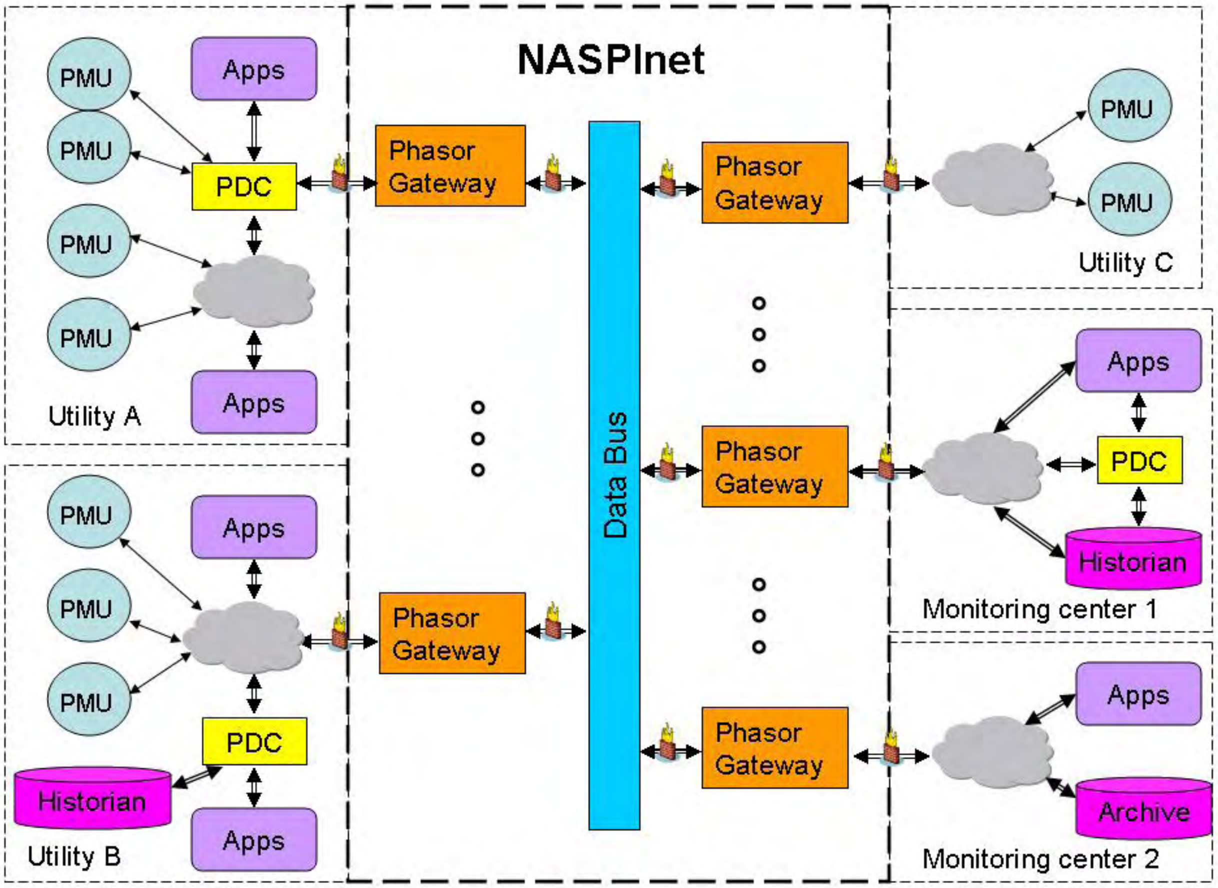
Phasor Gateway Technical Specifications for North American Synchro-Phasor Initiative Network (NASPInet)

Date: May 29, 2009



Prepared by: **Dr. Yi Hu (Project Manager)**

QUANTA TECHNOLOGY

Project Team

Quanta Technology LLC (Lead)

- Dr. Yi Hu (Project Manager)
- Dr. Matt Donnelly
- Hahn Tram
- Bob Uluski
- Kenneth Martin

Enspiria Solutions

- Mark Cioni
- Tom Helmer

Iowa State University

- Dr. Manimaran Govindarasu

Table of Contents

1 Introduction and Project Overview

This Technical Functional Requirements Specification document is part of the Request for Proposal (RFP) of the "PG_REQUESTER"[1] for implementing a Phasor Gateway (PG) to facilitate the connections and data exchanges of the PG_REQUESTER's Phasor Monitoring Units (PMU) and Phasor Data Concentrators (PDC) with the North America Synchro-Phasor Initiative Network (NASPInet) via the Data Bus (DB) of NASPInet. This section of the RFP contains an overview of the PG_REQUESTER's requirements for the PG. Overall project scope and responsibilities of the RFP proponent, hereafter referred to as the PG_SUPPLIER, and the PG_REQUESTER are also delineated in this section

1.1 About the PG_REQUESTER

<PG_REQUESTER will provide basic information about the PG_REQUESTER here.>.

1.2 About NASPInet and Its Overall Objectives

The North American Synchro-Phasor Initiative (NASPI) is a major effort by the North American electric power industry to create a robust, widely available and secure synchronized data (synchro-phasor) measurement infrastructure for the interconnected North American electric power system with associated analysis and monitoring tools for better planning and operation, and with improved reliability. NASPI's ultimate objective is to decentralize, expand, and standardize the current synchro-phasor infrastructure through the introduction of a NASPI network (NASPInet) that will be composed of Phasor Gateways (PGs) and a Data Bus (DB), both of which shall, where applicable, utilize, be compatible with, and integrate within the set of Common Services of the respective Requester's enterprise IT infrastructures. Once fully deployed, it is envisioned that the NASPInet could support hundreds of Phasor Gateways and thousands of Phasor Measurement Units (PMU), each typically sampling data at 30 times per second.

The NASPI data infrastructure currently consists of a number of devices, particularly PMUs and Phasor Data Concentrators (PDCs). PMUs are the sources of synchronized phasor data, taking power system measurements at stations and substations. They send the data to PDCs or other data collection device which may be located in the field or in a control center. Field collection devices typically send the data to a PDC at a control center where data from a number of stations is collected and combined. The PDC time-aligns the data and supplies it to applications as synchronized measurements. Applications include

[1] It is envisioned that NASPInet will involve two separate procurements: Data Bus (DB) procurement and Phasor Gateway (PG) procurement. Two separate technical requirement specification documents were developed for DB and PG procurements respectively. To distinguish the types of customers referred to in each specification, the DB_REQUESTER refers to the entity that is issuing the specification to request proposals for a DB, and likewise the PG_REQUESTER refers to the entity issuing the Request for Proposal (RFP) for PGs. Similarly, the entity responding to the DB RFP is referred to as "DB_SUPPLIER", and the responder of the PG RFP is referred to as "PG_SUPPLIER".

system visualization, alarming, data archiving, phasor data enhanced state estimator, congestion management, etc.

Current synchro-phasor systems do not necessarily include the components and facilities to meet scalability and flexibility required to meet NASPI's mission, and to facilitate secure and Quality of Service (QoS) guaranteed phasor data exchange among various entities, such as utilities and ISOs/RTOs. NASPInet is designed to provide the communication infrastructure, including a set of IT services such as Quality of Service management and cyber security, for a phasor data exchange system that will support NASPI's mission for all of North America.

NASPInet will be a complete networked system composed of a wide-area communication network (WAN) and gateways that provide access to the network as shown in Figure 1.1. The DB of NASPInet, includes the NASPInet WAN and associated IT services to provide basic connectivity, quality-of-service management, performance monitoring, and cyber security and access policy enforcement over different service classes of data exchanged through the NASPInet. PG is the sole access point of an entity to the DB. It manages the connected devices on the entity's side, manages quality of service, administers cyber security and access rights, performs necessary data conversions, and interfaces utility's own network with the DB.

NASPInet facilitates the secure exchange of both real-time streaming data and historical data stored outside of NASPInet. It features a secure and distributed Publisher-Subscriber based data exchange mechanism. The owner of a PG that publishes the data to NASPInet maintains full control of its data distribution regarding who could subscribe to its data and which data could be subscribed to.

The PGs that provide connections to NASPInet DB may have very different data publishing/subscribing functionalities and capabilities that depend highly upon the needs of each entity connected to the NASPInet through the PG.

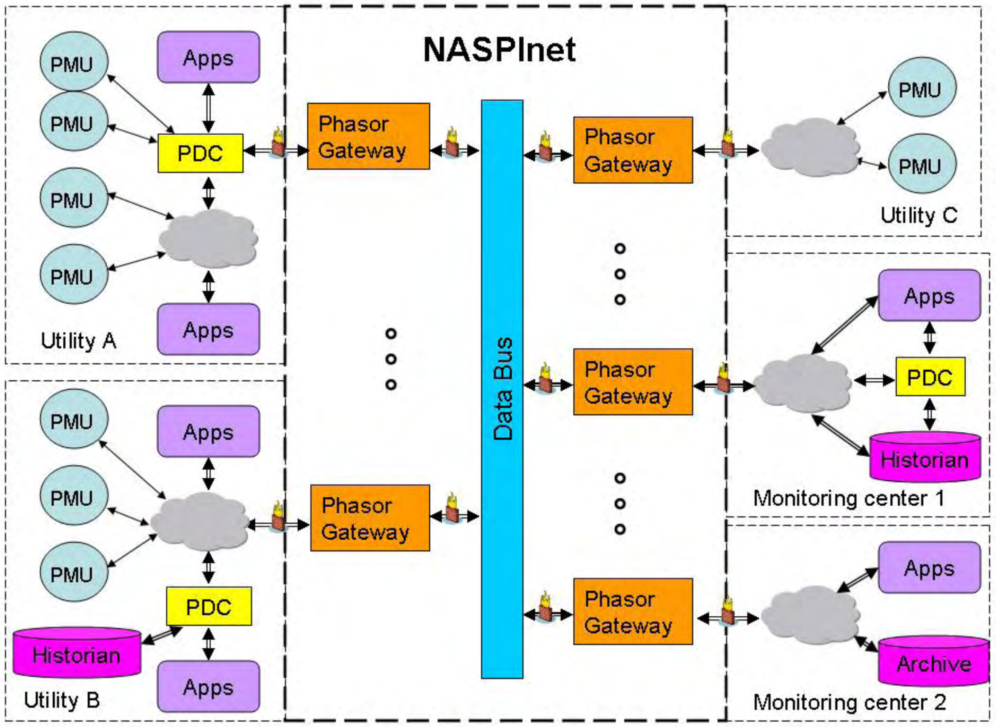


Figure 1-1: NASPInet Conceptual Architecture

1.3 Overview of Key PG Requirements

As a minimum, the PG shall perform the key functions listed below. These requirements are detailed in Sections 3 to 8 of this RFP.

1) Serve as the sole access point to the Data Bus;

2) Facilitate and administer registration of PG_REQUESTER's PMU, PDC, and signals;

3) Facilitate and administer the subscription and publishing of phasor data;

4) Administer and disseminate cyber security and access rights;

5) Monitor data integrity;

6) Manage traffic priority through the PG according to service classes;

7) Provide logging of data transmission, access controls, and cyber security for analysis of all anomalies; and

8) Provide Application Programming Interface (APIs) for interfacing with PG_REQUESTER systems and applications.

NASPInet will need to accommodate five classes of data services for supporting different types of applications

- **CLASS A:** This data service class supports the needs of high performance feedback control applications. This class is characterized by very low latency and a fast data rate (e.g., 60 messages per second). Class A data shall be transmitted and received as quickly as possible with a high level of data availability (there shall be no data gaps).
- **CLASS B:** This service class supports the needs of feed-forward control applications, such as state estimator enhancement. The latency requirement for Class B data is less strict than that for Class A data. High availability of the data is also required.
- **CLASS C:** This class of data supports view-only applications such as visualization by power system operators. The tolerance for accuracy and latency for Class C data are less stringent than Class B data. The system shall enable end-user applications to retrieve data from many PMUs across a wide geographical area.
- **CLASS D:** This service class supports the needs of post-mortem event analysis and other off-line studies. The system shall provide a high degree of data completeness and accuracy for this service class. However, latency of Class D data may be higher than Class A, B and C data since analysis of Class D data will generally conducted offline (hours or days later) with archived data, as opposed to an online data stream.
- **CLASS E:** Class E data primarily supports the needs for testing and Research and Development (R&D) applications. There are no guarantees on any attributes of this data class. Class E shall be given the lowest priority of all NASPInet data traffic.

The requirements contained in this specification may be considered mandatory for one class of data and desirable for another class of data service. In other words, the PG requirements may be different depending on the classes of data services that PG_REQUESTER expects to implement. The applicability of the requirements specified herein to PG_REQUESTER is indicated in Appendix A.

1.4 Scope of Supply

The PG_SUPPLIER's scope of supply shall include the software, hardware, and services required to design, build, install, configure, test, and integrate the required software and hardware for the PG. It shall include installing the PG, connection of the PG to the DB, integrating the PG with external systems (PDCs, PMUs, and Applications), training PG_REQUESTER personnel, and commissioning the PG.

Installation space and facilities will be provided by the PG_REQUESTER for all PG components that are installed in PG_REQUESTER control centers, substations or other field locations.

The PG_SUPPLIER shall be responsible for implementing the connections and interfaces between the PG and PG_REQUESTER devices (PMUs, PDCs), and between the PG and the NASPInet DB using the DB_SUPPLIER provided APIs. PG_SUPPLIER may also be required to interface the PG with PG_REQUESTER selected applications such as EMS systems. The application interfaces required will be specifed in Section 5 and Attachment II.

PG_REQUESTER personnel shall be responsible for configuring the PG_REQUESTER-owned PMUs and PDCs to support their interface to the PG. The PG_SUPPLIER shall work closely with PG_REQUESTER personnel and/or PG_REQUESTER's current sustainment organizations to ensure the correct end-to-end operation and satisfactory performance of the system as a whole.

The PG_SUPPLIER shall provide technical support to PG_REQUESTER during the installation, configuration, acceptance testing, connection, performance tuning, and commissioning of the PG. verifying successful data transmission and integration, investigating discrepancies in the PG operation (if any), and making the necessary corrections to the PG hardware/firmware and software (if required).

1.5 PG_REQUESTER and PG_SUPPLIER Responsibilities

The responsibilities of PG_REQUESTER and the PG_SUPPLIER for this project are summarized in the following sections.

1.5.1 PG_SUPPLIER Responsibilities

The PG_SUPPLIER shall provide a PG system that includes all the necessary components and interfaces needed to satisfy PG_REQUESTER's requirements that are described in this specification document, except for components that will be supplied by PG_REQUESTER (PDCs, PMUs, applications, etc.).

PG_SUPPLIER responsibilities shall include:

- Procure, design, build, integrate, test, ship, install, and perform site acceptance test and system commissioning of all components of the PG

- Supply PG communication links and interfaces needed to satisfy PG_REQUESTER's requirements.

- Provide an appropriate development system early in the project that will allow PG_REQUESTER personnel to test the connection and interface of the PG to the DB. This will also enable

PG_REQUESTER personnel to gain familiarity with the system, and develop commissioning and testing procedures.

