December 7, 2009

D&NMTT Group Comment Summary on Industry Comments to DOE Request

For the full text of the broad industry review comments, please reference the NASPI web site under the link, "Compiled Industry Comments Responding to DOE Request": http://www.naspi.org/resources/dnmtt/naspinet/naspinet_industry_comments_20090725.pdf . Included within this document is a high level review of the broad feedback as summarized by members of the Data and Network Management Task Team (D&NMTT). The D&NMTT provided a review of the broad feedback in order to refine the many comments received into a shorter list of pertinent items more actionable as NASPInet moves forward.

Question 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?

Key comments noted from the review were:

1. Need to have multiple vendors involved
2. Breakdown into PG & DB is beneficial
3. Need to document future work carefully so API's etc are well understood
4. Need to more clearly include the geospatial aspects of the data with the DB & PG specs
5. Need to more clearly define the middleware or interoperability standards
6. Team should review IEC/TR 62325 – ISO 15000 series of specs as a good example of the technical detailed that is required.
7. Migrate towards a publicly available standard.
8. Some hardcoded specifications seem to restrictive (such as Unix/Linux as the OS)

Question 2
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?

Key comments noted from the review were:

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

5. 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.
6. Lack of information addressing how increased deployment and communications will be handled over the proposed 30 year lifetime of the entire NASPInet.
7. NASPInet/Phasor Gateway should be able to identify and correct for time synchronization errors in PMUs and PDCs before communicating synchrophasors from these devices.
8. What analysis and monitoring tools that will be made available on top of the PG and DB facilities.
9. 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.
10. Need systematic performance goals to set the bar – how will we know if it works when deployed?
11. MTBF/MTTR/availability analysis is lacking.

Question 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?

General Observations:
As noted in DNMTT discussions, the more the IT experience/depth the less the liked it.
Here is a summary of noteworthy comments that were on topic for this question:

Issue	Author	Summary	Recommended Action
Adequacy	PJM, Duke	Says its fine	
Vendor lock-in	BPA	Incomplete spec, could allow vendor lock-in	Agreed, more details needed, but iteratively like the DARPA model
Adequacy	WebLOQ	Incomplete, recommends XML APIs and messaging	XML would be very slow compared to what is possible and needed
Pub-sub spec	RTI	Notes the OMG's DDS is pub-sub with multiple vendors	Investigate DDS (note: there will be an RTI presentation at Chattanooga).
Adequacy	ISO-NE	Says inadequate;	
Geospatial	Open	inadequate	TVA has long experience

Issue	Author	Summary	Recommended Action
interoperability	Geospatial	geospatial APIs/encodings	with this, get their inputs
Adequacy	ATT	Inadequate; also target COTS not special devices	Discuss; COTS pub-sub not intended for mission critical with very low delays
Adequacy	BBN	Very inadequate	More details needed; see BBN's presentation at Feb09 NASPI on the DARPA iterative model

Question 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?

Here is a summary of noteworthy comments that were on topic for this question:

Issue	Author	Summary	Recommended Action
Interoperability	PJM	OK for PMUs; maybe not for other data	Nnet will need to support non-PMU data over time; techniques well known for 20 years by middleware vendors (e.g., OMG)
(?)	BPA	OK if (missing) APIs done quickly, ergo not OK now.	
Maturity	RTI	Very incomplete; need to support evolvability	
Interoperability	Duke Energy	OK	
Geospatial data	Open Geospatial	Missing geospatial info	Leverage TVA experience
Interoperability & Real-Time	BBN	Much unspecified; real-time delivery	

		across entities not addressed enough in spec	
Completeness	ISO-NE	OK if (missing) APIs added, ergo not OK now.	
Completeness & security	ATT	Incomplete; also security interfaces missing	

Question 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?

