute time reference allows voltage phase angles to be measured, then referred to a reference bus. Bus real power injections are updated between State Estimator iterations to satisfy phase measurements. The phasor measurement also allows line current measurements to be resolved into a real part proportional to real power. Up to this time current measurements were not used because they degrade convergence of the State Estimation algorithm.

KEY WORDS
Phasor measurements, current measurements, State Estimation, snapshot data

1. Introduction

A Phase Measurement Unit (PMU) is a transmission line monitoring device first used in mid-1980s. PMU's are equipped with Global Positioning System (GPS) receivers for time synchronization of voltage and current phase angles at a given substation. GPS receivers mark identical time synchronization at all points on wide-spread networks [1]. Phadke and co-workers were the first researchers to introduce the use of PMU's and extended the investigation to optimal location of PMU's to monitor the system by a relatively small number of PMU's, much fewer than the number of buses [2-5].

As the PMU's become more inexpensive, their utilization will increase not only for substations and the control center, but for system protection, stability measurements, and transient measurements. One of the most important applications is for system monitoring and observability by the State Estimator. PMU's also have been implemented as a source of information to detect faults on transmission lines [6].

Criteria are developing on the proper placement of the PMU's. Among methods are modified annealing and direct combination. These two methods may be in opposition to each other, such that the optimal placement of the PMU may be a generic search algorithm [7]. In this latter method, the criterion is to maximize the redundancy and observability of the system. Other researchers advocate more criteria added to the optimal placement of PMU's, such as improving the security of the system [8].

In the past few years the National Science Foundation has supported projects that focus on the use of PMU measurements in State Estimators. The principle objective was to investigate methods of determining optimal locations for PMU's so that the system state of an entire power system is observable. Several factors affect how this can be accomplished. Among the factors are the available data from existing conventional measurements, the number and location of zero injection buses, the number and location of installed PMU's [9-10].

The focus of this paper is augmenting existing State Estimators with phasor measurements.

2. State Estimation

State Estimation is a well-known power system monitoring algorithm which is extensively used on 3-phase earth power systems. It is almost a 'standard' program resident in large utilities energy management system computers [11]. The weighted measurements from the power system, such as a line power flow measurement near the *i* bus toward bus *k*, $S_{ik} = z_{m1} + jz_{m2}$ where the complex *j* term is for reactive power, are used in the performance index J :

$$J = \sum_i W_i \left[h_i - z_{mi}\right]^2 = \left(\mathrm{h} - Z\right)^t W \left(\mathrm{h} - Z\right) \qquad (1)$$

The analytic function $h_i(x)$ or vector $\mathrm{h}(x)$ is nonlinear and dependent upon the state vector $x = \left[V \;\; \delta\right]^t$ .The performance index of Eq. (1) is minimized by up-dating the state vector x at each $n+1$ iteration by means of increments calculated in the Newton-Raphson expression:

$$\Delta x = \Delta \begin{vmatrix} V \\ x \end{vmatrix} = -\left|\frac{\partial^2 J}{\partial x^2}\right|^{-1} \frac{\partial J^n}{\partial x} \approx \left[\frac{\partial \mathrm{h}^t}{\partial x} W \frac{\partial \mathrm{h}}{\partial x}\right]^{-1} \frac{\partial J^n}{\partial x} \qquad (2)$$

where only the vector $x = \left[V \;\; \delta\right]^t$ appears in the Jacobian approximation and second-order effects in the Jacobian are ignored. The set of measurements are assumed to be simultaneous, in other words, a 'snapshot' of data without any time skew for processing or averaging of data. This is a valid assumption if the power system changes very slowly in time, and the data acquisition system completes the scan in a short time interval.

The weighting factor, W_i, of each measurement is based upon the accuracy of the measurement:

$$W_i = \frac{K}{\left[c_1 \left|z_{mi}\right| + c_2 (F.S.)\right]^2} \qquad (3)$$

where:

K = Normalization factor for convenient matrix inversion (constant numerical value)

c_1 = accuracy, typically .01, .02

c_2 = transducer and A/D converter accuracy in decimal form, typically 0.0025, 0.005

$F.S.$ = full scale range of the meter

If the weighting factor of a direct phase measurement, δ_{im}, is included in the measurement set and assigned a very large value, the phase angle at that bus is constrained so as to match the measurement. This method forces the least-squares-estimate solution to this phase angle and requires re-writing the computer code.

Let H ≒δh/δx be the linearized gradient evaluated at the final value of the state vector, x. H is used to compute the covariance matrix for the measurements:

$$\Sigma^2 = W^{-1} - H\,[H^t\, W\, H]^{-1}\, H^t \qquad (4)$$

From this matrix, Σ_i is the standard deviation of measurement i and is the square root of the i^{th} diagonal element.

When the standard deviation is used to normalize the residual value

$$\tau = \left|h(X)_i - Z_{mi}\right| / \Sigma_i \qquad (5)$$

for each measurement, the largest among all normalized residuals is the most probable bad data. [11].

3. Phase Measurements

The absolute time reference from the GPS is simultaneously (within nanoseconds) transmitted to transducers in power system generating stations, substations, and field bus locations. Each of these locations communicates with the system control center by means of Remote Terminal Units (RTU's). The RTU's are clocked computers that can be synchronized within several milliseconds to prepare for the advent of a specific GPS timing pulse. The one second pulse is from the IRIG-B train of one second pulses [12]. The arrival of the GPS time pulse starts a pulse counter within the RTU to measure the zero crossing of the voltages at remote locations as shown schematically in figure 1. Also shown in figure 1 is measurement of a line current angle, θ, at bus #2.

As power flow depends on phase differences, the reference bus is set to $\delta = 0.0$ and the phase angle of bus #2 with respect to the reference, as measured by RTU clock counts, is:

$$\delta_2 = \alpha_1 - \alpha_2 = \left(\frac{N_1 - N_2}{N} \right) * 180^0 \tag{6}$$

In Eq. (6), the clocks in both RTU's are assumed to have N counts per ½ power system cycle. The angles can be calibrated for slightly different frequency clocks in the RTU's.