- Develop integrated test plans and detailed test procedures for the PG.
- Conduct a pre-Factory Acceptance Test (“pre-FAT”) and certify that the Pre-FAT has been successfully completed.
- Coordinate and document the Factory Acceptance Test (FAT), if required by PG_REQUESTER, providing technical support and assistance during the test, providing the appropriate response to all variances identified during the FAT, and correcting and retesting all problems identified during the FAT. The PG_SUPPLIER shall provide suitable mechanisms to simulate during FAT items that are available only in the field, such as PDCs, PMUs, PG_REQUESTER applications, and the DB interface.
- Conduct Site Installation/Startup test, Site Functional test, and Site Integration test, and provide the appropriate response to all variances identified during these tests, correcting and retesting all problems identified during these tests to PG_REQUESTER’s satisfaction.
- Provide technical support as needed during the Site End-to-End Test and the Site Availability Test which will be conducted by PG_REQUESTER personnel. The PG_SUPPLIER shall provide the appropriate response to all variances identified during these tests, and correcting and supporting the retesting of all problems identified during these tests.
- Provide in depth technical assistance during the installation, configuration, tuning, troubleshooting, correction, and commissioning of the PG. The PG_SUPPLIER shall assist PG_REQUESTER in verifying that the PG is fully functional, including inputs, outputs, internal functions, and commissioning these systems.
- Provide detailed documentation and training to enable PG_REQUESTER personnel to operate and maintain the PG effectively with minimal outside assistance.
- Maintain all equipment through shipment and installation, providing a warranty against defects on all deliverables for a period of <N> years following final acceptance by PG_REQUESTER.
- Provide maintenance support and spare parts following acceptance of the PG.
- Assess the PG system for security vulnerabilities and technical compliance before commissioning the system. Identified vulnerabilities shall be resolved before the system is commissioned.

- Supply PG unit(s) with hardware and software, including the necessary ports, memory, processing capability and other services needed to satisfy PG_REQUESTER's requirements.

- Design, develop, implement, and test both sides, "end-to-end", of the PG interfaces with the DB and with other PG_REQUESTER systems and applications as specified.

- Implement the PG_REQUESTER-supplied configuration parameters, and electrical interface.

1.5.2 PG_REQUESTER Responsibilities

PG_REQUESTER's responsibilities will include:

- Review and approve the technical architecture, design and deliverables.

- Provide information required by the PG_SUPPLIER, such as desired PG location, expected data volume through the PG, preferred IT platforms, and existing communication infrastructures and facilities, to complete the design of the PG configuration.

- Define the basic objectives, constraints, and other information required by the PG_SUPPLIER to design and implement the PG, and provide information requested by the PG_SUPPLIER that is needed to build the PG.

- Review and approve in a timely manner all documents, including design, test plans and procedures, and other relevant documents supplied by the PG_SUPPLIER.

- Participate in formal training courses conducted by the PG_SUPPLIER at the PG_SUPPLIER's offices and/or at PG_REQUESTER's offices.

- Conduct the PG FAT with support from the PG_SUPPLIER as needed, perform all "unstructured" testing in the factory, and perform the SAT.

- Provide the PG_SUPPLIER with technical assistance during the installation of the PG equipment as needed.

- Witness and approve results of the Site Installation/Startup test, the Site Functional test, and the Site Integration test.

- Conduct the Site End-to-End Test and the Site Availability Test. and retest all problems identified during these tests after the variances have been resolved by the PG_SUPPLIER.

- Do final system commissioning

- Provide facilities including power supplies need for the PG.

- Provide the necessary LAN/WAN infrastructure for connecting the PG to DB and PG_REQUESTER’s information systems to the PG**.**

1.6 Organization of the NASPInet and PG Technical Specifications

The procurement of NASPInet is divided into DB procurement and PG procurement. As such, there are two separate specifications for NASPInet: the Data Bus Specification and the Phasor Gateway Specification.

The Data Bus specification covers the data communication network and all the services required for the NASPInet. Its communication network and links, as well as all the DB components and services are required to be flexible and expandable from initial implementation to the full anticipated system. Participants and additional PG connections can be added by securing and attaching communication links. Capacity can be added by securing more bandwidth and additional equipment for providing DB services. Since the DB is central to the system, the DB_SUPPLIER will specify API requirements for attachment, management, and data exchange with PGs over the NASPInet. These APIs will be used by PG_SUPPIERS in implementing the DB interface.

The Phasor Gateway Specification (This Specification) covers overall NASPInet requirements and specific requirements for PG. This PG specification contains all requirements for a full featured PG that supports the full publishing and subscribing capabilities of all data service classes of real-time streaming data and historical data. The PG_REQUESTER has indicated the desired publish and subscribe capabilities in terms of supported data service classes in this specification. The applicability of each requirement specificed in this document for each data service class is listed in a PG requirement applicability checklist in Appendix A. PG_SUPPLIER shall consult the checklist to determine the overall functional requirements of the procured PG by PG_REQUESTER.

The PG_SUPPLIER is encouraged to obtain the NASPInet Data Bus Specification to gain an in-depth understanding of the DB functionalities and services, and the interactions between PGs and DB.

The Phasor Gateway Technical Specification is organized as follows:

- ***Section 1: Introduction and Overview of Requirements***: This section contains introductory remarks and general corporate information about the PG_REQUESTER, provides project background information and information about the general objectives of the project, and describes the organization of this specification document. This section also contains an overview of PG_REQUESTER’s technical requirements. Specific responsibilities of PG_REQUESTER and the PG_SUPPLIER are also outlined in this section of the RFP.

- ***Section 2: System Architecture:*** This section describes the overall NASPInet architecture framework of the DB and PG components. While PG_SUPPLIERs are encouraged to propose their standard, field proven system architecture design, the proposed architecture must adhere to the general framework and guidelines identified in this section

- ***Section 3: Overall NASPInet Functional Requirements***: This section details the overall system, process, and functional requirements of NASPInet to be performed by the DB and the PG systems in concert. To the fullest extent possible, the requirements are specified in "functional" terms ("what is required" rather than "how to do it") to provide maximum flexibility for the PG_SUPPLIERs to propose their standard offerings with minimal customization.

- ***Section 4: Phasor Gateway Functional Requirements***: This section details the specific functional requirements for the PG. To the fullest extent possible, the requirements are specified in "functional" terms ("what is required" rather than "how to do it") to provide maximum flexibility for the PG_SUPPLIERs to propose their standard offerings with minimal customization. Besides the functional requirements outlined earlier in this section, the PG design shall accommodate expansibility, scalability, availability, interoperability, Quality of Service management, cyber security, and other technical requirements.

- ***Section 5: System Integration Requirements***: This section clarifies the points of demarcation for the overall NASPInet system integration requirements and describes the integration and interface development requirements of the PG_SUPPLIER.

- ***Section 6: Network and Communication Requirements:*** This section describes the requirements for the NASPInet communication infrastructure and the PG interfaces to meet the needs of the PG covered by this specification. This section covers requirements for the PG, which is essentially the interface between the PG_REQUESTER's phasor data communication infrastructure and the DB. Additional interfaces for user equipment including type, speed, and protocols are also described.

- ***Section 7: System Security:*** This section focuses on the security functions that are required for the PG. Primary focus is on cyber security though there are physical security issues that PG_SUPPLIER also needs to address, such as a physically secure environment for hardware components.

- ***Section 8: System Sizing, Performance and Availability:*** This section describes PG sizing and performance, system availability, spare capacity, and scalability requirements.

- ***Appendix A PG Requirements Applicability Checklist***: This Appendix contains a checklist provided by the PG_REQUESTER to indicate the applicability of the full-featured requirements documented in this specification to the requested PG specifically. In the applicability checklist, requirements contained in this specification are divided into four categories as applicable to each data service class:

  - ***Mandatory requirement (M):*** These are essential and must-meet requirements of the PG. Failure to meet these requirements will eliminate the proposed solution from consideration.
  - ***Highly-desirable requirement (H):*** Important but not absolutely essential; would be very advantageous to have.
  - ***Desirable requirement (D):*** Not essential, but would be nice to have.
  - ***Not-a-requirement (N):*** Not a requirement, but PG_SUPPLIER should take note and acknowledge the information provided in its response.

- ***Appendix B Abbreviations and Acronyms***: This appendix contains a list of common abbreviations and acronyms used in the document.

- ***Attachment I PG_REQUESTOR Information***: This attachment is a placeholder for DB_REQUESTER to provide information that PG_SUPPLIER would need to design configurations of the proposed system. The information may include for example: anticipated PG location, PMU/PDC locations, expected data volume through the PG, the PG_REQUESTER's preferred IT platforms; IT governance, policies and guidelines; existing facilities and telecom infrastructures, etc.

- ***Attachment II PG_REQUESTER Specific System and Service Requirements***: This attachment is a placeholder for the DB_REQUESTER to specific hardware, software, and system implementation and sustainment services to suite its operating environment and resource availability. Sample "boilerplate" specifications are included in the attachment for PG_REQUESTER reference. The PG_REQUESTER may tailor these materials for its own needs for the PG RFP or replace them in whole with its own standard materials. The reference, boilerplate materials include the following:

  – ***Section 9: Hardware Requirements***: This section describes the preferred and required attributes for the PG_SUPPLIER-supplied equipment. Equipment covered in this section includes the PG servers, Local Area Network (LAN) facilities, communication interfaces, interconnecting cables, enclosures, power supply and distribution, and spare parts. This section also covers requirements of a general nature that shall apply to the overall system. This includes service conditions for equipment at the installation location (temperature, humidity, etc.).

- ***Section 10: Software Requirements***: This section covers the required characteristics of the system software. Topics include operating system, network management facilities, database and display maintenance facilities, report writers, diagnostic tools (online and offline), etc.

- ***Section 11: Implementation and Sustainment***: This section describes services that DB_SUPPLIER shall provide during and following the project. This includes project management services, cutover and commissioning plan, installation support, and hardware and software maintenance activities. It also covers requirements for system documentation, training, testing, and quality assurance.

2 NASPInet System Architecture

This section describes the overall NASPInet architecture framework and overviews of the DB and PG components. While PG_SUPPLIERs are encouraged to propose their standard, field proven system architecture design, the proposed architecture must adhere to the general framework and guidelines identified in this section. The section uses architectural views to depict the various aspects of interest inherent within the system. It also captures and conveys the significant architectural preferences of the system, and reflects the defined functional and non-functional requirements based on an understanding of the strategic goals and objectives for NASPInet.

This document depicts the envisioned system architecture of NASPInet by:

- Identifying the objectives, guiding principles, and constraints driving architectural choices;
- Specifying the logical (conceptual) model that will establish major architectural aspects and services, the components that will support those services, and the component interactions; and
- Specifying the system components, including for example only the possible products and other technologies that will map into the logical architecture specification to physically instantiate the architecture.

2.1 Architectural Foundation

2.1.1 Overview

This section discusses the key drivers that have influenced the decisions underlying the envisioned NASPInet architecture. The DB_SUPPLIER and PG_SUPPLIER proposed DB/PG designs shall support these key drivers. The key drivers have been derived from many areas, including but not limited to:

- NASPInet’s current and envisioned Process, Technology, Organization and Information infrastructures;
- Specific functional and non-functional requirements;
- Existing and emerging standards for relevant Utility operations, including device communication standards, system integration standards, security standards, system and device interoperability standards, etc.;
- Existing and emerging relevant regulatory constraints such as SOX and others; and
- Existing and emerging best practices and packaged solutions for relevant Utility operations.

2.1.2 Objectives

The proposed System Architecture must enable the following objectives:

- The architecture shall provide the ability to share Phasor information and measurements, between the Publishers and Consumers of that information, under the auspices of defined interaction scenarios, message classifications, performance levels, security constraints and other governing criteria.
- Where practical and otherwise aligned with specific requirements for NASPInet, the DB_SUPPLIER/PG_SUPPLIER should consider commercially available solution components. The DB_SUPPLIER/PG_SUPPLIER shall explain the necessities or advantages of any proposed custom development.
- The System Architecture shall support fulfillment of the specified functional, non-functional, work process, information and technical goals specified in Section 3, Overall NASPInet Functional Requirements.
- NASPInet shall comply with all applicable regulatory constraints including but not limited to those specified by the FERC, SOX and others.
- The System Architecture shall enable the appropriate ongoing management and growth of NASPInet's investment in Information Technology resources consistent with NASPInet and PG_REQUESTER's IT Portfolio Management strategy and other relevant best practices.
- The architecture shall ensure end to end Quality of Service (QoS) for the spectrum of NASPInet data classes (A – E).
- The architecture shall ensure cyber security and information protection throughout the entirety of the lifecycle for NASPInet information.

2.1.3 Principles

Following are the key design principles which the NASPInet architecture must balance pragmatically in order to help enable the Objectives outlined above:

- Availability – Architectural elements shall exhibit sufficient fault tolerance, Mean Time Between Failure (MTBF), and Mean Time To Repair (MTTR) characteristics to enable defined functional and technical requirements, business goals and objectives, and business/technical values and constraints.
- Configurability – Architectural elements shall be sufficiently configurable, rather than requiring custom development, to enable defined functional and technical requirements, business goals and objectives, and business/technical values and constraints.
- Extensibility – Architectural elements shall exhibit sufficient ease of augmentation or aggregation to enable additional functional and technical requirements in the future.
- Flexibility – Architectural elements shall exhibit sufficient adaptive characteristics to rapidly enable changing operating environments.

- Instrumentation – Architectural elements shall exhibit sufficient visibility into their operations and “health” to enable defined functional and technical requirements, business goals and objectives, and business/technical values and constraints.
- Interoperability – Architectural elements shall exhibit sufficient integration mechanisms and capabilities to enable interoperability and facilitate replacements, upgrades, and/or addition of components.
- Knowledge – Sufficient knowledge transfer to appropriate stakeholders shall be provided to enable continued operations and development of the system.
- Maintainability – Architectural elements shall exhibit sufficient characteristics to support relative ease of maintenance to minimize maintenance costs.
- Manageability – Architectural elements shall exhibit characteristics that enable sufficient management of their operation and evolution to minimize system management costs.
- Performance – Architectural elements shall continuously and sufficiently deliver their solution functional capabilities within defined time and cost constraints.
- Portability – Architectural elements shall be instantiated on different development, test, and deployment platforms with relatively little effort.
- Reliability – Architectural elements shall exhibit sufficient capabilities and integrity to ensure that they and the services that they enable fulfill their functional contracts entirely.
- Scalability – Architectural elements shall exhibit a proportional (linear or greater) increase/decrease in supported load and performance given a similar increase/decrease in underlying system resources.
- Security – Architectural elements shall enable and exhibit sufficient controls on their access and use to ensure integrity of the system and data.
- Stability – Architectural elements shall exhibit sufficiently few defects relative to specifications, best practices, defined functional and technical requirements. Software defects, hardware problems, or data errors shall be detected at their source and isolated to the extent possible so as not inhibit functions of other unaffected system components and functions.
- Testability – Architectural elements shall exhibit sufficient mechanisms to enable the testing of their functional capabilities, implementation, performance, and reliability.
- Usability – Architectural elements shall exhibit sufficient overall capabilities for enabling ease of use by business users, technical developers, systems administrators, and other stakeholders.

2.2 Architectural Representation

This section provides an overview of the Architectural Representation used to describe NASPInet in subsequent sections of this document. This representation uses a set of views to describe the architecture, with each view describing the most significant aspects within a focused area of concern. The views that are reflected in this Specification document are:

- Use Case – This view describes architecturally significant usage scenarios that the proposed system must enable.
- Data Flow – This view describes, via data flow diagrams within and external to NASPInet, the high level scope and interactions to be supported by NASPInet.
- Logical – This view describes the high level conceptual components within the architecture and their various functions and relationships.
- Component – This view describes the components that instantiate the logical architecture.
- Security – This view describes the components that enable Security within NASPInet.
- Quality of Service (QoS) – This view describes functions that enable the management of QoS.
- Data – This view describes the high level logical and physical components that enable persistent and transient information flow and repositories within NASPInet.
- Network – This view describes the high level logical and physical components that enable data communication within NASPInet.
- Deployment – This view describes the high level physical instantiation of the NASPInet components identified in the Logical and Component views.