Comments were received from nine organizations. At least one vendor thought that all standards had been addressed, whereas others broadly referenced international or Internet2 standards. Additional standards were also brought up in the "Other" section, which are not included here. The concrete suggestions to address are as follows:

Commenter	Suggested Standards	Resolution
PJM	IEC (61850, 61970) standards	Incorporate, as appropriate
RTI	Object Management Group (OMG) standards. In particular, the OMG Data Distribution Service for Real-Time Systems specification and OMG Real-Time Pub-Sub interoperability wire protocol.	OMG standards have a proven track record, use as appropriate
OGC	Open geospatial standards from OGC and ISO TC/211	Determine the applicability of geospatial data in the NASPI DB & PG.
ABB, Inc	Standards cited by NIST in its Smart Grid Interoperability Standards Framework	Incorporate, as appropriate
BBN	Design for change, don't tie to closely to transient standards	Agreed.
ISO-NE	IEC/TR 62325 (aka, ISO 15000-2:2004)	Incorporate, as appropriate

The DNMTT believes that IEC TC 57 standards should be used if they meet stated requirements. The DNMTT also believes that, if appropriate, existing utility standards should be extended to meet NASPInet requirements so to minimize the amount of new technology that needs to be introduced.

Relevant draft and international standards and reports for current phasor measurement exchange:

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

Relevant draft and international standards and reports for NASPInet configuration as well as network model sharing. Note that IEC 61970 Part 502-8 includes IEC 62541 as a normative reference:

IE	65	8	IEC	OPC Unified Architecture Specification - Part 1:

C	E		62541-1	Overview and Concepts
IE	65	8	IEC	OPC Unified Architecture Specification - Part 2:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 3:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 4:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 5:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 6:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 7:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 8:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 9:
IE	65	8	IEC	OPC Unified Architecture Specification - Part 10:
IE	57	1	61970-1	EMSAPI – Part 1: Guidelines and General
IE	57	1	61970-2	EMSAPI – Part 2: Glossary
IE	57	1	61970-	EMSAPI – Part 301: Common Information Model
IE	57	1	61970-	CIM Transmission Network Model Exchange
IE	57	1	61970-	Web Services for IEC 61970 Part 4 Abstract
IE	57	1	61970-	Naming Service

Notes:
With regard to the recommendation that IEC 61850 technology be considered, the DNMTT believes that that the streaming data exchange mechanism envisioned for NASPInet is inappropriate for local or wide area protection due to the following reasons:

- Wide area protection typically operates on an event driven basis. Frequently, signals need to be conveyed over long distances in less than 100 ms. Using NASPInet for protection introduces an additional signal transmission latency equal to the phasor data sampling period. Given the sampling period for NASPInet is not envisioned to be less than 16ms (60 samples per second), NASPInet introduces an unnecessary delay that renders it unsuitable for high speed protection. Alternatively, IEC 61850 GOOSE messaging is event driven and does not introduce this delay.
- Existing devices employ IEC 61850. It is not clear that protection device vendors will add NASPInet protocols to their devices. Instead, it is more likely that protection will be handled in a way that extends the existing standard ways of today.
- If NASPInet streaming is not used to for high speed protection, it can be constructed having less stringent speed and latency requirements. This would make NASPInet less vulnerable to network problems or denial-of-service attacks focused on slowing speed and increasing latency.

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/extending off the shelf software currently available from multiple utility software vendors.

The DNMTT recommends the use of a Service Oriented Architecture (SOA) for NASPInet configuration and management. 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 should be considered.

Question 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?

General observations:
There is a lot of interest in learning about and suggesting specific security technologies. The spec is weak on that but its not clear if we are there yet.