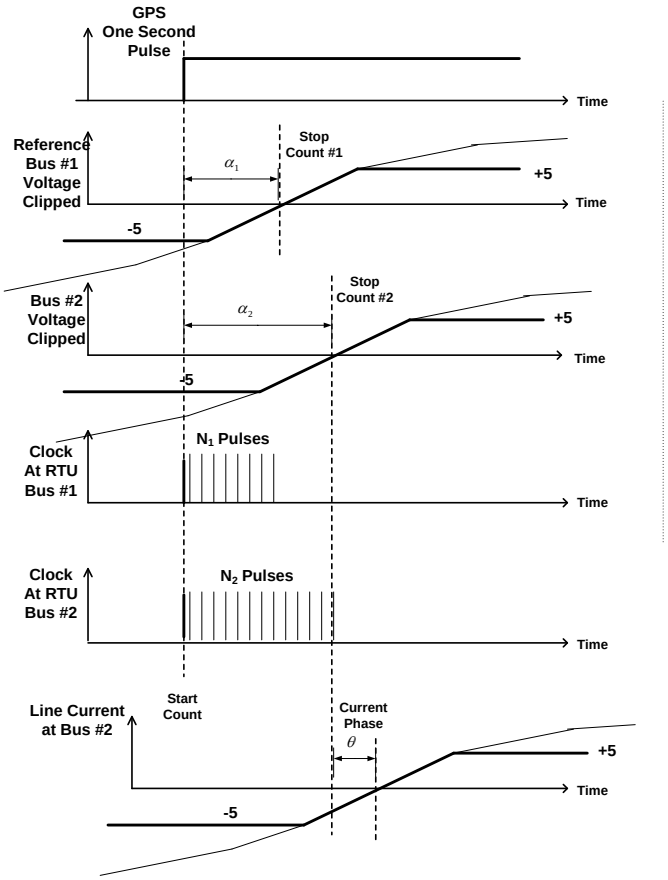


Figure 1. Method to measure voltage and current angles with respect to the GPS time signal

It must be noted that virtually all transmission line voltages and currents at a bus are already available at analog signal levels at the RTU's. The RTU amplifies the signals to achieve a large rate of change at zero crossover, then clips these voltages to +/- 5 volt logic. An And-gate starts the counter when GPS timing and the signal are positive. There are no additional circuits necessary.

The zero crossings of voltage and current signals, as converted from the high voltage power lines, are subject to magnitude and phase shift instrumentation errors in potential and current transformers. It must also be noted that an error of one clock pulse in a 1.0 MHz counter converts into a 0.023 degree phase angle error.

Two cases of modifications to the State Estimator algorithm to accommodate phasor measurements are as follows:

1) The real power injection at a bus is varied between iterations so as satisfy the measured absolute phase angle at the bus. The weighting factor of the calculated injected real power is maintained at the same value as all other measurements.
2) Using the GPS time reference, the power factor angle $\cos(\theta)$ of the transmission line current I_{ik} from bus *i* to bus *k* with respect to the *i* bus voltage is measured. This yields an in-phase component of current that aids convergence of the State Estimator algorithm. This component is obtained from real and reactive power flow

$$S_{ik} = V_i \left| I_{ik} \right| [\cos(\theta) + j \sin(\theta)] = P_{ik} + jQ_{ik}$$
$$z_{mi} = \left| I_{ik} \right| \cos(\theta)$$

It is seen that an in-phase current measurement is redundant to a real power flow measurement. Current flow absolute value measurements are normally discarded from State Estimation because they degrade convergence of the algorithm [13].

4. Network Example

A utility in the Western USA performed Supervisory Control and Data Acquisition (SCADA) snapshot measurements of injections and transmission line flows for the network shown in Fig. 2.

The numerical values for impedance and line charging susceptance for the network of Fig. 2 are specified in Table 1 and a SCADA snapshot for the network is given in Table 2. The SCADA snapshot is as received in the central computer and includes all calibration errors, A/D errors, round off and communication errors.

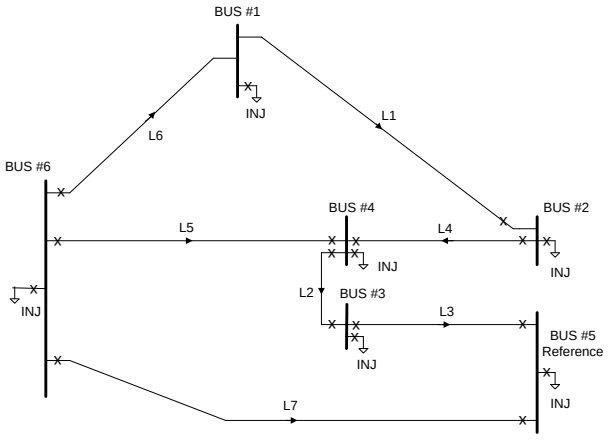


Figure 2. A 138 kV network (X's indicate SCADA measurements)

Table 1
Utility line parameters for Fig. 2 network, p.u.

Line	From	To	R	X	Y
L1	BUS #1	BUS #2	.01390	.04159	.02132
L2	BUS #3	BUS #4	.00181	.01318	.00900
L3	BUS #3	BUS #5	.00174	.01270	.07120
L4	BUS #2	BUS #4	.00435	.01154	.00660
L5	BUS #4	BUS #6	.00590	.03040	.01600
L6	BUS #1	BUS #6	.00200	.00130	.00100
L7	BUS #5	BUS #6	.00460	.03350	.02256

Table 2
Snapshot measurements (N.M. = No Measurement)

L	FrMW	FrMvar	ToMW	ToMvar	Fr/To
L1	N.M.	N.M.	-29.50	9.50	BUS 1-2
L2	-10.60	15.10	10.90	-15.50	BUS 3-4
L3	29.70	-10.10	-27.35	8.02	BUS 5-3
L4	8.02	-7.60	-7.60	-9.40	BUS 4-2
L5	43.20	-15.60	-43.34	15.40	BUS 6-4
L6	92.80	-25.01	N.M.	N.M.	BUS 6-1
L7	35.10	-16.70	-35.50	15.80	BUS 6-5

Injections	MW	Mvar
BUS#1	0.0	0.0
BUS#2	-37.3	0.100
BUS#3	-37.9	23.12
BUS#4	-25.62	7.92
BUS#5	-69.52	14.28
BUS#6	171.1	-57.31

The State Estimator algorithm of section II, with weighting factors $W_i = 1.0$, was performed with all line flow and injection SCADA data of Table 2. This computation converged to $|\Delta x| \leq .00001$ for all busses in 3 iterations. Partial results (injections only) of the computation are shown in Table 3 for the calculated bus voltages and normalized residuals. The quantity **Best Est** is the calculated best estimate for the measurement. The bad data threshold is $\tau = 0.1$, where the real power measurement at bus #1 is the worst among the bad data points. Not shown here is one additional 'bad data' point, the MW line flow from bus #6 to bus #1, which had 0.3353 as the normalized residual.

It is clear from the results of Table 3 that the real power measurement at bus #1 is the worst of the bad data points. This location is therefore a prime location for introducing a phasor measurement.

If the phase angle $\delta_1 = 0.01 rad \rightarrow 0.573^0$ was measured by GPS timing at bus #1, as referenced to $\delta = 0.0^0$ for bus #5, this fixed value measurement could be used to set the real power injection at bus #1.