2.2.1 Use Case View

Section 3, Overall NASPInet Functional Requirements, encapsulates the envisioned processes and associated DB and PG functions for various system administration and operation activities. The processes include for example:

- Register a PG
- Change/Remove a PG registration
- Register a device and signal
- Change/remove a device/signal registration
- Subscribe streaming/historical data
- Unsubscribe streaming/historical data
- Start/stop streaming data
- Get historical data

As an example, Figure 2-1 below illustrates the use case of registering a streaming device in the form of a sequence diagram.

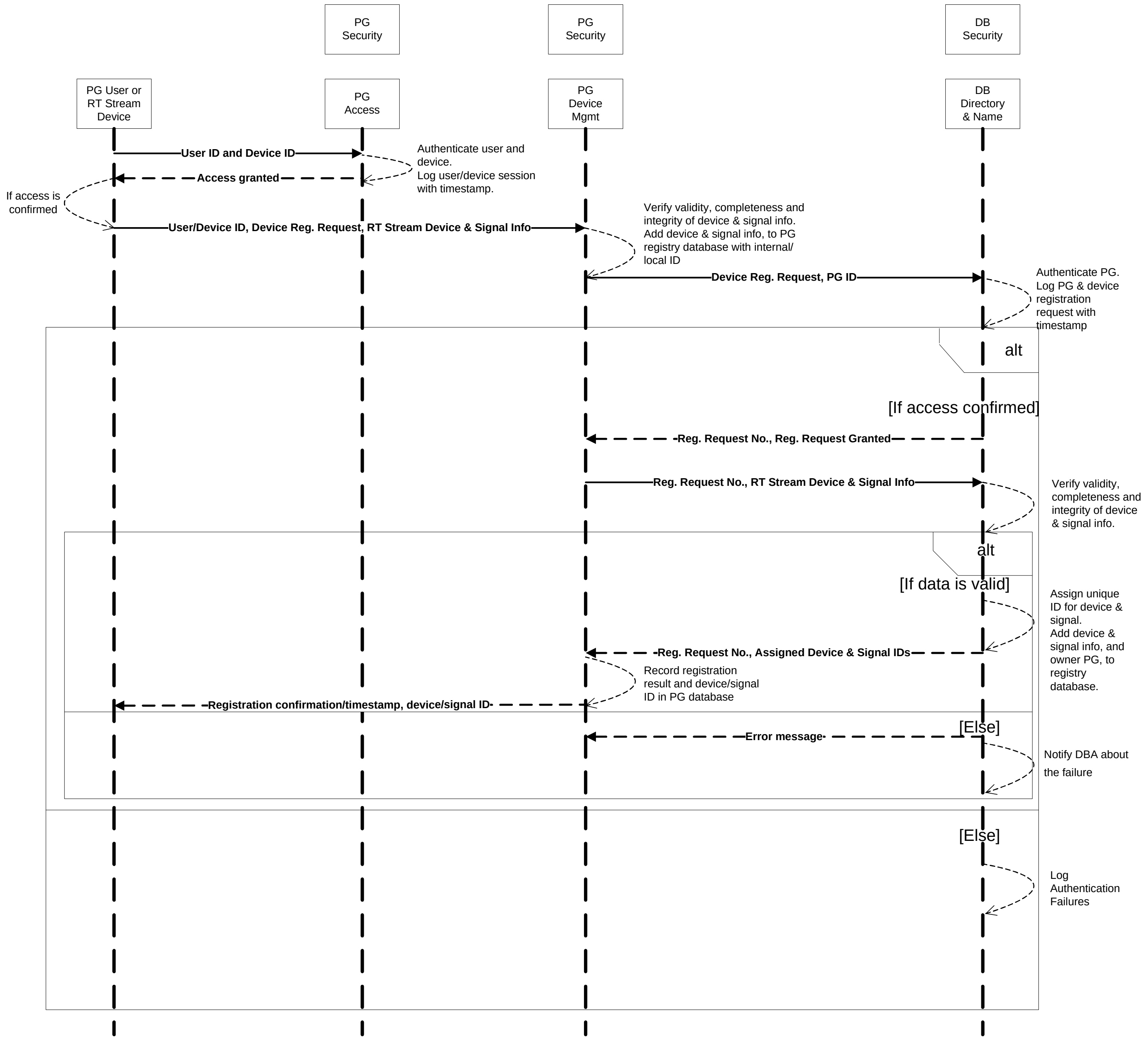

PG Security
PG Security
DB Security
PG User or RT Stream Device
PG Access
PG Device Mgmt
DB Directory & Name
User ID and Device ID
Authenticate user and device.
Log user/device session with timestamp.
Access granted
If access is confirmed
User/Device ID, Device Reg. Request, RT Stream Device & Signal Info
Verify validity, completeness and integrity of device & signal info.
Add device & signal info, to PG registry database with internal/ local ID
Device Reg. Request, PG ID
Authenticate PG.
Log PG & device registration request with timestamp
alt
[If access confirmed]
Reg. Request No., Reg. Request Granted
Reg. Request No., RT Stream Device & Signal Info
Verify validity, completeness and integrity of device & signal info.
alt
[If data is valid]
Assign unique ID for device & signal.
Add device & signal info, and owner PG, to registry database.
Reg. Request No., Assigned Device & Signal IDs
Record registration result and device/signal ID in PG database
Registration confirmation/timestamp, device/signal ID
[Else]
Error message
Notify DBA about the failure
[Else]
Log Authentication Failures

Figure 2-1: Use Case Example – Registering a Device in NASPinet

The other process sequence diagrams are interim working papers that have been translated to the overall NASPInet functional requirements in Section 3 and thus not included here in this specification document. As part of the project implementation services, the SUPPLIER/PG_SUPPLIER shall provide detailed UML representation of the processes using the specific solution proposed.

2.3 Data Flow View

2.3.1 Data Flow Definitions

2.3.1.1 Context Diagram

The context diagram (Figure 2-2) shows the scope of the types of applications that might want to interact with NASPInet in the future. This was developed to ensure that all potential types of interactions were identified and is intended to illustrate the "big picture" of potential users and applications to improve understanding of the NASPInet architecture framework. The PG_SUPPLIER scope of the specific RFP is defined in other sections of this RFP. The flows of information depicted are not meant to represent any specific level of automation. The flow of information from one system to another could be automated directly through a point to point interface via one of the stream-engine based components or it could be automatically implemented through a web service on top of an enterprise service bus component. The system context diagram is exploded into data flow diagrams to illustrate the major flows that will be supported by NASPInet and identify major system components that form the functional building blocks of NASPInet.

Table 2-1 provides more detail on the information flows depicted in the context diagram. For each information flow, the table contains the potential external system (shown on the outside boundary of the context diagram), the direction of the information flow (i.e. to NASPInet or from NASPInet), a brief description of the flow that indicates typical data items to be passed, and a description of the flow. Note that all data flows in and out of NASPInet will go through Phasor Gateways.

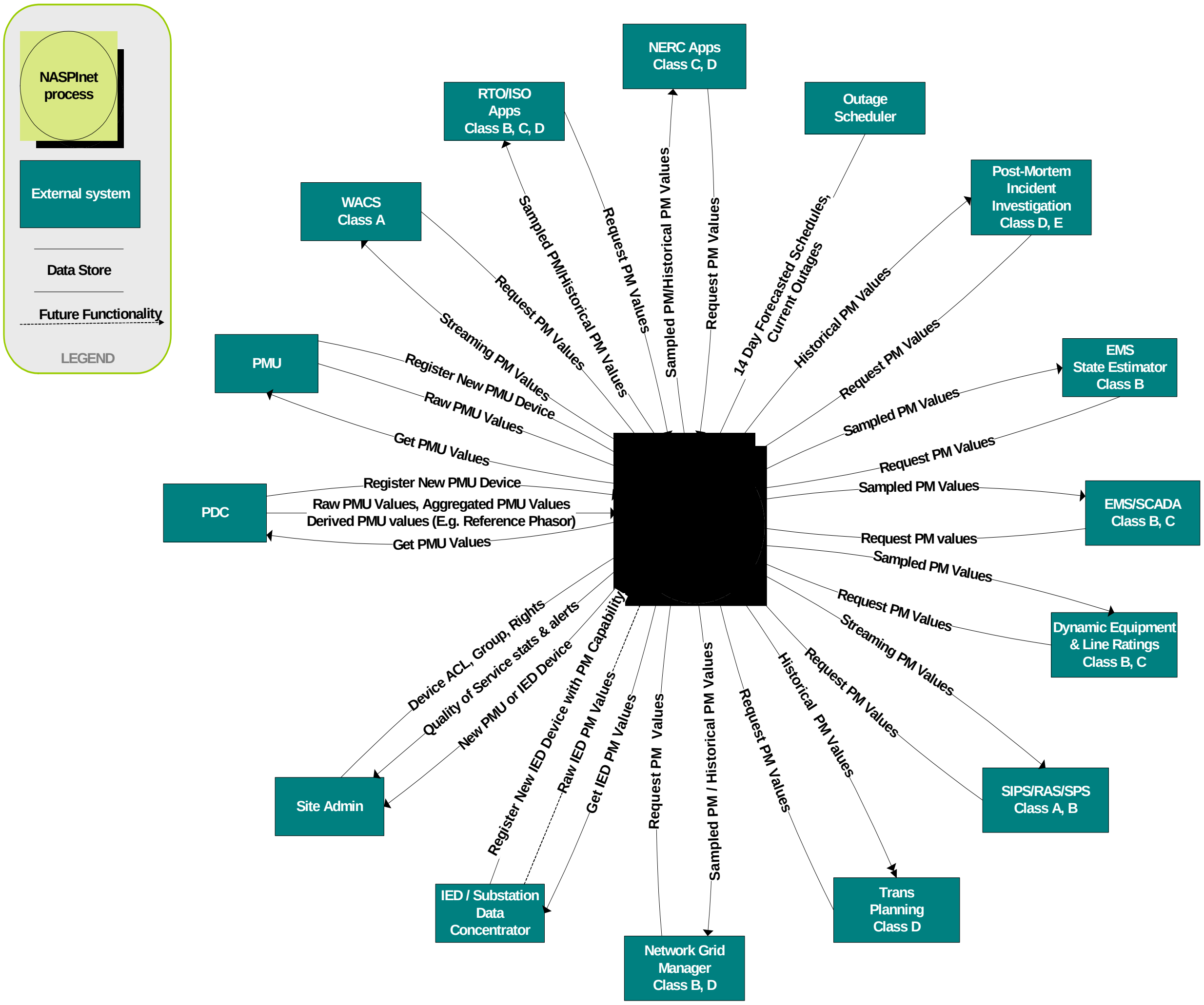


Figure 2-2: NASPinet System Context Diagram

Table 2-1: High Level NASPInet Data Flows

External System or Application	Direction	Flow Name	Description
PMU	To NASPInet	Register new PMU device	New PMUs shall be able to identify themselves to NASPInet and if they've been provisioned within the NASPInet system administration components, allowed to participate within the NASPInet community.
PMU	To NASPInet	Raw PMU data values	PMU synchro-phasor data values will typically be ingested at maximum data rate and for those applications that want less data, it will be filtered by the stream engine.
PMU	From NASPInet	Get PMU values	Request to establish a new source of PMU values for the NASPInet community.
PDC	To NASPInet	Register new PDC device	New PDCs shall be able to identify themselves to NASPInet and if they've been provisioned within the NASPInet system administration components, allowed to participate within the NASPInet community.
PDC	To NASPInet	Raw PMU data values, Derived PMU data values, Aggregated PMU values	PMU synchro-phasor data values will typically be ingested at maximum data rate and for those applications that want less data, it will be filtered by the stream engine. Need to support PDC's derived Phasor data and aggregation of signal values.
PDC	From NASPInet	Get PMU values	Request to establish a new source of processed PMU values for the NASPInet community.
Site Admin	To NASPInet	Device ACL, group, rights	NASPInet site administrator will define the access control list, groups and access rights on each PG, PDC/PMU device, and signal.

External System or Application	Direction	Flow Name	Description
Site Admin	From NASPInet	New PMU or IED device	Site Admin will be notified of when new devices are visible but not provisioned to be usable yet by the NASPInet community.
Site Admin	From NASPInet	QoS stats & alerts	Site Admin will receive QoS statistics and alerts relating to both ingested data and data received for distribution.
IED	To NASPInet	Register new IED device with PMU capability	In the future as IED functionality expands, NASPInet will allow new IED devices to register themselves.
IED	To NASPInet	Raw PM data values from IED	A potential future flow to provide synchro-phasor data values from IEDs.
IED	From NASPInet	Get PM values from IED	Request to establish a new source of PM values from IEDs for the NASPInet community.
Network Grid Manager Class B, C	To NASPInet	Request PM data and historical values	Local utility may request to visualize or to use PMU values in its own analysis applications.
Network Grid Manager Class B, C	From NASPInet	Historical PMU Values	Requested PMU values
Transmission Planning Class D	To NASPInet	Request PMU Historical Values	Local utility may request to high-quality historic values to do post-mortem analysis and to do forecasting simulations.
Transmission Planning Class D	From NASPInet	Historical PMU Values	Requested PMU values for post event investigation or forecasting and simulations.

External System or Application	Direction	Flow Name	Description
SIPS/RAS/SPS Class A, B	To NASPInet	Request PM Values	Automation and protection systems may request real-time streaming PM data for feedback and feed-forward controls.
SIPS/RAS/SPS Class A, B	From NASPInet	PM Values	Real-time streaming PM data for feedback and feed-forward controls
Dynamic Equipment & Line Ratings Class B, C	To NASPInet	Request PM Values	Potential request of PMU data at a lower sampling rate for dynamic equipment and line rating calculations or for visualization associated with such applications..
Dynamic Equipment & Line Ratings Class B, C	From NASPInet	Sampled PM Values	Sampled PM values for calculating the ratings of equipment and subsections of transmission lines in near real-time and to visualize the results.
EMS/SCADA Class B, C	To NASPInet	Request PM Stream	Request of PM data at a desired sampling rate for EMS/SCADA applications and visualization.
EMS/SCADA Class B, C	From NASPInet	Sampled PM Values	Sampled PM values for EMS/SCADA system visualization and applications
EMS State Estimator Class B	To NASPInet	Request PM Values	Request of PM data at a desired sampling rate for EMS state estimator applications.
EMS State Estimator Class B	From NASPInet	Sampled PM Values	Sampled PM values for EMS State Estimator applications
Post-Mortem Incident Investigation Class D, E	To NASPInet	Request Historical PM Values	Request for historic values with various data quality requirements based on specific needs..