Issue	Author	Summary of Comment	Recommended Action
EMP	Advanced Fusion Systems and John Weyer Cyber Security Subgroup	EMP should be considered as a threat	EMP is not a cyber security threat and therefore can be considered out of scope. In general, it might be an interesting threat to keep track of; e.g., there is an ongoing discussion of EMP's impact on the power grid at empcommission.org.
Dedicated and Fault Tolerant Physical Network	Entergy, John Weyer Cyber Security Subgroup	NASPInet must mandate the use of a dedicated physical data network with sufficient fault tolerance	This is a worthy issue to discuss in a DNMTT meeting at an appropriate time
Core Network Management and Security Tools	Entergy	NASPInet core should provide all network management and security tools the very beginning	This is a NASPInet process comment and not a specification issue. Interesting point but can be considered out of scope.
Key Management details	WebLOQ	Highly distributed and defensible key management structure that can	DNMTT has considered at adding more details to key management in the specification. It will be good to

Issue	Author	Summary of Comment	Recommended Action
		survive client and server compromises is needed. The key management structure should be under a single central authority.	discuss this specific recommendation and, in general, endeavor to add details in the spec.
DTLS	RTI	DTLS should be added to the spec (e.g., in Figure 2-12)	This sounds like a reasonable addition to make to the spec.
Web Services Security	SISCO	IEC 62541 (OPC UA) build on web service security is proposed as an approach	The spec should be evaluated to see that using this proposed approach is not excluded.
Encrypted passwords	ABB	"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". "	This comment makes sense and the suggested change should be made.
Failure recovery and	BBN	Timely recovery from failure and	This issue should be addressed in the spec and

Issue	Author	Summary of Comment	Recommended Action
survivability		survivability in general should be considered.	has not been done so to date. Fault tolerance is mentioned but not in much detail.
NERC/FERC CEII requirements	ISO-NE	NASPInet may contain critical energy infrastructure information (CEII) and therefore could be subject to NERC and FERC security requirements for CEII.	CEII requirements should be reviewed and considered for inclusion in the spec.

Other Comments (Not associated with Questions)

Some of the comments showed that the specification, as written, did not capture the DNMTT "vision" of NASPInet. Others also clearly focused on the need to articulate the business case for NASPInet. Cyber security was a significant concern for several reviewers.

There were several comments on the steps needed prior to implementing NASPInet: Key (actionable) comments are as follows:

Commenter	Comment(s)	Resolution
PJM	Need a pilot	Agreed
Entergy	Look to other programs Need a pilot NASPInet is being overcome by NIST Smart Grid work Unbundle the Phasor Gateway and Data Bus	Agreed
SISCO	If NASPInet is not used for protection, then the requirements become easy	Need to clarify NASPInet use cases.

Other Key (actionable) comments are as follows:

Commenter	Comment(s)	Resolution
EEI	Need a long term business plan	Agreed
BPA	Consider 60 phasors per second (& other performance related comments) Need detailed Phasor Gateway to Phasor Gateway data format specifications	Need to clarify NASPInet use cases, platform independent and

Commenter	Comment(s)	Resolution
		platform specific models
G. Kusic	Need data snapshots of the power system around each PMU	Need to clarify NASPInet use cases
SISCO	Long discussion on IEC standards (e.g., IEC 61970, 61850)	Incorporate, as appropriate
OGC	Need to be geo-spatial aware Consider OGC standards and OGC Geography Markup Language	Determine the applicability of geospatial data in the NASPI DB & PG.
Southwest Power Pool	"Our strongest concern with the NASPInet project for SPP and our members is the Cyber Security Protection…"	Address cyber security in more detail.
Xcel Energy	How will CIP standards be met?	Address cyber security in more detail.
CAT-1	Incorporate a legacy layer (OPC)	Need to clarify NASPInet use cases and define NASPI Phasor Gateway to legacy devices and or protocols
AEP Trans. Asset.Mgmt.	Need to clarify responsibilities Unclear: Is the, Databus WAN or Point-to-Point? Redundancy—what is meant? Latency requirements need to address how the data is packetized	Need to clarify NASPInet use cases, platform independent and platform specific models
Southern Cal. Edison	Need to address additional cyber security standards/ documents (e.g., NIST SP800-30, FISMA,NIST SP800-53, DHS Control Systems Catalog)	Address cyber security in more detail.