Let $G_1 + jB_1$ and $G_6 + jB_6$ be the series admittances of transmission lines L1 and L6 respectively. The real power injection at bus #1 was up-dated for State Estimation at the n+1 iteration using calculated $V_1^n, V_2^n, \delta_2^n, V_6^n, \delta_6^n$ from the nth iteration. according to:

$$
\begin{aligned}
P_1^{n+1} &= \left(V_1^{\,n}\right)^2 \left[G_1 + G_6\right] \\
&- V_1^n V_2^n \left[G_1 \cos(\delta_1 - \delta_2^n) + B_1 \sin(\delta_1 - \delta_2^n)\right] \\
&- V_1^n V_6^n \left[G_6 \cos(\delta_1 - \delta_6^n) + B_6 \sin(\delta_1 - \delta_6^n)\right]
\end{aligned} \qquad (7)
$$

With up-dates on the real power injection at bus #1 , the State Estimator calculation took 11 iterations to converge to $|\Delta x| \le .00001$. The results of this computation are shown in Table 4. for only the bus injections. There are no bad data points, for injections or line flows, where the normalized residual is greater than 0.10. Observe that the adjustment of real power at bus #1 forces the State Estimator solution to $\delta_1 = 0.5778 \deg$.

The in-phase component of current computed by the power factor, $|I|\cos(\theta)$, is not yet available from field measurements, such that a power flow computation is used to obtain the current flows on the network. The bus injections listed in Table 2, with exception of bus #5, were used to compute the power flow solution. From this analytic base case solution, the in-phase current components and Mvar out of each transmission line were calculated and used as a snapshot for State Estimation. The snapshot of calculated data is shown in Table 5. Only line flows were used in this State Estimation. The combination of in-phase current and Mvar flow measurements makes the system observable because each line has at least one measurement analogous to real power and one measurement of reactive power. Without the Mvar line flows, the system is not observable, and the State Estimation computation does not converge.

Table 3
State Estimation for snapshot of Table 2

Bus	**Voltage**	**Angle(deg)**		
		meas	**Norm Err**	**Best Est**
BUS1	1.0296	0.7108		
BAD DATA detected for this measurement 1				
	MW p.u.	0.0000	1.6168	-0.3407
	MVAR p.u.	0.0000	0.0557	0.0543
BUS2	1.0310	-0.1550		
	MW p.u.	-0.3730	0.0625	-0.4354
	MVAR p.u.	0.0010	0.0313	0.0323
BUS3	1.0345	-0.2107		
	MW p.u.	-0.3790	0.0284	-0.4074
	MVAR p.u.	0.2312	0.0194	0.2118
BUS4	1.0325	-0.1170		
	MW p.u.	-0.2562	0.0511	-0.3071
	MVAR p.u.	0.0792	0.0033	0.0825
BUS6	1.0306	0.7812		
BAD DATA detected for this measurement 9				
	MW p.u.	1.7110	0.1077	1.6083
	MVAR p.u.	-0.5731	0.0220	-0.5511
BUS5	1.0341	0.0000		
	MW p.u.	-0.0760	0.0362	-0.1122
	MVAR p.u.	0.0570	0.0220	0.0350
Worst Residual 1.6168 Detected at Measurement 1				

Table 4

State Estimation with phase measurement $\delta_1 = 0.01 rad$ at bus #1

Bus	Voltage	Angle (deg)	meas	Norm Err	Best Est
BUS1	1.0287	0.5778			
		MW p.u.	-0.6881	0.0220	-0.6659
		MVAR p.u.	0.0000	0.0549	0.0536
BUS2	1.0311	-0.1349			
		MW p.u.	-0.3730	0.0219	-0.3511
		MVAR p.u.	0.0010	0.0316	0.0326
BUS3	1.0346	-0.1971			
		MW p.u.	-0.3790	0.0036	-0.3826
		MVAR p.u.	0.2312	0.0190	0.2122
BUS4	1.0326	-0.1067			
		MW p.u.	-0.2562	0.0055	-0.2507
		MVAR p.u.	0.0792	0.0052	0.0844
BUS6	1.0302	0.6664			
		MW p.u.	1.7110	0.0127	1.7237
		MVAR p.u.	-0.5731	0.0153	-0.5578
BUS5	1.0341	0.0000			
		MW p.u.	-0.0760	0.0076	-0.0684
		MVAR p.u.	0.0570	0.0221	0.0349

The State Estimation performed with the snapshot of Table 5 is presented in Table 6. Because exact measurements are used, the exact state computed from the power flow is duplicated. The normalized residual of every measurement is therefore zero (less than 0.00005), so numerical round-off in transferring data was not significant.

Table 5
Calculated in-phase line currents and Mvar used for State Estimation with phase measurement

Line	Amps(in)	Mvar(out)	Amps(out)	Fr	To
LINE1	271.6	14.514	-269.8	BUS1	BUS2
LINE2	-256.2	-24.138	257.1	BUS3	BUS4
LINE3	9.25	-0.291	9.25	BUS5	BUS3
LINE4	-7.43	-14.415	7.49	BUS4	BUS2
LINE5	432.0	18.324	-429.5	BUS6	BUS4
LINE6	271.7	16.106	-271.6	BUS6	BUS1
LINE7	500.0	21.589	-496.4	BUS6	BUS5

Table 6
State Estimation performed with line flows of 2 in-phase current measurements and one Mvar flow per transmission line

Bus #1 V = 1.0301

From	To		meas	Norm Err	Best Est
BUS1	BUS2	I		0.3748	0.0000	0.3748
BUS1	BUS6	I		-0.3748	0.0000	-0.3748
BUS1	BUS6	MVAR	0.1611	0.0000	0.1611

Bus #2 V = 1.0311

From	To		meas	Norm Err	Best Est
BUS2	BUS1	I		-0.3723	0.0000	-0.3723
BUS2	BUS1	MVAR	0.1451	0.0000	0.1452
BUS2	BUS4	I		0.0103	0.0000	0.0103

BUS2	BUS4	MVAR	-0.1442	0.0000	-0.1442

Bus #3 V = 1.0350

From	To		meas	Norm Err	Best Est
BUS3	BUS4	I	-0.3536	0.0000	-0.3536
BUS3	BUS5	I	-0.0128	0.0000	-0.0128
BUS3	BUS5	MVAR	-0.0029	0.0000	-0.0029

Bus #4 V = 1.0326

From	To		meas	Norm Err	Best Est
BUS4	BUS3	I	0.3548	0.0000	0.3548
BUS4	BUS3	MVAR	-0.2414	0.0000	-0.2414
BUS4	BUS2	I	-0.0103	0.0000	-0.0102
BUS4	BUS6	I	-0.5927	0.0000	-0.5928
BUS4	BUS6	MVAR	0.1832	0.0000	0.1832

Bus #6 V = 1.0307

From	To		meas	Norm Err	Best Est
BUS6	BUS4	I	0.5962	0.0001	0.5961
BUS6	BUS1	I	0.3749	0.0000	0.3749
BUS6	BUS5	I	0.6900	0.0000	0.6900

Bus #5 V = 1.0346

From	To		meas	Norm Err	Best Est
BUS5	BUS3	I	0.0128	0.0000	0.0128
BUS5	BUS6	I	-0.6850	0.0000	-0.6851
BUS5	BUS6	MVAR	0.2159	0.0000	0.2159

5. Conclusions

Two methods of using the GPS time reference to determine bus voltage phase angle measurements were demonstrated in this paper. The measured voltage phase angles have inherent errors because of the potential transformers used to step transmission voltages down to signal processing levels. There are also errors inherent in the current transformers used to monitor transmission line currents and bring it down to signal processing levels. One method to minimize these errors is to duplicate the same instrumentation at every PMU installation, including the reference bus. In this case, only linearity errors in sensing different magnitudes of voltages or currents become important. Any phase measurement errors are in turn incorporated in real power, reactive power, and current values.