External System or Application	Direction	Flow Name	Description
Incident Investigation Class D,E	From NASPInet	Historical PMU Values	Signal file to be used as part of post event investigation.
Outage Scheduler	To NASPInet	14-day forecasted or scheduled outages and current outages	Potential future flow from various outage schedulers to NASPInet for determining and providing advanced warnings on the availability of data.
NERC Apps Class C, D	To NASPInet	Request PM Values/Historical PMU values	Requests to subscription of PM values at lower sampling rates and to get high-quality historical information.
NERC Apps Class C, D	From NASPInet	Sampled PM values, Historical PM values	NERC apps are envisioned to want to be able to subscribe to NASPInet to visualize current state and to request historical information to do post-mortem analysis.
RTO/ISO Apps Class B, C, D	To NASPInet	Request PM Values Historical PM values	Requests to setup a subscription for streaming PM data and to get historical information for various RTO/ISO applications..
RTO/ISO Apps Class B, C, D	From NASPInet	Sampled PMU values, Historical PMU values	Sampled PM values and historical data for RTO/ISO users and applications.
WACS Class A	To NASPInet	Request PM Values	Advanced Wide Area Control Systems (WACS) may request real-time streaming PM data for feedback controls.
WACS Class A	From NASPInet	PM Values	Real-time streaming PM data for WACS feedback controls

The use cases and information flows illustrated by the Context Diagram and outlined in Table 2-1 above can be encapsulated into two high-level dataflow diagrams, one for data usage and one for PG administration functions. These two representative dataflow diagrams are presented below.

2.3.1.2 Phasor Gateway Data Usage Dataflow Diagram

The PG data usage dataflow (Figure 2-3) shows the systems involved in collecting PMU data, publishing it to the NASPInet DB and distributing it to the subscribers of streaming and sampled PMU data and to the requestors of historical PMU data. This dataflow diagram also breaks out the NASPInet component represented in the context diagram and presents some of the building block architectural components of the NASPInet Phasor Gateway:

- Phasor Gateway Ingest Service: This is a logical component of the PG that uses and interfaces with the DB services through the DB APIs to ingest streaming and historical PM data from devices (PMU, PDC, IED) connected to the PG into the DB. In other words, the DB services enable these data functions in the PG through interfacing with the PG Ingest Service component.

- Phasor Gateway Distributor: This is a logical component of the PG that uses and interfaces with the DB services through the DB APIs to get streaming and historical PM data available from NASPInet, and distribute the data to users and applications connected to the PG via the PG APIs. A Gatway Cache is represented in the dataflow diagram to indicate some local memory and data storage capability in the PG to improve its performance and overall data availability, if needed.

- Phasor Gateway Historian: This is a logical component of the PG that uses and interfaces with the DB services through the DB API to get historical data from external PGs or other connected historical PM data sources, and distribute the data to users and applications connected to the PG via the PG APIs. A PMU Data Mart is represented in the dataflow diagram as a placeholder for the potential future possibility that the DB_REQUESTER may want to have data store capability for select data within the DB. Regardless, the logical service PG Historian component is still applicable as it would manage historical data requests and the resulting data processing in the PG as indicated above.

Figure 2-3 depicts the ingestion of streaming data from the PMUs and potentially in the future: IEDs via substation data concentrators, and shows the data being archived to support requests for historical information.

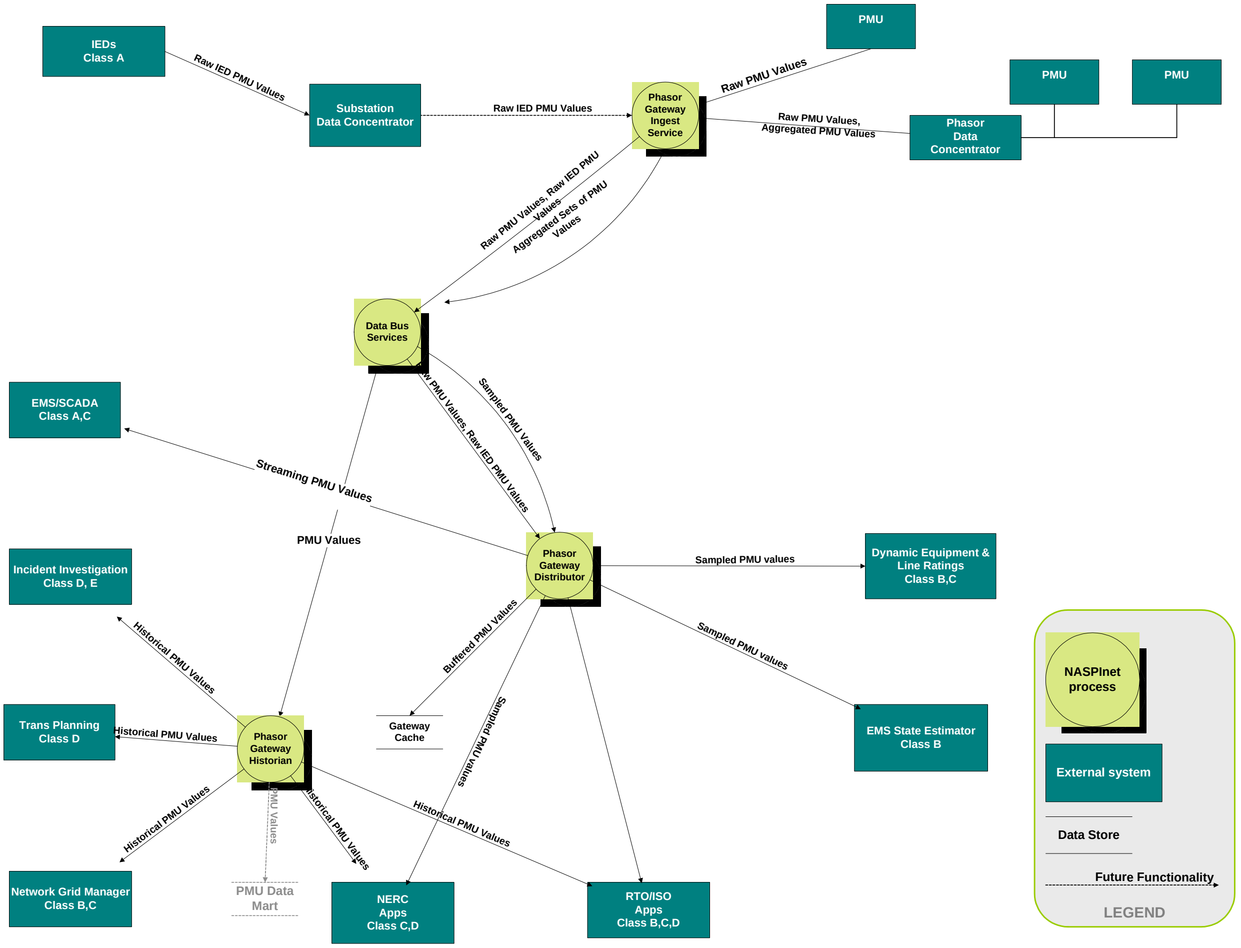


Figure 2-3: PG Data Usage DFD

2.3.1.3 Phasor Gateway Administration Dataflow Diagram

The PG administration dataflow (Figure 2-4) shows the various flows associated with managing PMU devices, granting access to new device signals, removing old devices, having applications setup subscriptions with NASPInet for PMU data, being authenticated and being able to monitor and view the current performance of NASPInet.

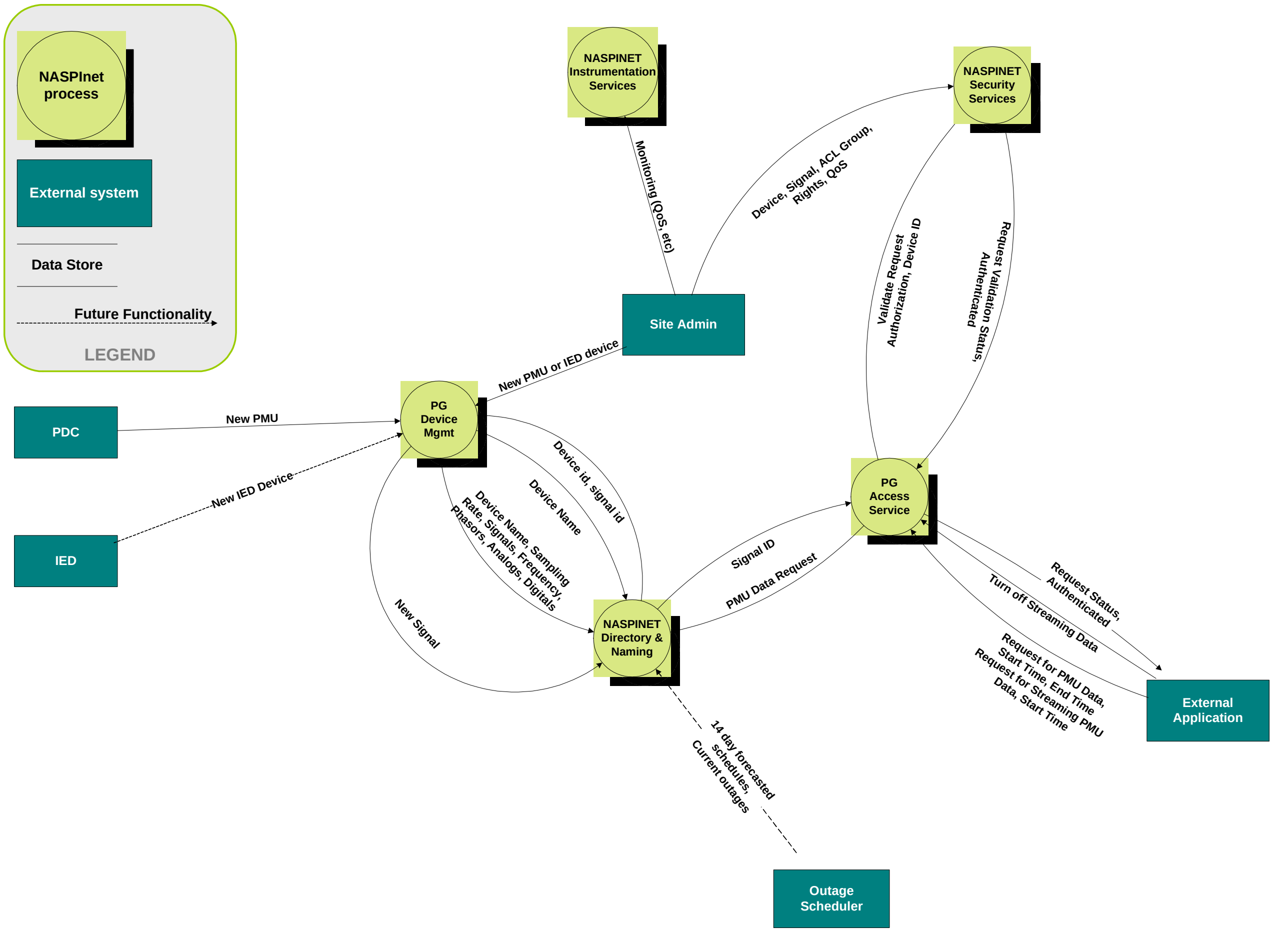

NASPInet process
External system
Data Store
Future Functionality
LEGEND
NASPINET Instrumentation Services
NASPINET Security Services
Monitoring (QoS, etc)
Device, Signal, ACL Group, Rights, QoS
Validate Request Authorization, Device ID
Request Validation Status, Authenticated
Site Admin
New PMU or IED device
PDC
New PMU
IED
New IED Device
PG Device Mgmt
Device id, signal id
Device Name
Device Name, Sampling Rate, Signals, Frequency, Phasors, Analogs, Digitals
New Signal
PG Access Service
Signal ID
PMU Data Request
NASPINET Directory & Naming
Request Status, Authenticated
Turn off Streaming Data
Request for PMU Data, Start Time, End Time
Request for Streaming PMU Data, Start Time
External Application
14 day forecasted schedules, Current outages
Outage Scheduler

Figure 2-4: PG Administration DFD

2.4 Logical View

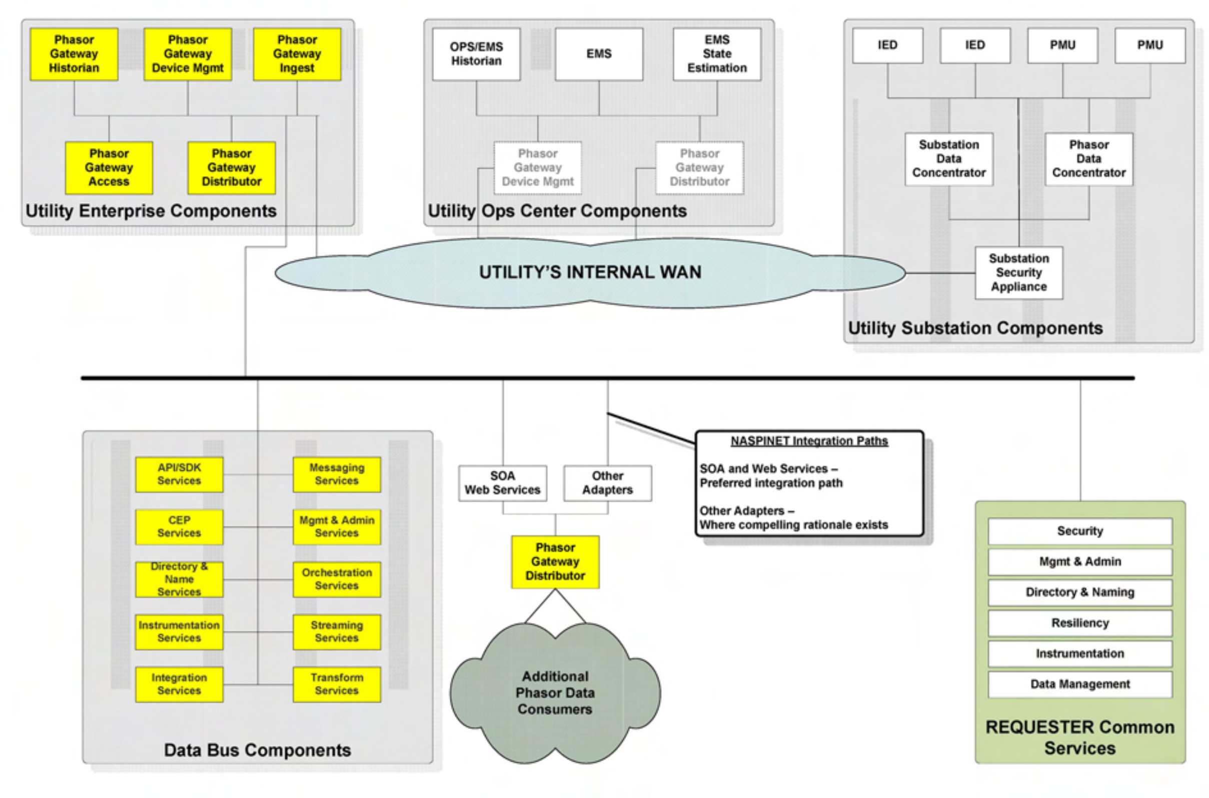
2.4.1 Introduction

The intent of this view is to describe the high level components that form the Phasor Gateway and Data Bus macro entities within the envisioned NASPInet architecture. The diagram (Figure 2-5) maps these components to the business entities in which they would most likely be deployed:

- Utility and Other User Organization (e.g. NERC) Enterprise Level
- Operational Centers
- Substations

The following assumptions apply to the Logical View:

- Services – Within the Data Bus and the Requester's enterprise IT Common Services domains, references are made to "services" such as Streaming Data Services or Security Services. At this level of abstraction, these components are not intended to represent instantiated services but are instead a blanket term to describe the general functionality delivered by a particular set of components.
- Service-Oriented Architecture – An SOA-based approach is one possible solution to parts of NASPInet development and integration, however the intent of this diagram is not to imply that SOA is a preferred or proscribed approach. Rather, SOA should be employed where it adds value (such as propensity for reuse, abstraction, etc.) and can meet the requirements of the functionality to be enabled (such as performance, latency, security, etc.).
- Web Services – Similarly to SOA, we allow for the possibility that a Web Services-based approach to development and integration, or even a derivative approach such as XML-RPC, may be viable where it adds value and meets requirements.



Phasor Gateway Historian
Phasor Gateway Device Mgmt
Phasor Gateway Ingest
Phasor Gateway Access
Phasor Gateway Distributor
Utility Enterprise Components
OPS/EMS Historian
EMS
EMS State Estimation
Phasor Gateway Device Mgmt
Phasor Gateway Distributor
Utility Ops Center Components
IED
IED
PMU
PMU
Substation Data Concentrator
Phasor Data Concentrator
Substation Security Appliance
Utility Substation Components
UTILITY'S INTERNAL WAN
API/SDK Services
Messaging Services
CEP Services
Mgmt & Admin Services
Directory & Name Services
Orchestration Services
Instrumentation Services
Streaming Services
Integration Services
Transform Services
Data Bus Components
SOA Web Services
Other Adapters
NASPINET Integration Paths
SOA and Web Services – Preferred integration path
Other Adapters – Where compelling rationale exists
Phasor Gateway Distributor
Additional Phasor Data Consumers
Security
Mgmt & Admin
Directory & Naming
Resiliency
Instrumentation
Data Management
REQUESTER Common Services

Figure 2-5: NASPInet System Components Logical View

2.4.2 Logical View Details

The Phasor Gateway components shall include:

- Phasor Gateway Distributor – all of the data request services shall be supplied by this component. All external applications and systems shall communicate to NASPInet via services provided by this system component. This component shall make use of Data Bus services providing the API/SDK and Directory/Naming services.

- Phasor Gateway Ingest – As depicted in the ingest Data Flow Diagram, the services provided by this component shall deal with communicating with devices in the substation and potentially aggregating them before putting them on the data bus for consumption.

- Phasor Gateway Device Management – This component shall make use of the NASPInet Data Bus services and the PG specific services to support adding, removing, activating and de-activating devices.

- Phasor Gateway Access - This component shall make use of the NASPInet Data Bus services and where appropriate the Requester's enterprise IT Common Services, as well as the PG specific services to provide the security administration services to grant user roles/application access to specific device and signal data.

- Phasor Gateway Historian – As far as having historical data stores within NASPInet, unless stated otherwise by the PG_REQUESTER, this component is out of scope of the PG_SUPPLIER but has been included to manage historical data requests and process the obtained data (data that is stored in sources connected to but not part of NASPInet.

The Data Bus infrastructure shall enable the flow of Phasor and other information between Phasor Gateways and additional appropriate entities interacting with NASPInet. The major functional characteristics of the Data Bus shall include:

- Implementation via middleware that provides QoS and security guarantees. The middleware shall provide abstractions for QoS and security services. An abstraction of a potential future extension of NASPInet is the notion "virtual signal" for a PMU signal, which is the sub-sampled (lower rate) data stream of the original PMU data stream, supporting subscribers who may not need the complete PMU data stream.

- Providing information connectivity between producers and consumers of Phasor data including streaming (message-based, publish/subscribe, asynchronous and synchronous with guaranteed delivery scenarios), historical Phasor data, and other non Phasor data such as NASPInet QoS metrics and event/error logs:
    - Unicast – Data Bus shall support secure unicast (point-to-point) information flow with specified security and QoS properties.
    - Publish/Subscribe – Data Bus shall support multicast capabilities to implement publisher/subscriber model of data exchange in a resource-efficient manner. Security services shall ensure that published data will only reach those entities that have been

authorized to receive that data; subscribed data will only come from the authorized publishers.

- Ensuring information flow relative to defined classes which specify latency, Quality of Service and other characteristics inherent to that class:
    - QoS management – The middleware shall implement a distributed resource management architecture that encompasses a set of algorithms for resource monitoring, QoS mapping, admission control, resource reservation, resource negotiation and other attributes. The architecture shall support a diverse set QoS classes with wide range of rate, delay, delay-jitter and other requirements.
    - The architecture shall support a set of predefined QoS (priority) and that application services are mapped onto these classes for resource management purposes. The QoS mapping function shall map application level QoS into system level QoS in terms of bandwidth, delay, jitter, CPU demand, etc.
    - The admission control function shall determine if an incoming flow (with certain QoS and security specification) is admitted into NASPInet without jeopardizing the QoS and security guarantees that have been provided to the previously admitted flows. Admission control shall account for both QoS and security requirements of the information flow. If a higher priority flow cannot be admitted due to constrains on sufficient resources, a lower priority flow shall be degraded in QoS or even be dropped to accommodate the higher priority flow. This functionality is called QoS adaptation. For admitted flows, the QoS guarantees shall be ensured through resource reservations and run-time scheduling algorithms.
- Providing an integration framework for the entities communicating using the Data Bus.
- Enabling transformation of the data flowing through the bus.
- Providing the ability to execute business logic, including process and event-based logic, based on the data transiting the bus.
- Functioning under the broader auspices of Requester's enterprise IT Common Services including but not limited to Security, Management and Administration.

The Data Bus Components shall implement the following macro-level services generally within the Data Bus:

- API/SDK (Application Programming Interface / Software Development Kit) – This service shall enable applications, integration mechanisms, user interfaces, content delivery and other NASPINET components to be customized, developed and deployed.
- CEP (Complex Event Processing) – This service shall enable event-driven processing, such as actions to be performed based on the values of multiple phasor measurement units and/or IEDs.

- Name & Directory – This service shall enable the registry of services, components, processes, streams and other entities internal to the Data Bus for subsequent invocation.
- Instrumentation – In concert with Management and Administration Services, instrumentation services shall provide visibility into key aspects of Data Bus components and services, such as performance, utilization and general health indicators.
- Integration – This service shall enable external integration to NASPInet by exposing Data Bus services, processes and components via adapters.
- Messaging – This service shall enable synchronous and asynchronous message-based communication between NASPInet components and services with support for features such as guaranteed delivery, publish/subscribe and content-based routing.
- Management & Administration – This service shall enable the initial configuration and ongoing operation of Data Bus components and services.
- Orchestration – This service shall enable business process modeling, development, instantiation, execution and monitoring functionality. An example would be the processes to support the provisioning of new Phasor Gateway Devices.
- Streaming – This service shall enable massive volume, low latency delivery and processing of NASPInet data from Phasor Devices and other IEDs.
- Transform – This service shall enable data transformation to be performed on the information flowing through the Data Bus.

The NASPInet DB and PG shall utilize, be compatible and integrate with the Requester's enterprise IT Common Services to perform the following macro-level services throughout the NASPInet infrastructure. Contrasting some of these services with equivalent services within the context of the DB and PG, such as System Management and Administration, the Common Services shall perform similar functions but on a broader scale throughout the Requester's enterprise IT infrastructure.

- Security – this service shall provide enabling services and infrastructure to ensure the appropriate access to and usage of NASPInet resources and information. Key components typically include Authentication, Authorization, Access Control, Confidentiality, Auditing, Non-Repudiation and many others.
- Management & Administration – this service shall enable the initial configuration and ongoing operation of NASPInet components and services, and will likely integrate or aggregate the analogous but more focused services within the Data Bus.

- Name & Directory – this service shall enable the system-wide registry of Phasor Measurement devices as well as the services, components, processes and other entities required by the Phasor Gateway and/or Data Bus components.
- Resiliency – This service and infrastructure to ensure critical system attributes such as Fault Tolerance, Availability, Disaster Recovery, Business Continuity and similar aspects.
- Instrumentation – In concert with NASPInet Management and Administration Services, this service shall provide visibility into key aspects of the NASPInet infrastructure such as performance, utilization and general health indicators.
- Data Management – this service shall enable the logical and physical architecture, storage, access and management of persistent and transient data within NASPInet. Key components typically include Relational Database Management engines, Storage Area Network infrastructure, Metadata Management, Hierarchical Storage Management, Information Lifecycle Management and other services.

2.5 Component View

2.5.1 Introduction

The intent of the Architecture and Software Componemt views (Figure 2-6 and Figure 2-7) is to describe the next level of detailed components that form the Phasor Gateway and Data Bus macro entities within the envisioned NASPInet architecture. The diagrams further decompose the Logical View presented earlier into the macroscopic building blocks encapsulated within that view's components.

The following assumptions apply to the Component View and diagrams:

- The diagrams reference commercially available components at a high level, for example Enterprise and Streaming middleware. This is in no way intended as a constrained or preferred solution, but rather an assessment of classes of commercial components that could conceivably play a role within the NASPInet architecture.

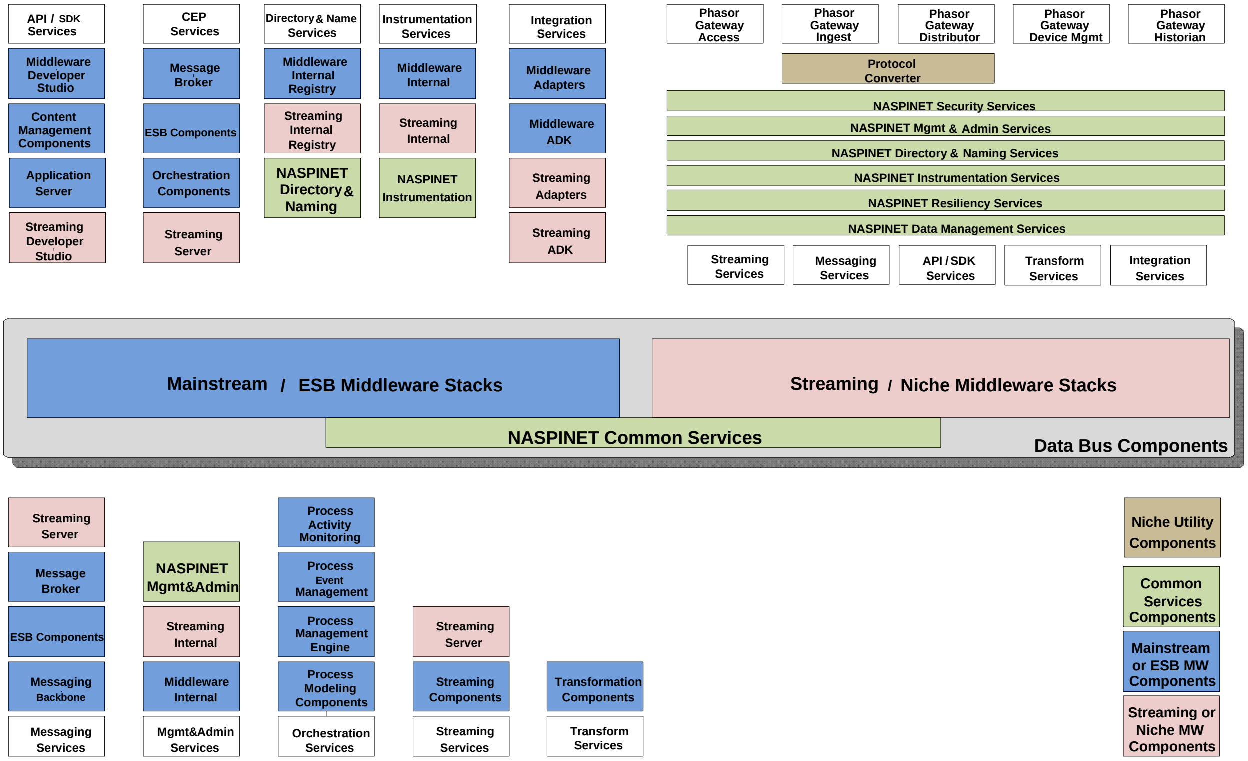


Figure 2-6: NASPInet Architecture Components

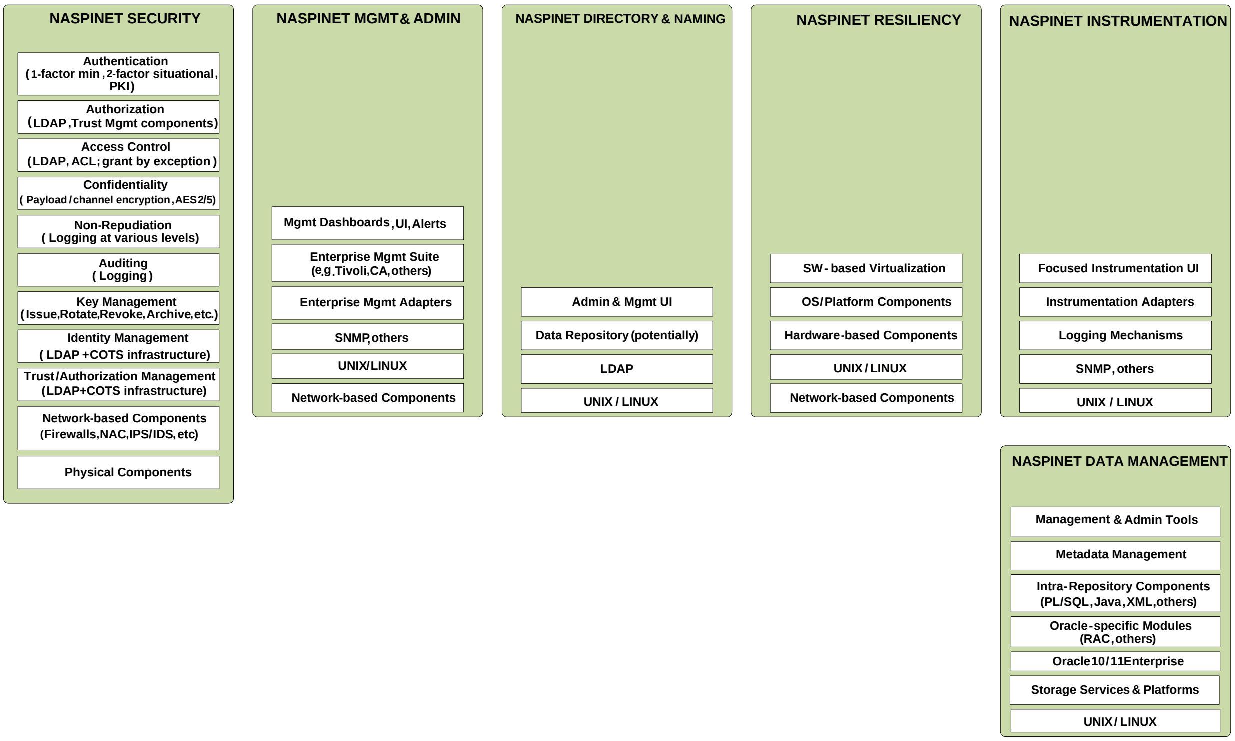

NASPINET SECURITY
Authentication (1-factor min, 2-factor situational, PKI)
Authorization (LDAP, Trust Mgmt components)
Access Control (LDAP, ACL; grant by exception)
Confidentiality (Payload / channel encryption, AES2/5)
Non-Repudiation (Logging at various levels)
Auditing (Logging)
Key Management (Issue,Rotate,Revoke,Archive,etc.)
Identity Management (LDAP +COTS infrastructure)
Trust/Authorization Management (LDAP+COTS infrastructure)
Network-based Components (Firewalls,NAC,IPS/IDS,etc)
Physical Components
NASPINET MGMT & ADMIN
Mgmt Dashboards, UI, Alerts
Enterprise Mgmt Suite (e.g.Tivoli,CA,others)
Enterprise Mgmt Adapters
SNMP, others
UNIX/LINUX
Network-based Components
NASPINET DIRECTORY & NAMING
Admin & Mgmt UI
Data Repository (potentially)
LDAP
UNIX / LINUX
NASPINET RESILIENCY
SW-based Virtualization
OS/Platform Components
Hardware-based Components
UNIX / LINUX
Network-based Components
NASPINET INSTRUMENTATION
Focused Instrumentation UI
Instrumentation Adapters
Logging Mechanisms
SNMP, others
UNIX / LINUX
NASPINET DATA MANAGEMENT
Management & Admin Tools
Metadata Management
Intra-Repository Components (PL/SQL, Java, XML, others)
Oracle-specific Modules (RAC, others)
Oracle10/11Enterprise
Storage Services & Platforms
UNIX / LINUX

Figure 2-7: NASPInet Software Components

2.5.2 Component View Details

Note that some of the components depicted in Figure 2-6 are in different subsystems (DB, PG, and enterprise IT Common Services); they will be described once only in the following text. Also, the software components in Figure 2-7 are common IT terms (e.g. LDAP, SNMP, UNIX/LINUS, etc.) and hence not explained further here.