The first method of the paper, variable real power injection at a bus due to measure phase angle, is equivalent to power flow considerations where 2 of the bus conditions -- $P_{in}, Q_{in}, V, \delta$ -- may be held fixed and 2 computed. This method has been used with constant success on several test networks.

The second method, to obtain the line power factor and the in-phase component of current, should be extensively applied in the field. Utilities have many more current measurements than MW or Mvar transducers in substations and other facilities. At the present time these current transformers are not employed in State Estimation because they lack phase information. The in-phase current method can be implemented in the RTU's by means of software operations once a PMU is installed.

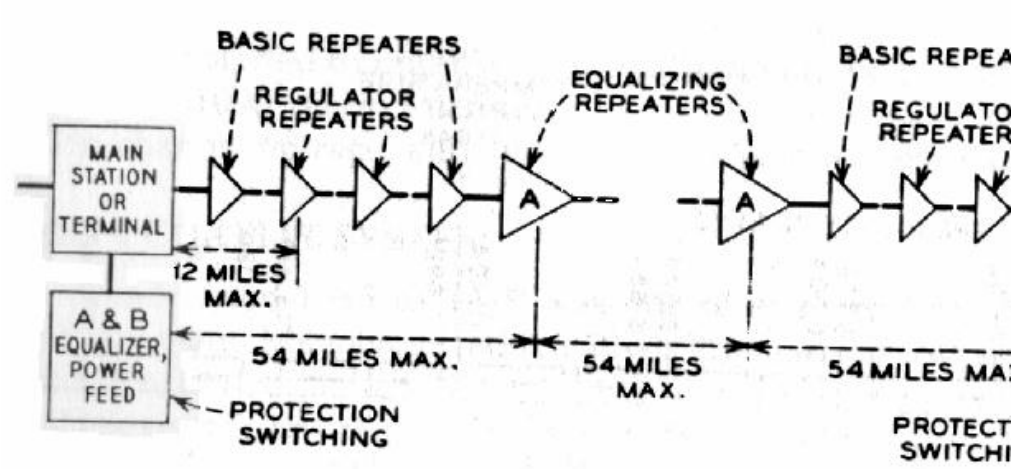
References

[1] K. Chow, J. Shin, S. Hyun, "*Optimal Placement of Phasor Measurement Units with GPS Receiver*," Proceedings of the Power Engineering Society Winter Meeting, Vol. 1, January 2001, pp. 258-262.
[2] A. G. Phadke, "*Synchronized Phasor Measurements in Power Systems*", IEEE Computer Applications in Power, Vol. 6, Issue 2, pp. 10-15, April 1993.
[3] A. G. Phadke, J. S. Thorp, and K. J. Karimi, "*State Estimation with Phasor Measurements*", IEEE Transactions on Power Systems, Vol. 1, No. 1, pp. 233-241, February 1986.
[4] T. L. Baldwin, L. Mili, M. B. Boisen, and R. Adapa, "*Power System Observability With Minimal Phasor Measurement Placement*", IEEE Transactions on Power Systems, Vol. 8, No. 2, pp. 707-715, May 1993.
[5] A. G. Phadke, "*Synchronized Phasor Measurements, a Historical Overview*," Proceedings of the Transmission and Distribution Conference and Exhibition 2002: Asia/Pacific, Vol. 1, Oct 2002, pp. 476-479.
[6] W. Lewandowski, J. Asoubib, W. J. Klepczynski, "*GPS: Primary Tool for Time Transfer*," Proceedings of the IEEE, Vol. 87, No. 1. Jan. 1999, pp. 163-172.
[7] B. Milosevic, M. Begovic, "Nondominated Sorting Genetic Algorithm for Optimal Phasor Measurement Placement," IEEE Transactions on Power Systems, Vol. 18, No. 1, February 2003, pp. 69-75.
[8] G. B. Denergi, M. Invernizzi, F. Milano, M. Fiorina, P. Scarpellini, "*A Security Oriented Approach to PMU Positioning for Advance Monitoring of a Transmission Grid,*" Proceedings of the International Conference on Power System Technology, Vol. 2, October 2002, pp. 798-803.
[9] M. Rice, G. T. Heydt, "*Phasor Measurement Unit Data in Power System State Estimation,*" Intermediate Project Report for PSERC Project, January 2005.
[10] B. Xu, A. Abur, "*Optimal Placement of Phasor Measurement Units for State Estimation,*" Intermediate Project Report for PSERC Project, October 2005.
[11] J.F. Dopazo, et.al., "State Estimation of Power Systems from Line Flow Measurements', *IEEE Trans. PAS Vol. 89*, Sept/Oct 1970
[12] G.Benmouyal, et.al., "Synchronized Phasor Measurement in Protective Relays for Protection, Control, and Analysis of Electric Power Systems", 29th Annual Protective Relay Conference, Spokane, WA, Oct 22-24, 2002
[13] G.L. Kusic, *Computer-Aided Power System Analysis*, 1st ed. Prentiss-Hall, 1986 2nd ed. Taylor and Francis, Nov 2008

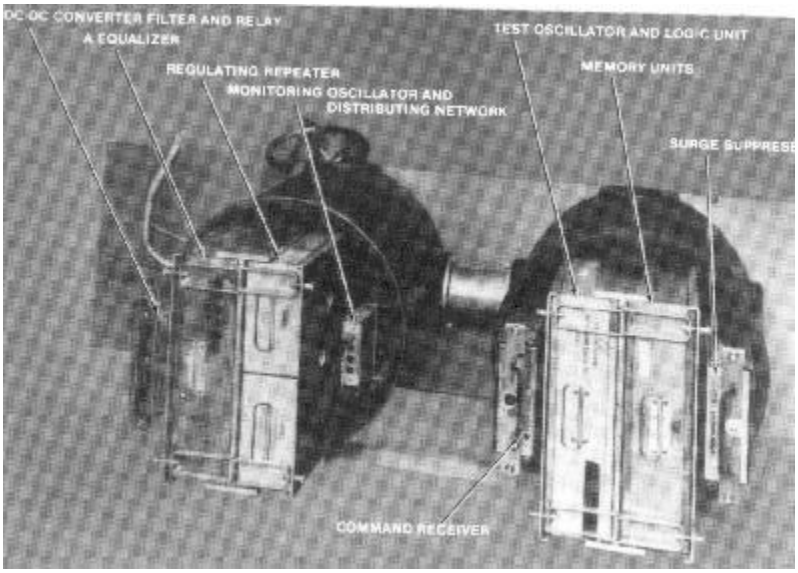
Attachment 2 – Material submitted by John A. Weyer, Cyber Security Subgroup

THE L-4 SYSTEM

For technical reasons these L-4 centers existed every 150 miles in the cable route (buried repeaters existed every 2 miles).

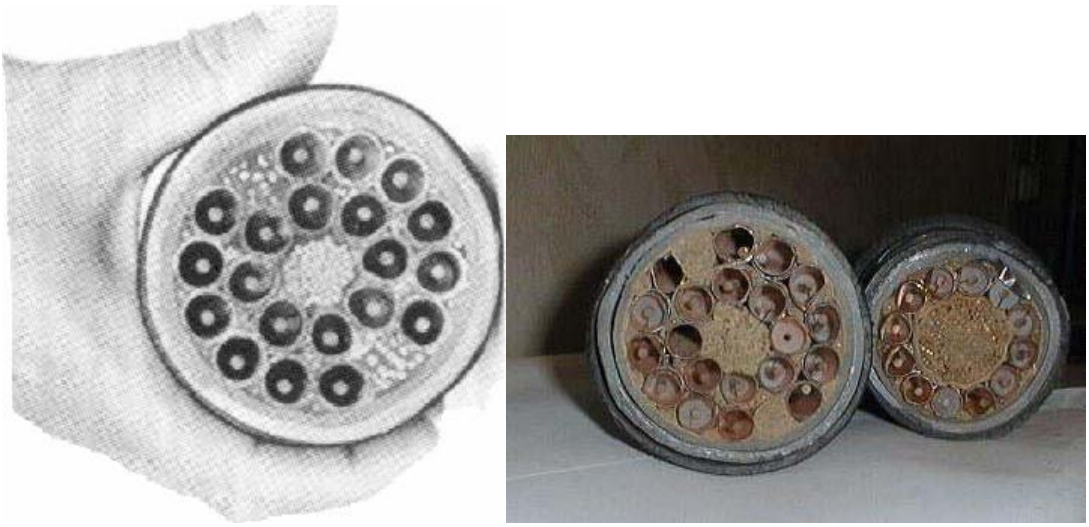


The repeaters were buried every 2 miles. A typical repeater for one coaxial tube is shown below.



Across section of a piece of L-4 coaxial cable is shown below. This is a 20 tube cable. Copper wires in the middle are for signaling and order wire circuits, alarms etc. Each tube could carry 3600 voice circuits. The cable was incased in a lead sheath and weighed 11 pounds per linear foot. The cable was buried 4 feet deep to insure that it stayed at 50 degrees F regardless of weather. Changes is temperature adversely effected the cable electrical characteristics.

TWENTY TUBE COAXIAL L-4 CABLE



The top photo is a 20 tube coaxial cable held to show relative size. The lower photo is a 20 L-4 System tube L-4 cable placed next to a 12 tube cable that was formerly part of a L-3 system. The original route ran from Massachusetts to Miami. Then across the country to CA and many other routes followed to insure redundancy (four separate routes served Cheyenne Mountain to insure communications). Several of the major cable routes are shown below.

Repeater site at Hubbardston, MA. The repeaters were below grade in the vault that looks like a foundation for the building. This one is owned by a gas station and used for storage. The owner bought it from AT&T in the late 70's.

Cable marker next to Hubbardston repeater facility. Note bird house on top (probably not Western Electric issue). Also note two devices on side of pole that hold test points for order wire contained in L-3 cable.

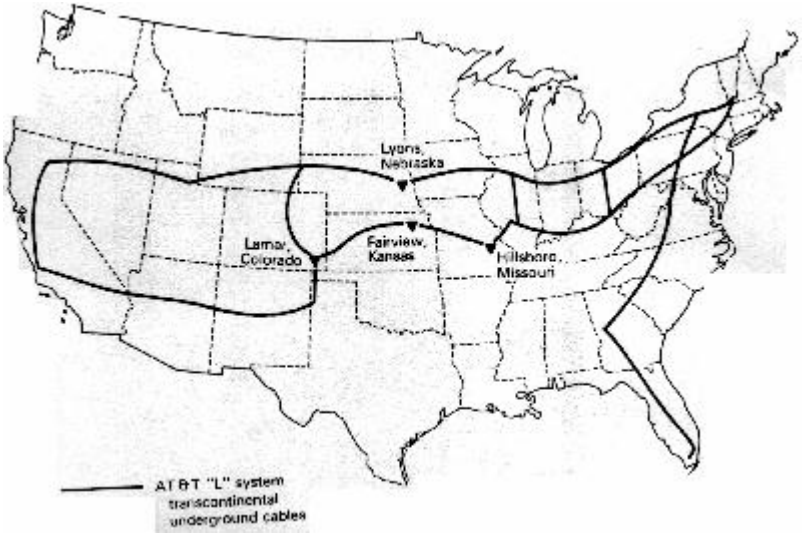
Closeup of test points on the L carrier order wire. The technician would use a 100A

portable battery powered test set to attach to the test points. Using the 100A test set a fiddle technician could talk to the main station or another technician. The 100A tst set was designed to talk up to 54 miles. (The order wire circuits in a L carrier route are supplemented by repeaters at 54 and 108 miles). This particular repeater station had 2 test points (east and west). A second pair of test points is inside the repeater vault.