- Middleware & Streaming Developer Studios – shall enable solution developers to configure, customize and develop other NASPInet Data Bus components; examples would include adapters, business logic and many others.
- Content Management – shall enable the development, publishing and management of content such as web-based information, context-sensitive help and other textual and graphical content elements.
- Application Server – shall provide the framework in which Data Bus components can be instantiated and executed, monitored and managed to perform their intended functions; an example would be J2EE or managed code components.
- Message Broker – shall provide the framework for message delivery within the Data Bus and exposes functionality such as Publish/Subscribe, asynchronous messaging, guaranteed delivery and more.
- ESB Components – shall provide the framework for developing and exposing services for complex architectures within the Data Bus, as well as providing the features with which a Service-Oriented Architecture (SOA) may be implemented.
- Orchestration Services & Components – shall provide the mechanisms by which complex, process-based business logic can be modeled (via Process Modeling), instantiated and executed (Process & Event Management) and monitored (Activity Monitoring) within the Data Bus.
- Streaming Server – shall provide the framework for processing streaming data within the NASPInet Data Bus. Streaming Data is characterized by continuous (or nearly so) output, processing and delivery according to Quality of Service (QoS) tiers defined in terms of data volume, latency and other parameters.
- Enterprise and Streaming Middleware Internal Registry – shall provide mechanisms within the Data Bus middleware that manage the registry and discovery of services offered by the Data Bus.
- Enterprise, Streaming Middleware, and other NASPInet Internal Instrumentation – shall provide mechanisms within the Data Bus middleware components that measure and indicate the functional health of those components.
- Middleware & Streaming Adapters – shall provide pre-built integration functionality for Enterprise and Streaming middleware frameworks which can then be configured, customized or

aggregated to deliver integration services for the Data Bus; examples could include adapters for 3rd party software products, protocol adapters such as XML-RPC and many others.

- Middleware & Streaming Adapter Development Kit (ADK) – shall provide the tools, such as language libraries and Application Programming Interfaces that enable developers to configure, customize or build new adapters for the Data Bus.
- NASPInet Security Services – described in more detail in the next subsection.
- Enterprise & Streaming Middleware Internal Management & Administration – shall provide mechanisms within the Data Bus middleware components that enable the management of those components and their internal functionality.
- Transformation Components – shall provide the mechanisms by which information flowing within the Data Bus can identified, segregated, transformed in terms of format/content/interpretation, aggregated or otherwise affected during its transit from source entity to destination entity; an example of transformation could include splitting a group of PG signals into its components preparatory to subscriber delivery.
- Name & Directory Services – shall enable the system-wide registry of Phasor Gateways, Phasor Measurement Units, and IED devices as well as the services, components, processes and other entities required by the Phasor Gateway and/or Data Bus components.
- Instrumentation Services – In concert with DB Management and Administration Services, shall provide visibility into key aspects of the NASPInet infrastructure, such as performance, utilization and general health indicators, for the DB network, hardware and software subsystems of DB and PG.
- Resiliency Services – shall ensure critical system attributes such as Fault Tolerance, Availability, Disaster Recovery, Business Continuity and similar aspects.
- Data Management Services – shall enable the logical and physical architecture, storage, access and management of persistent and transient data within NASPInet. Key components typically include Relational Database Management engines, Storage Area Network infrastructure, Metadata Management, Hierarchical Storage Management, Information Lifecycle Management and other services.

2.6 Security View

2.6.1 Introduction

The intent of this view (Figure 2-8 and Figure 2-9) is to describe at a high level those components which provide Security within the envisioned NASPInet architecture. The diagrams further decompose the Logical View presented earlier into the focused classes of components which provide security in the major areas of concern including Authentication, Authorization, Access Control, Confidentiality, Integrity, Non-Repudiation, Auditing, Platform, Network, and Physical Security.

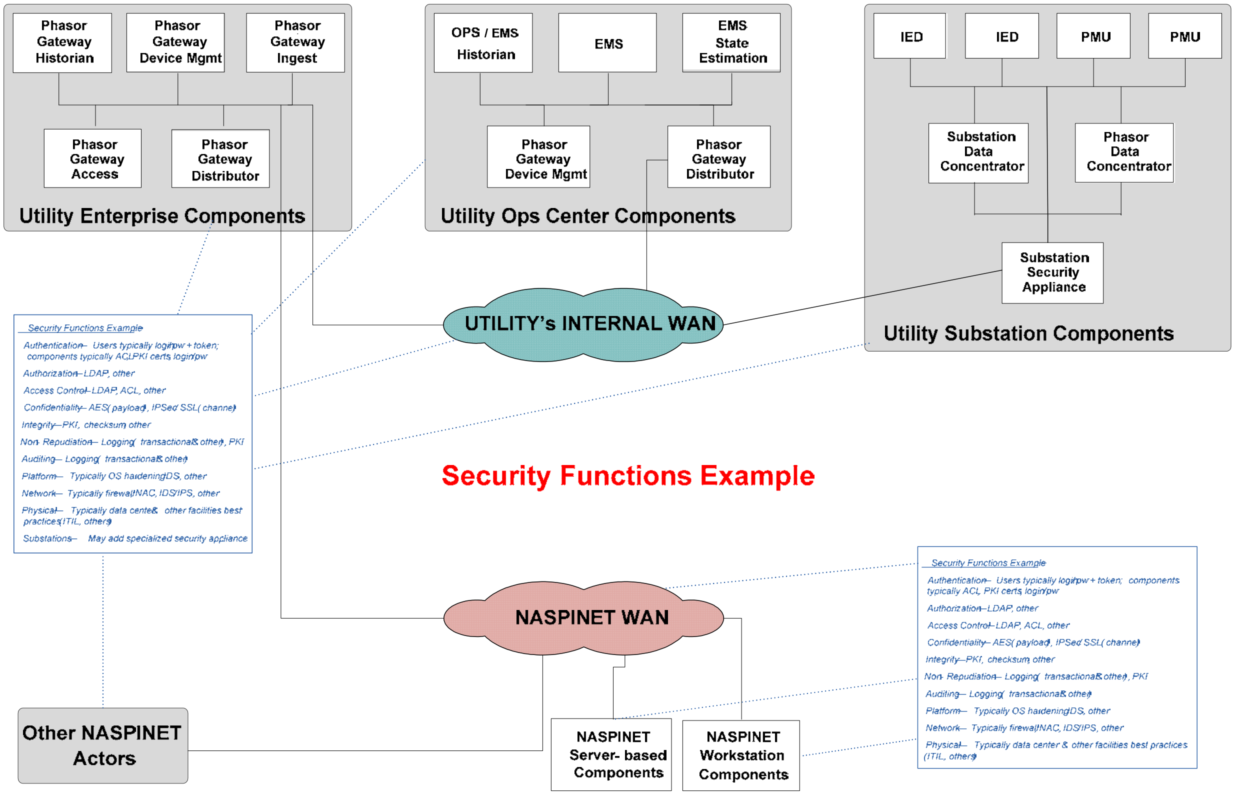
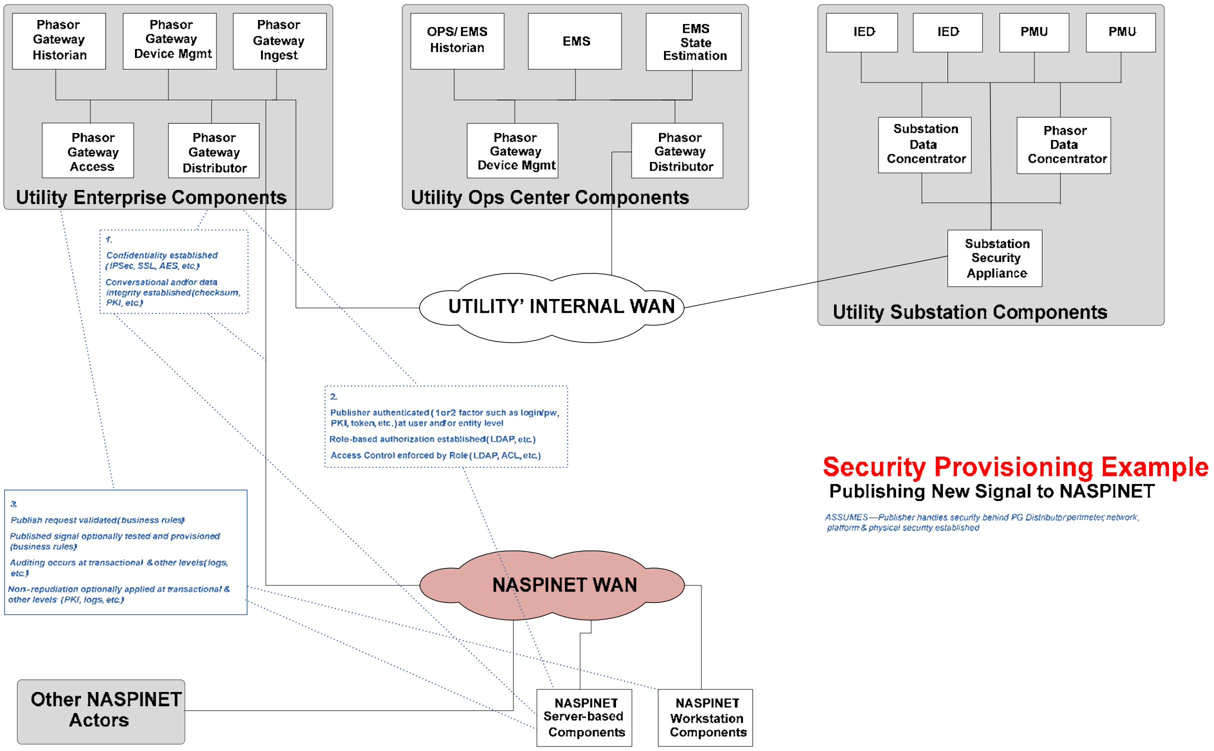

Phasor Gateway Historian
Phasor Gateway Device Mgmt
Phasor Gateway Ingest
Phasor Gateway Access
Phasor Gateway Distributor
Utility Enterprise Components
OPS / EMS Historian
EMS
EMS State Estimation
Phasor Gateway Device Mgmt
Phasor Gateway Distributor
Utility Ops Center Components
IED
IED
PMU
PMU
Substation Data Concentrator
Phasor Data Concentrator
Substation Security Appliance
Utility Substation Components
UTILITY's INTERNAL WAN
Security Functions Example
Authentication – Users typically login/pw + token; components typically ACL, PKI certs, login/pw
Authorization – LDAP, other
Access Control – LDAP, ACL, other
Confidentiality – AES (payload), IPSec/ SSL (channel)
Integrity – PKI, checksum, other
Non-Repudiation – Logging (transactional & other), PKI
Auditing – Logging (transactional & other)
Platform – Typically OS hardening, IDS, other
Network – Typically firewall, NAC, IDS/IPS, other
Physical – Typically data center & other facilities best practices (ITIL, others)
Substations – May add specialized security appliance
Security Functions Example
NASPINET WAN
Security Functions Example
Authentication – Users typically login/pw + token; components typically ACL, PKI certs, login/pw
Authorization – LDAP, other
Access Control – LDAP, ACL, other
Confidentiality – AES (payload), IPSec/ SSL (channel)
Integrity – PKI, checksum, other
Non-Repudiation – Logging (transactional & other), PKI
Auditing – Logging (transactional & other)
Platform – Typically OS hardening, IDS, other
Network – Typically firewall, NAC, IDS/IPS, other
Physical – Typically data center & other facilities best practices (ITIL, others)
Other NASPINET Actors
NASPINET Server-based Components
NASPINET Workstation Components

Figure 2-8: NASPInet Architecture – Security Functions Example


Phasor Gateway Historian
Phasor Gateway Device Mgmt
Phasor Gateway Ingest
Phasor Gateway Access
Phasor Gateway Distributor
Utility Enterprise Components
OPS/ EMS Historian
EMS
EMS State Estimation
Phasor Gateway Device Mgmt
Phasor Gateway Distributor
Utility Ops Center Components
IED
IED
PMU
PMU
Substation Data Concentrator
Phasor Data Concentrator
Substation Security Appliance
Utility Substation Components
UTILITY' INTERNAL WAN
NASPINET WAN
Other NASPINET Actors
NASPINET Server-based Components
NASPINET Workstation Components

1.
Confidentiality established (IPSec, SSL, AES, etc.)
Conversational and/or data integrity established (checksum, PKI, etc.)

2.
Publisher authenticated (1or2 factor such as login/pw, PKI, token, etc.) at user and/or entity level
Role-based authorization established (LDAP, etc.)
Access Control enforced by Role (LDAP, ACL, etc.)

3.
Publish request validated (business rules)
Published signal optionally tested and provisioned (business rules)
Auditing occurs at transactional & other levels (logs, etc.)
Non-repudiation optionally applied at transactional & other levels (PKI, logs, etc.)

Security Provisioning Example
Publishing New Signal to NASPINET
ASSUMES—Publisher handles security behind PG Distributor perimeter; network, platform & physical security established

Figure 2-9: NASPInet Architecture – Security Provisioning Example

2.6.2 Security View Details

Ensuring QoS and maintaining cyber security are two main requirements of NASPInet. However, meeting one requirement may cause the degradation on meeting the other requirement. For example, increasing security by using longer encryption key will require more processing time at PGs during encrypting and decrypting processes, which may result in NASPInet not being able to meet QoS (e.g., end-to-end delay, delay jitter) requirement.

The design shall ensure that both the required QoS and security properties for the various flows are supported in the NASPInet. In case of overloads that arise due to unanticipated contingencies, suitable resource management mechanisms shall be in place to degrade QoS for low-priority flows, or even drop them if necessary, to support high-priority flows while protecting system integrity and security.

The design shall also address QoS and security guarantees for multicast flows for efficient implementation of publisher/subscriber model of data communication. The key distribution and rekeying overhead shall be kept small in order to meet this requirement.

Section 7 of this RFP focuses on Security.

2.7 Quality of Service (QoS) Management

The proposed system shall support a distributed resource management architecture that encompasses a set of algorithms for resource monitoring, QoS mapping, admission control, resource reservation, resource negotiation. The architecture shall support a diverse set of QoS classes with wide range of rate, delay, and delay-jitter requirements. The architecture shall support a set of predefined QoS (priority), and the application services shall be mapped onto these classes for resource management purposes. The QoS mapping function shall map application level QoS into system level QoS in terms of bandwidth, delay, jitter, CPU demand, and other such items. The admission control function shall determine if an incoming flow (with certain QoS and security specification) can be admitted into the NASPInet without jeopardizing the QoS and security guarantees that have been provided to the previously admitted flows. The admission control shall account for both QoS and security requirements of the flow.