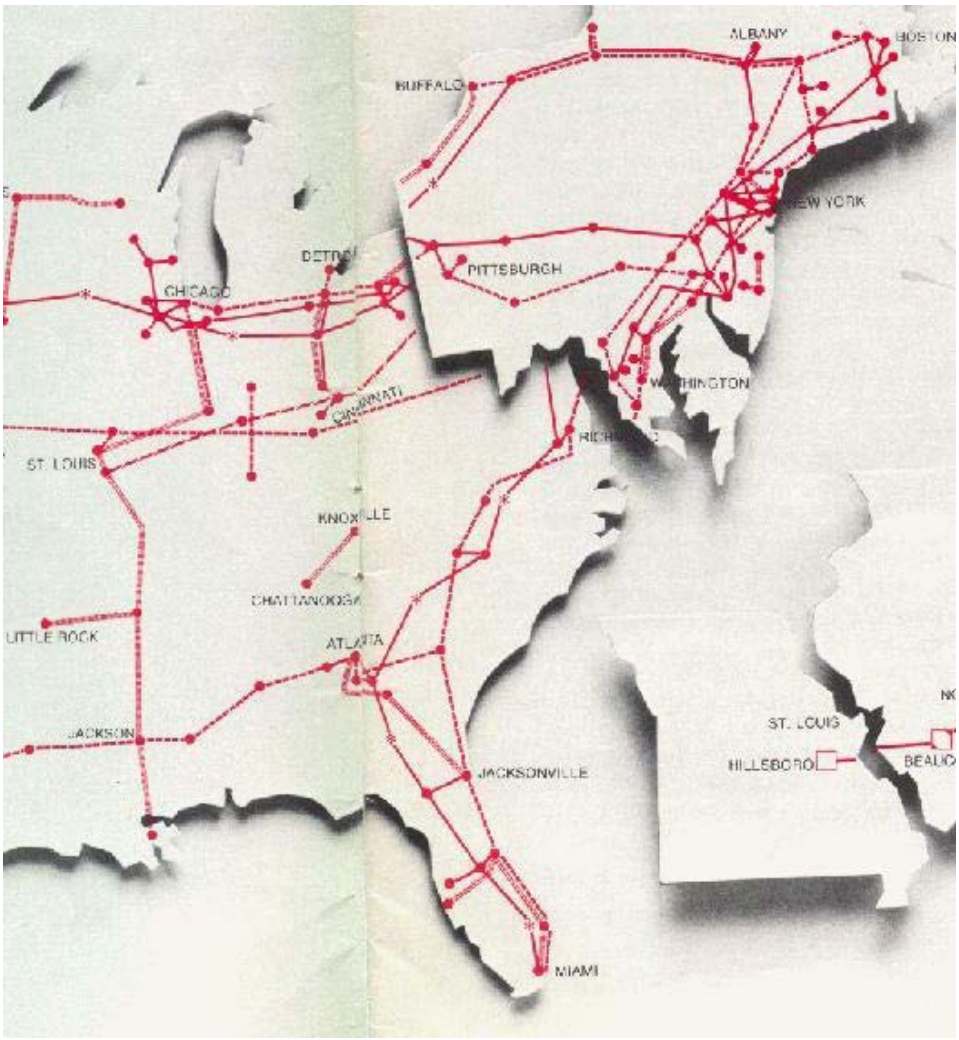
Open the door and the hatch to the vault is on the floor. Well secured by key and latches. This vault was filled with water. Repeater huts had commercial power fed to them for use by the technician. Power was needed for the blowers necessary to ventilate the vault before use, lighting and an occasional pumping. Remote facilities required the technician to bring a generator along. Some remote sites required snowmobiles in the winter to tow the generator, blower and test equipment.

L CARRIER CABLE MAPS

The following map show key routes for the Department of Defense's communication's system during the Cold War.



A detailed map of the L-Carrier system in 1973 for the Eastern United States is shown below. Solid lines are L-4 cables/routes dashed lines are L-3 cables/routes. Fuzzy lines (/////////) are L-1 cables/routes.



Many of the routes were marked to show the utility right of way. This old L-4 cable marker assumes a new life a a fiber optic cable maker. Beneath the new colored warning sign a faded sign reads "WARNING DO NOT DIG TRANSCONTINENTAL CABLE". This marker is on the Littleton, MA to Blackstone, MA L-4 cable route.

L-4 CABLE MARKER

These facilities also supported many other related military communications matters including inter connectivity with Presidential as well as other military aircraft, the NAWAS warning net, the SACDIN warning system, Civil Defense key circuits, nuclear detonation detection, an other systems. To the best of my knowledge the system was dismantled in the mid 80's. Break up of the bell system as well as the introduction of fiber hastened the demise (not to mention the fall of the Russian empire). Currently many of these centers have an after life supporting cellular telephone antennas on their little used microwave towers (Most of the huge cornucopia antennas "turned down" as inefficient and expensive to maintain) and also serving as hubs for fiber cables that have supplanted the old L-4 cable that existed in thousands of miles of Bell System right of way.