QoS adaption capabilities shall be provided. That is, if a higher priority flow cannot be admitted due to unavailability of sufficient resources, a lower priority flow shall be degraded in QoS or even be dropped to accommodate the high priority flow.

For admitted flows, the QoS guarantees shall be ensured through resource reservations and run-time scheduling algorithms. In summary, the middleware must support a distributed QoS management architecture, security architecture, and their interactions.

2.8 Risk-based Approach to System Design

It is quite possible that the designer will be faced with the dilemma of choosing among achieving the required QoS, robust dependability (reliability and availability), and strong information assurance guarantees. In some of these cases, it may not be possible to meet all these three key requirements simultaneously due to resource constraints, unavailability of suitable algorithms and technologies, and possibly lack of interoperability among various technologies. To address such cases, a risk based design approach should be adopted. Risk is the net negative impact of the exercise of a given security vulnerability, QoS violation, or fault condition, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

To balance the tradeoffs among QoS, security, and dependability metrics, a risk based system design approach should be adopted as the guiding principle to minimally relax guarantees on one metric over others. To practically achieve that, for each of the three metrics (QoS, security, dependability), multiple levels of guarantees should be defined. Each application, flow, and service specifies its guarantees at two levels: “desired level” – the guarantee level it ideally requires, and the “acceptable level” – the guarantee level that it can live with. In between a given “acceptable” and “desired” levels, there could be multiple discrete levels of guarantees that can be supported by the NASPSInet. When tradeoff arises in the design, the risk-based approach would relax one or more metrics from their desired level to lower levels subject to the constraint that none of the metric is relaxed below the desired level. Also, the risk based design should attempt to improve the level of guarantees as much as possible beyond the “acceptable” level of each metric. In case if “acceptable” level itself is not guaranteed even for a metric, then the service/flow/application should not be realized, and exception must be generated and reported to the administrator.

The following NIST publications provide good practices for a risk-based design approach.

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

http://csrc.nist.gov/groups/SMA/fisma/framework.html

2.9 Data View

2.9.1 Introduction

The intent of this view (Figure 2-10) is to describe at a high level those components which provide data management and persistence within the envisioned NASPInet architecture. The diagram describes the existence of data management and persistence components within the Utility enterprise, the NASPInet architecture itself, and externally to NASPInet. The following assumptions apply to the Data View:

- Persistent storage shall follow industry best practices for file system and enterprise Relational Database Management System (RDBMS) products including but not limited to logical data models and architecture, physical data deployment, storage services, performance and resiliency characteristics including RAID implementations, security, etc.
- Transient storage, such as in-memory databases, temporary storage or others, may exist in the NASPInet architecture as processing components (e.g. for streaming data) as appropriate.
- Storage characteristics may potentially include spatial data attributes, content-addressable storage, Hierarchical Storage and Information Lifecycle Management constructs, and other technology enabling NASPInet objectives.

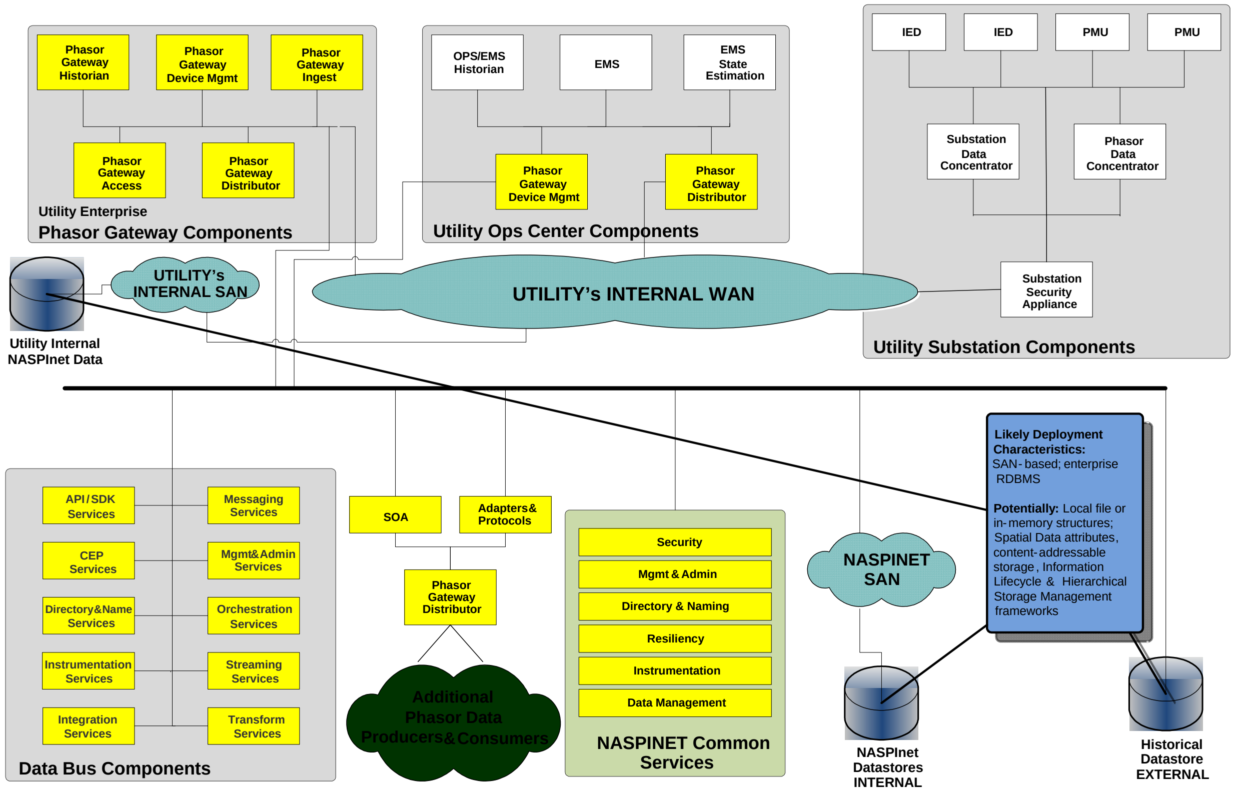

Phasor Gateway Historian
Phasor Gateway Device Mgmt
Phasor Gateway Ingest
Phasor Gateway Access
Phasor Gateway Distributor
Utility Enterprise
Phasor Gateway Components
OPS/EMS Historian
EMS
EMS State Estimation
Phasor Gateway Device Mgmt
Phasor Gateway Distributor
Utility Ops Center Components
IED
IED
PMU
PMU
Substation Data Concentrator
Phasor Data Concentrator
Substation Security Appliance
Utility Substation Components
Utility Internal NASPInet Data
UTILITY's INTERNAL SAN
UTILITY's INTERNAL WAN
Likely Deployment Characteristics:
SAN- based; enterprise RDBMS
Potentially: Local file or in- memory structures; Spatial Data attributes, content- addressable storage , Information Lifecycle & Hierarchical Storage Management frameworks
API / SDK Services
Messaging Services
CEP Services
Mgmt& Admin Services
Directory& Name Services
Orchestration Services
Instrumentation Services
Streaming Services
Integration Services
Transform Services
Data Bus Components
SOA
Adapters & Protocols
Phasor Gateway Distributor
Additional Phasor Data Producers & Consumers
Security
Mgmt & Admin
Directory & Naming
Resiliency
Instrumentation
Data Management
NASPINET Common Services
NASPINET SAN
NASPInet Datastores INTERNAL
Historical Datastore EXTERNAL

Figure 2-10: NASPInet Architecture – Data View

2.9.2 Data View Details

The proposed system architecture shall support the following types of data:

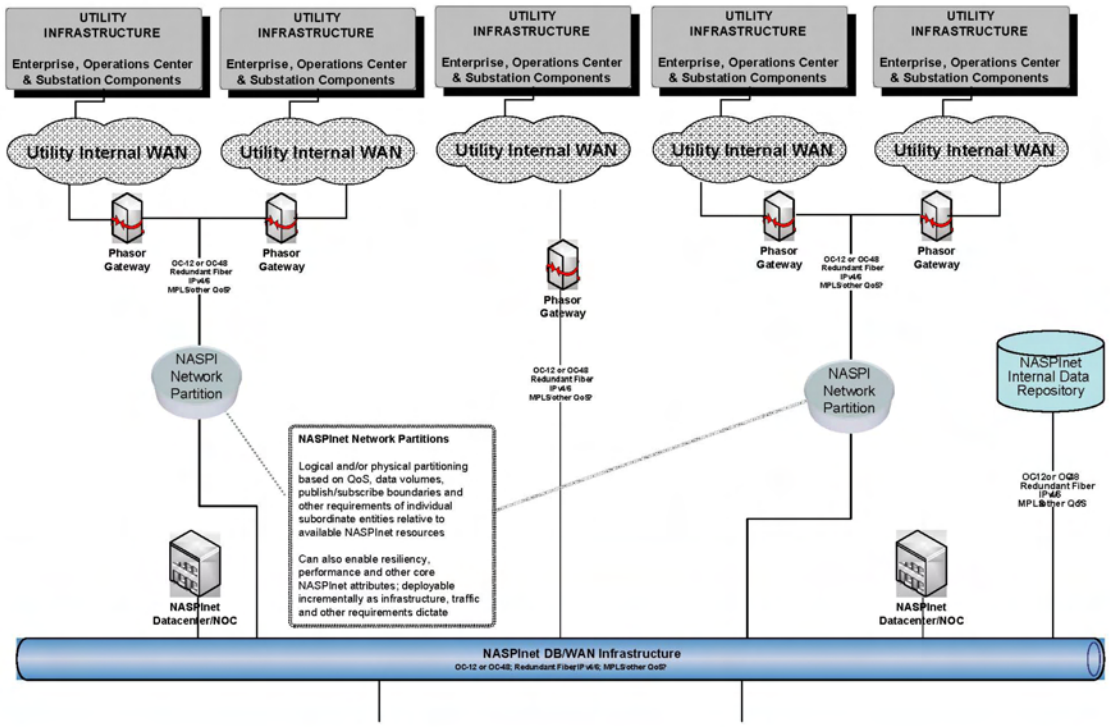
- Utility Enterprise – Data in the Utility will include but is not limited to: Phasor measurements and other Phasor information, and supporting data.
- NASPInet Internal – Data internal to NASPInet will include Directory and Naming constructs, Security credentials, auditing information, QoS history, and other supporting data.
- Historical External – Historical data may be stored outside of the primary NASPInet infrastructure, and may include raw data as well as derived, transformed or aggregated data. NASPInet entities request historical data assuming compliance with Security and other constraints.

2.10 Network View

2.10.1 Introduction

The intent of this view (Figure 2-11) is to describe at a high level potential Network deployment within the envisioned NASPInet architecture. The following assumptions apply to the Network View and diagrams:

- Network logical and physical partitioning shall be used to aggregate and separate NASPInet entities in order to optimize bandwidth and other network resources relative to evolving requirements.
- The network shall impose its own mechanisms for QoS, security and other attributes, which may complement or enable similar attributes for higher level components such as middleware, integration and application constructs.


UTILITY INFRASTRUCTURE
Enterprise, Operations Center & Substation Components
UTILITY INFRASTRUCTURE
Enterprise, Operations Center & Substation Components
UTILITY INFRASTRUCTURE
Enterprise, Operations Center & Substation Components
UTILITY INFRASTRUCTURE
Enterprise, Operations Center & Substation Components
UTILITY INFRASTRUCTURE
Enterprise, Operations Center & Substation Components
Utility Internal WAN
Utility Internal WAN
Utility Internal WAN
Utility Internal WAN
Utility Internal WAN
Phasor Gateway
OC-12 or OC48 Redundant Fiber IPv4/6 MPLS/other QoS?
Phasor Gateway
Phasor Gateway
Phasor Gateway
OC-12 or OC48 Redundant Fiber IPv4/6 MPLS/other QoS?
Phasor Gateway
NASPI Network Partition
OC-12 or OC48 Redundant Fiber IPv4/6 MPLS/other QoS?
NASPI Network Partition
NASPInet Internal Data Repository
OC12or OC48 Redundant Fiber IPv4/6 MPLS/other QoS
NASPInet Datacenter/NOC
NASPInet Datacenter/NOC
NASPInet DB/WAN Infrastructure
OC-12 or OC48; Redundant Fiber IPv4/6; MPLS/other QoS?

NASPInet Network Partitions

Logical and/or physical partitioning based on QoS, data volumes, publish/subscribe boundaries and other requirements of individual subordinate entities relative to available NASPInet resources

Can also enable resiliency, performance and other core NASPInet attributes; deployable incrementally as infrastructure, traffic and other requirements dictate

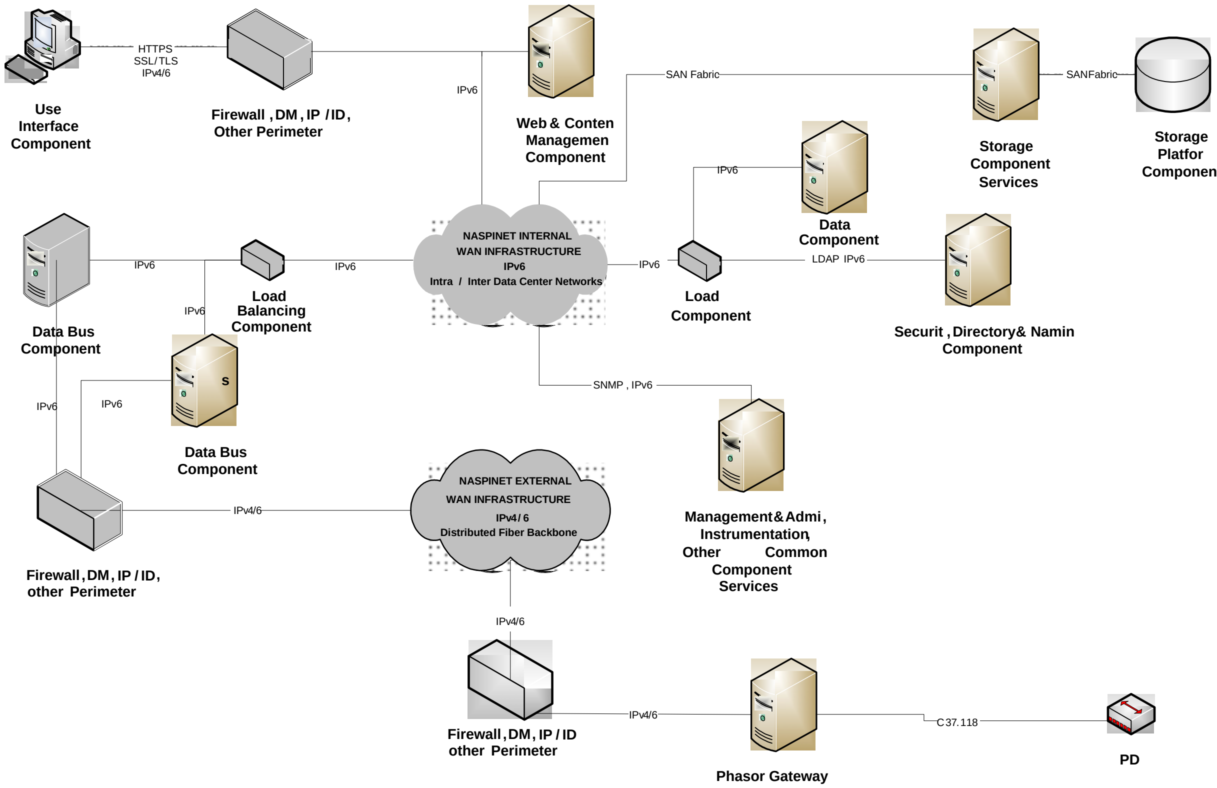
Figure 2-11: NASPInet Architecture – Network View

2.11 Deployment View

2.11.1 Introduction

The intent of this view (Figure 12) is to provide a high level example of how the NASPInet architecture could be instantiated physically for deployment. There are obviously myriad options for deploying a given technical architecture, and the optimal choice for NASPInet will depend on design recommended and proven for the PG_SUPPLIER proposed solution. The diagram below merely illustrates one possible alternative. The following assumptions apply to the Deployment View:

- NASPInet architecture does not mandate the use of virtualization, multiple instances of components, grid-based deployments or other deployment options; rather, the architecture should allow for a deployment design that is logically and physically partition-able in order to provide the widest range of deployment options.
- The NASPInet deployment architecture shall allow for logical and physical partitioning to achieve requirements for performance, fault tolerance and other functional and non-functional attributes.