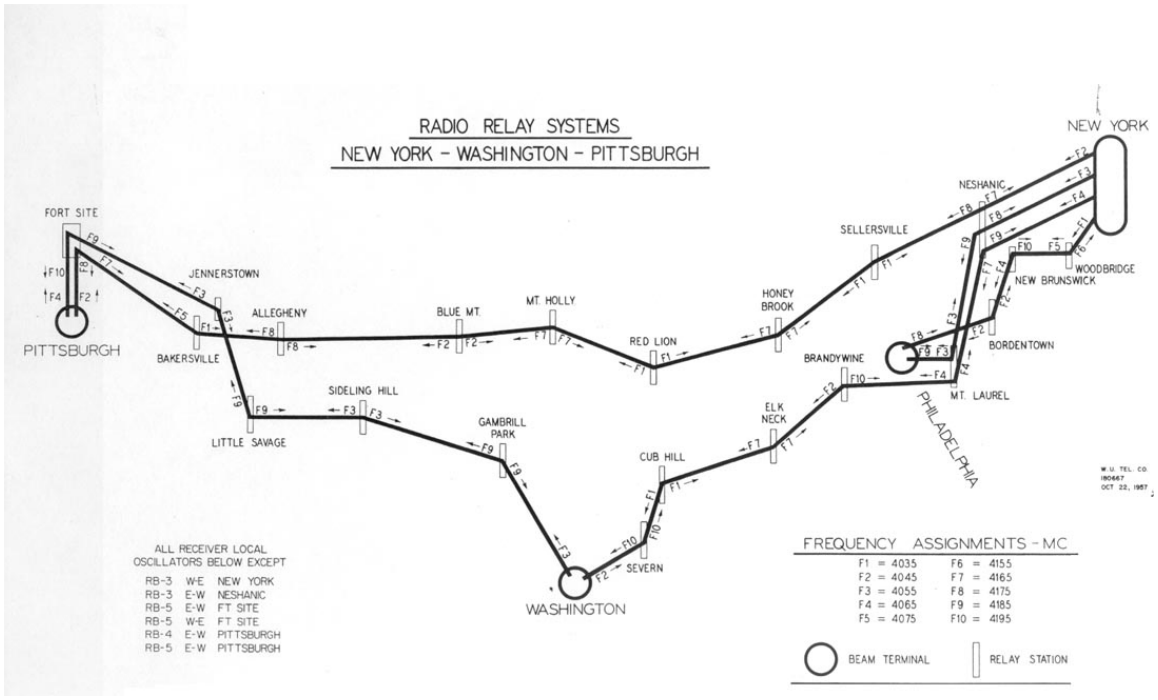
SYSTEM CAPACITY

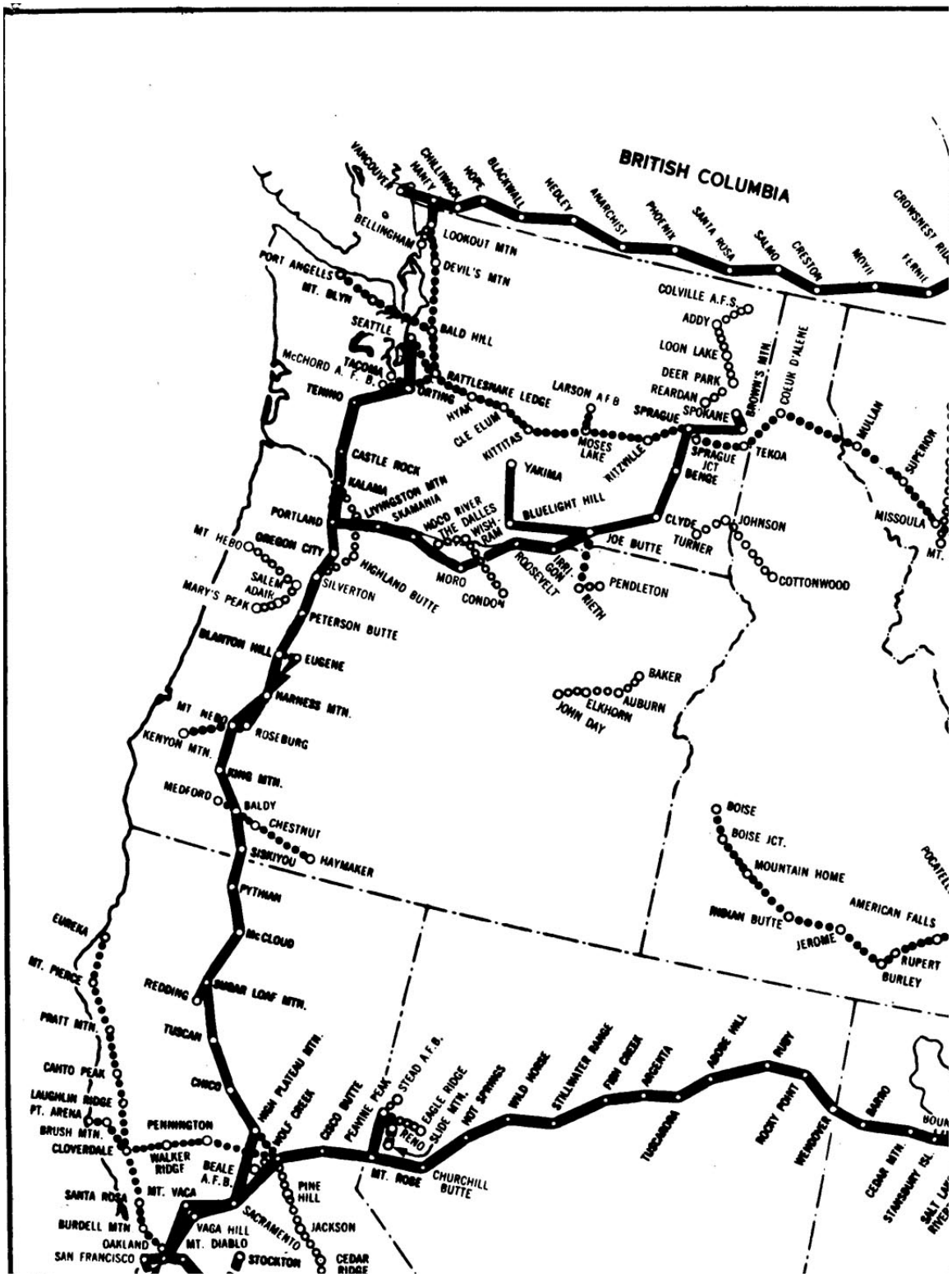
SYSTEM	***DATE***	***BANDWIDTH***	***COAXIALS PER CABLE***	***REPEATER SPACING***
L-1	*1941*	*3 mhz*	*4*	*8*
Miles	*600 voice circuits*			
L-2	*1942*	*840 khz*	*4*	*16*
miles	*360 voice circuits **			
L-3	*1953*	*8 mhz*	*8*	*4*
miles	*5,580 voice circuits*			
L-3 (Improved)	*1960*	*8 mhz*	*12*	*2*
miles	*9,300 voice circuits*			
L-4	*1967*	*17 mhz*	*20*	*2*
miles	*32,400 voice circuits*			
L-5	*1972*	*57 mhz*	*22*	*1*

miles 108,000 voice circuits

***** *Only one L-2 Coaxial System was installed between Baltimore and Washington. The outbreak of WWII mothballed the L Carrier system bring this system development to a halt. Rapid economic development after the war made the L-2 system obsolete.*

Note: *Currently a single fiber cable can carry 3,200,000 voice circuits.*




BRITISH COLUMBIA
VANCOUVER
CHILLIWACK
HARRY
HOPE
BLACKWALL
HEDLEY
ANARCHIST
PHOENIX
SANTA ROSA
SALMO
CRESTON
MOYIE
FERNIE
CROWSNEST RIDGE
BELLINGHAM
LOOKOUT MTN
DEVIL'S MTN
PORT ANGELES
MT. OLYM
SEATTLE
BALD MTN
TACOMA
McCHORD A. F. B.
TENINO
ORTING
BATTLESNAKE LEDGE
LARSON A F B
HYAK
CLE ELUM
KITTITAS
MOSES LAKE
RITZVILLE
SPRAGUE
SPOKANE
COLVILLE A.F.S.
ADDY
LOON LAKE
DEER PARK
REARDAN
BROWN'S MTN.
COEUR D'ALENE
MULLAN
SUPERIOR
TEKOA
SPRAGUE JCT
BERGE
CASTLE ROCK
KALAMA
LIVINGSTON MTN
SKAMANIA
YAKIMA
BLUELIGHT HILL
PORTLAND
HOOD RIVER
THE DALLES
WISH-RAM
CLYDE
JOHNSON
TURNER
JOE BUTTE
MISSOULA
MT.
MT HEBO
GREGON CITY
SALEM
ADAIR
MARY'S PEAK
SILVERTON
HIGHLAND BUTTE
MORO
CONDON
ROOSEVELT
IRRI-GON
RIETH
PENDLETON
COTTONWOOD
PETERSON BUTTE
BLANTON HILL
EUGENE
BAKER
AUBURN
ELKHORN
JOHN DAY
HARNESS MTN.
MT NEBO
KENYON MTN.
ROSEBURG
KING MTN.
MEDFORD
BALDY
CHESTNUT
SISKIYOU
HAYMAKER
PYTHIAN
BOISE
BOISE JCT.
MOUNTAIN HOME
AMERICAN FALLS
RHOAM BUTTE
JEROME
RUPERT
BURLEY
EUREKA
MT. PIERCE
McCLOUD
REDDING
SUGAR LOAF MTN.
PRATT MTN.
TUSCAN
CANTO PEAK
CHICO
HIGH PLATEAU MTN.
LAUGHLIN RIDGE
PT. ARENA
BRUSH MTN.
PENNINGTON
WOLF CREEK
CISCO BUTTE
PLUMINE PEAK
STEAD A.F.B.
EAGLE RIDGE
SLIDE MTN.
HOT SPRINGS
WILD HORSE
STILLWATER RANGE
FISH CREEK
ARGENTA
HORSE HILL
TUSCARORA
ROCKY POINT
WELDOVER
BARRO
CLOVERDALE
WALKER RIDGE
BEALE A.F.B.
MERO
MT. ROSE
CHURCHILL BUTTE
CEDAR MTN.
STANSBURY ISL.
SALT LA
RIVER
SANTA ROSA
MT. VACA
PINE HILL
BURDELL MTN
VACA HILL
SACRAMENTO
JACKSON
OAKLAND
MT. DIABLO
SAN FRANCISCO
STOCKTON
CEDAR RIDGE

The Washington Area Wideband System (WAWS) Microwave Route Map
From the Western Union Telegraph Company's proposal document, dated 1979

Notes:
- ***Fort Meade*** *houses the headquarters of the National Security Agency*
- ***NSS*** *was the Naval Security Station near Ward Circle on Nebraska, Ave. NW, Washington, DC (now headquarters of the Department of Homeland Security)*
- ***Friendship Annex*** *is the National Security Agency's facility near Baltimore-Washington International Airport*
- ***Andrews*** *is Andrews Air Force Base in Prince Georges County, MD*
- ***Liberty Dam*** *is a former Western Union microwave relay station*
- ***Blue Ridge*** *is the Alternate Joint Communications Center (Site R), near Blue Ridge Summit, PA*
- ***Damascus*** *is the former U.S Army Strategic Communications Command microwave tower near that town*
- ***Tenley*** *is the former Western Union's Tenley Tower in the Tenleytown neighborhood of northwest Washington, DC*
- *The node south of Tenley and NSS is the Pentagon in Arlington, VA*

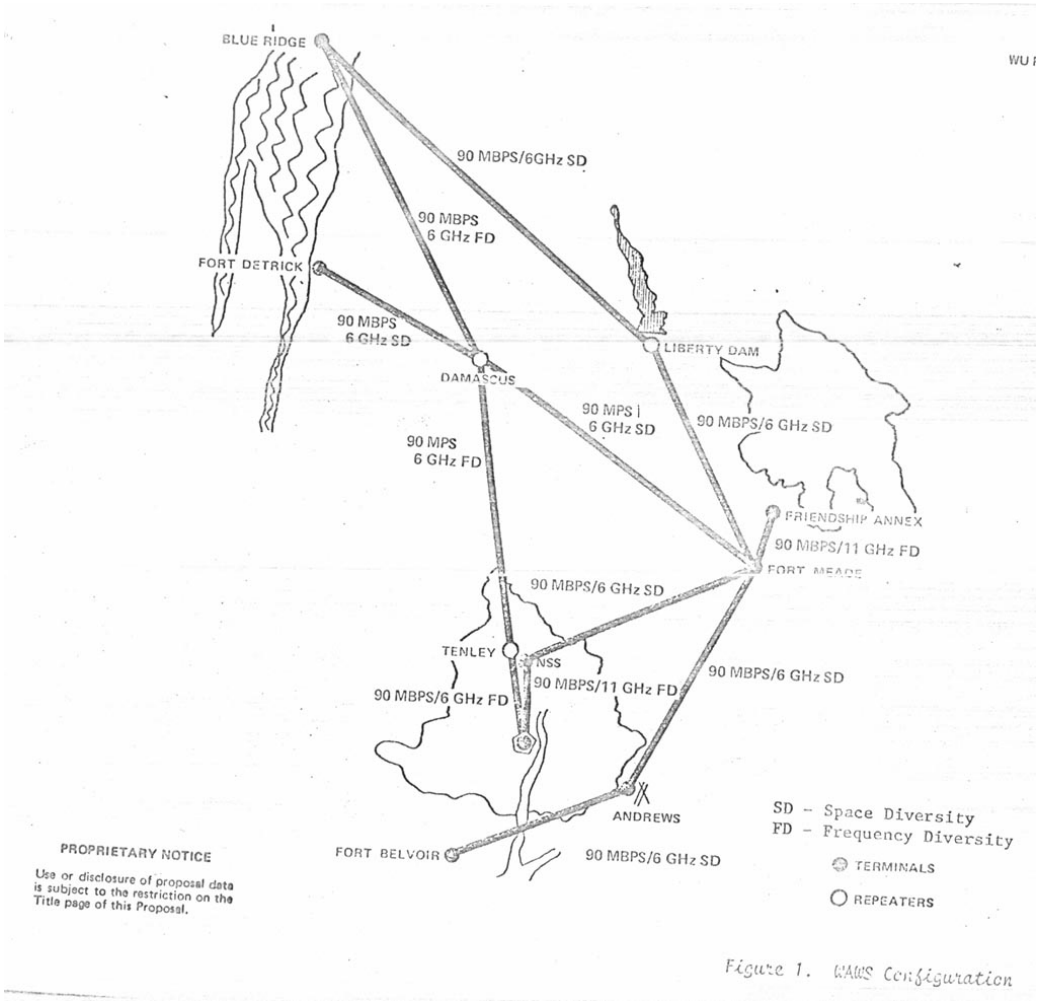


Figure 1. WAWS Configuration

The Federal Telecommunications System

Beginning operation in 1963, the FTS was a "private" long-distance telephone network servingthe civilian agencies of the federal government. It was built and operated by AT&T under contract to the General Services Administration, a federal agency which provides a wide variety of support services across the entire civilian sector of the federal government. The FTS has been replaced by the Federal Telecommunications Service 2000.

The FTS design used a hierarchical arrangement of switching centers, or "switches". In this system, every switch was assigned to one of several "ranks". The switches were connected to certain other switches, of the same, higher, or lower rank, by trunk lines. A trunk line (or simply "trunk") is a circuit which carries a call between switches. When an FTS subscriber placed a call to a phone outside the territory of the switch serving his line, that switch would attempt to find a route to the destination switch through the lowest possible levels of the hierarchy, advancing to higher levels as needed until a route was established. This strategy helped make efficient use of network resources by minimizing the number of trunks and switches used to complete a call.
In the Washington area, FTS switches in two AT&T facilities in Maryland. Both installations are still active in the AT&T network, and in accordance with a request from AT&T Corporate Security, their names and exact locations are not published here. Photos and a description of one of these facilities can be viewed on my AT&T Long Lines web site, under the fictitious name MD-1.

Another FTS switch was located in Illinois, at a facility whose Common Language Location Identifier (CLLI) is NRWYILNO.