HTTPS
SSL/TLS
IPv4/6
Use Interface Component
Firewall , DM , IP / ID , Other Perimeter
IPv6
Web & Conten Managemen Component
SAN Fabric
Storage Component Services
SANFabric
Storage Platfor Component
IPv6
Data Component
Data Bus Component
IPv6
Load Balancing Component
IPv6
NASPINET INTERNAL WAN INFRASTRUCTURE IPv6 Intra / Inter Data Center Networks
IPv6
Load Component
LDAP IPv6
Securit , Directory& Namin Component
IPv6
S
Data Bus Component
IPv6
IPv6
SNMP , IPv6
Management& Admi , Instrumentation, Other Common Component Services
Firewall , DM , IP / ID , other Perimeter
IPv4/6
NASPINET EXTERNAL WAN INFRASTRUCTURE IPv4/ 6 Distributed Fiber Backbone
IPv4/6
Firewall , DM , IP / ID other Perimeter
IPv4/6
Phasor Gateway
C37.118
PD

Figure 2-12: NASPInet Deployment Architecture - EXAMPLE

3 Overall NASPInet Functional Requirements

This section describes the major functions of NASPInet as a whole, including those to be performed by the Phasor Gateway (PG) and the Data Bus (DB) of NASPInet. The functional requirements in this section describes what functions that the overall NASPInet system is expected to perform, not how the function will be designed and implemented. The PG_SUPPLIERs and DB_SUPPLIER are encouraged to propose their designs that satisfy the functional requirements while making the best use of their standard offerings and commercial off-the-shelf products.

The NASPInet functional requirements are covered in this section in the following logical progression:

- **NASPInet General Functional Requirements**: This subsection provides, at the system level, the general functional requirements of NASPInet.
- **NASPInet System Administration Functions**: This subsection describes the main system administration functions of NASPInet to provide information for the PG_SUPPLIER to understand the subsequent PG Functional Requirements related to the NASPInet system administration functions.
- **NASPInet Operational Functions**: This subsection describes the main operational functions of NASPInet to provide information for the PG_SUPPLIER to understand the subsequent PG Functional Requirements related to the NASPInet operation functions.

3.1 NASPInet General Functional Requirements

As a system, NASPInet shall provide secure and QoS guaranteed data exchange services for various types of data and control signals (See Data Service Classes below). Specifically, NASPInet shall provide the following data exchange service capabilities.

SYS-1. NASPInet shall provide a publish/subscribe based mechanism for its data exchange services. The mechanism shall enable a publisher (a publishing PG) to control the subscription to its data on a per-subscriber and per-signal basis. This means that the publisher shall be able to control the subscription to its published data at the signal granularity level for each subscriber (subscribing PG). This also means that non-subscribers shall be prevented from receiving the published data and/or decoding the data without a valid subscription.

SYS-2. NASPInet shall support publishing and subscription of both real-time streaming data and historical data available through one of the connected PGs . The publish/subscribe mechanism of real-time streaming data shall support both one-to-one and one-to-many publishing-to-subscription scenarios. The real-time streaming data exchange shall support, as a minimum, IEEE

C37.118-2005 synchro-phasor data exchange protocol for data coming into and leaving the NASPInet.

SYS-3. NASPInet shall provide a Name & Directory Service (NDS) to support the publish/subscribe mechanism. The NDS shall guarantee the unique identification of any publishing device and published signal across the entire NASPInet by using a 128-bit device ID and/or signal ID. The NDS shall provide secure means for NASPInet publishers to manage the registrations of their publishing devices, and for subscribers to obtain information of published data that are registered with the NDS and to manage their subscriptions.

SYS-4. NASPInet shall support the simultaneous data exchange of multiple subscriptions with different data service classes; each has its own QoS requirements. NASPInet shall guarantee the data exchange of each subscription meeting its QoS requirements under normal operating conditions while facilitating the data exchange of multiple subscriptions with different data service classes through network traffic management.

SYS-5. NASPInet shall monitor the QoS conformance of exchanged data to detect and report any non-conformance.

SYS-6. NASPInet shall be able to tolerate certain levels of system degradation, such as a single component failure, and shall provide emergency traffic management mechanism to sustain the best level of data exchange under degraded system conditions.

SYS-7. NASPInet shall ensure that access to its resources, such as PGs and DB components/services, are highly secure, both physically and in cyber space. The security of NASPInet shall meet corresponding NERC CIP, FIPS, and other relevant cyber security standards/guidelines.

SYS-8. NASPInet shall be flexible and expandable to support a gradual system expansion in a phased implementation approach.

SYS-9. NASPInet shall be based on open standards to the extent possible.

3.1.1 Data Service Classes

SYS-10. To support varying end-user application requirements with different data needs, NASPInet shall support, as a minimum, five (5) classes of synchro-phasor data services as identified below. Suitable service requirements shall be provided within the NASPInet to support the varying functional and performance requirements for each data class.

- **CLASS A:** This data service class supports the needs of high performance feedback control applications. This class is characterized by very low latency and a fast data rate (e.g., 60 messages per second). Class A data shall be transmitted and received as quickly as possible with a high level of data availability (i.e., there shall be minimum data gaps).

- **CLASS B:** This service class supports the needs of feed-forward control applications, such as state estimator enhancement. The latency requirement for Class B data is less strict than that for Class A data. High availability of the data is also required.
- **CLASS C:** This class of data supports view-only applications (i.e. visualization) by power system operators. The tolerance for accuracy and latency for Class C data are less stringent than Class B data. The system shall enable end-user applications to retrieve data from many PMUs across a wide geographic area.
- **CLASS D:** Class D service class supports the needs of post-mortem event analysis and other off-line studies. The system shall provide a high degree of data completeness and accuracy for this service class. However, latency of Class D data may be higher than Classes A, B and C data since analysis of Class D data will generally conducted off-line (hours or days later) with archived data, as opposed to an online real-time data stream.
- **CLASS E:** Class E data primarily supports the needs for testing and Research and Development (R&D) applications. There are no guarantees on any attributes of this data class. Class E shall be given the lowest priority of all NASPInet data traffic.

SYS-11. It is highly desirable that NASPInet is designed and implemented in an architecture framework that would provide for additional synchro-phasor data service classes in the future.

SYS-12. It is also highly desirable that NASPInet is designed and implemented in an architecture framework that would support non-synchro-phasor data exchange and non-synchro-phasor data service classes in the future, such as fault record data, non-electrical data (weather forecast data, video streams, etc.) through its publish/subscribe mechanism.

The attributes for each of the five data service classes identified above are summarized in Table 3-1 below. The QoS requirements for each data service class of NASPInet are specified in Section 8.

Table 3-1: NASPInet Traffic Attributes

NASPInet Traffic Attribute	Real-time streaming data			Historical data	
	CLASS A <u>Feedback Control</u>	CLASS B <u>Feed-forward Control</u>	CLASS C <u>Visualization</u>	CLASS D <u>Post Event</u>	CLASS E <u>Research</u>
Low Latency	4	3	2	1	1
Availability	4	2	1	3	1
Accuracy	4	2	1	4	1
Time Alignment	4	4	2	1	1
High message rate	4	2	2	4	1
Path Redundancy	4	4	2	1	1

Table key:
4 – Critically important, 3 – Important, 2 – Somewhat important, 1 – Not very important

3.1.2 Real-time Streaming Data and Historical Data

The five classes of data services for synchro-phasor data identified above can be grouped into two major categories: real-time streaming data and historical data. Real-time streaming data are used for real-time control and visualization applications, such as closed-loop voltage control, feed-forward remedial action control, and system stress display and visualization applications. Historical data is typically used for non-real-time applications, such as post-disturbance analysis and off-line studies.

Synchro-phasor measurement devices (e.g., PMUs) generate accurate time-tagged phasor measurement data as continuous real-time data streams. Phasor measurements are taken at pre-defined intervals with each measurement moment precisely synchronized to the UTC with a precision of < 1 u-second. The synchro-phasor data taken at each measurement moment typically is packaged into a data frame, such as IEEE C37.118-2005 data frame protocol; and the data frames are sent to applications/users as a steady data stream. The real-time streaming data from one or more measurement devices may be aggregated/disaggregated, time-aligned, and/or processed (e.g., down-sampling) by various intermediate devices, such as Phasor Data Concentrators (PDC), and then redistributed as different real-time data streams to end-users and applications. The real-time stream phasor data may also be stored and archived outside of NASPInet and become historical data for later retrieval via NASPInet.

The class A, B, and C data services of NASPInet are real-time streaming data services. The class D and E data services of NASPInet are historical data services. NASPInet shall limit the historical data that can be subscribed to data sources available via publishing PGs.

SYS-13. NASPInet shall support the real-time streaming data exchange on real-time basis, which typically must meet very strict QoS requirements for each class of the real-time streaming data. The real-time streaming data shall, as a minimum, be able to be delivered on a frame-by-frame basis.

SYS-14. The real-time streaming data may be subscribed in both one-publisher-to-one-subscriber and one-publisher-to-many-subscriber scenarios. NASPInet shall be able to deliver real-time streaming data in both scenarios.

SYS-15. NASPInet shall employ suitable techniques (e.g. IP multicasting) to optimize the communication network bandwidth usage in a one-publisher-to-many-subscriber scenario.

SYS-16. Historical data shall be delivered through NASPInet only on a one-publisher-to-one-subscriber basis. NASPInet shall deliver the historical data to subscribers as a self-sufficient data file including appropriate configuration information of the data (measurement devices, measured items, time period, data points, data format, etc.). NASPInet shall transport the historical data in a format that can be output by the data source as is – i.e., it will be up to the requesting application to transform and load the data.

3.1.3 Publish/Subscribe Mechanism

The publish/subscribe mechanism of NASPInet shall consist of three parts: device/signal registration by publishers, subscription setup between publisher and subscriber initiated by subscribers, and QoS and information assurance (data confidentiality and integrity through security measures) of the subscribed data. Publishers, i.e. publishing PGs, of the data generally would only register the data that they are willing to publish, and would not actively advertise the availability of their published data. NASPInet shall provide the following for supporting this publish/subscribe mechanism.

SYS-17. NASPInet shall limit data browsing capability to authorized subscribing PGs to minimize the risk of unauthorized access of the published data. Subscribers will be required to initiate the process of setting up a subscription by discovering available published data that they are allowed to access through data discovery requests, selecting the data to subscribe, and making the formal subscription requests for the selected data.

SYS-18. Publishers shall respond to subscribers' data discovery requests and subscription requests by granting access rights to part or all of their published data based on the authenticated identities of the subscribers.

SYS-19. NASPInet shall provide a Name & Directory Service (NDS) for its publish/subscribe mechanism, uniquely identifying each and every registered signal across the entire NASPInet. The NASPInet NDS shall also support PG registration and PG discovery for all PGs connected to the NASPInet DB. The NASPInet NDS shall be provided through DB NDS and PG device management functionality.

SYS-20. The NASPInet NDS shall enable publishers to register devices/applications and the associated signals for data publishing before their data can be published to NASPInet.

SYS-21. The NASPInet NDS shall enable subscribers to discover any accessible data that they could select and subscribe to.

SYS-22. NASPInet shall provide means for setting up subscriptions between a publisher and a subscriber for its publish/subscribe mechanism. The means shall include accessible signal discovery, subscription request, and subscription setup mechanisms.

SYS-23. The NASPInet publish/subscribe mechanism shall provide means for QoS and information assurance . Delivery of subscribed data shall meet the QoS requirements of the corresponding data classes.

SYS-24. The information assurance shall ensure the information confidentiality and integrity of the delivered data. NASPInet shall be designed to prevent published data to be received and understood by non-subscribers to maintain the data confidentiality between publisher and subscriber.

SYS-25. Information integrity assurance measures shall be implemented for detecting and reporting any tampering and degradation of the exchanged data.

3.1.4 Name & Directory Service

NASPInet shall provide a Name & Directory Service (NDS) to meet the following requirements.

SYS-26. NDS shall enable the system-wide registry of Phasor Gateways, Phasor Measurement Units, Phasor Data Concentrators, and IED devices and their associated signals as well as the services, components, processes and other entities required by the Phasor Gateway and/or Data Bus components.

SYS-27. NDS shall enable unique identification of any registered signal across the entire NASPInet on an individual signal basis.

SYS-28. NDS shall enable discovery of accessible device/application/signal.

SYS-29. NDS shall allow the concurrent use of different naming conventions.

SYS-30. NDS shall provide basis for resource management, subscription management, and traffic management.

SYS-31. NDS shall be based on metadata storage and retrieval systems to provide flexible and expandable metadata storage and retrieval capabilities. The number of fields and the size of each field of a metadata record, and the total storage capacity shall all be adjustable and expandable.

SYS-32. NDS shall provide unique IDs for each and every registered item. The IDs shall be a 128-bit random number.

SYS-33. NDS shall work in concert with NASPInet Security Service and PG Security Component to enable registered PGs to discover accessible signals by sending request to DB. NDS shall authenticate requesting PG’s identity, granting access rights by source data owners, and provide accessible signal information to requesting PGs.

SYS-34. NDS shall not provide general browsing of all registered signals to minimize the risk of unauthorized access to registered signals, regardless whether the request is from registered PGs or unknown/unauthorized devices/applications.

SYS-35. NDS naming convention may include PG-OWNER's existing naming convention, NASPInet global naming convention (to be developed), and other naming conventions.

3.1.5 QoS Assurance

SYS-36. NASPInet shall implement QoS assurance based on the NASPInet resource management mechanism. The NASPInet resource management mechanism shall include resource condition monitoring, resource usage monitoring, QoS performance monitoring, QoS provisioning, and traffic management. NASPInet resources include PGs, DB components/services, and NASPInet data network components.

SYS-37. NASPInet resource condition monitoring shall provide both real-time and historical resource condition information for each resource, including logging, reporting and alarming. NASPInet resource condition monitoring shall be able to detect and report any failure and out-of-service conditions for any of its resources.

SYS-38. NASPInet resource usage monitoring shall provide both real-time and historical resource usage information on each resource through resource usage tracking, logging, reporting and alarming. The resource usage tracking shall include all resources that are involved in the data delivery chain from data entering NASPInet to data leaving NASPInet.

SYS-39. The resource usage information tracked, logged and reported shall include but not limited to detailed loading information (instant, peak, and average) of each resource for each class of the data services.

SYS-40. The NASPInet resource usage monitoring shall allow setting of alarm thresholds and generate alarms whenever tracked usage exceeds the threshold(s).

SYS-41. NASPInet QoS performance monitoring shall enable end-to-end QoS performance monitoring on a per subscription basis. NASPInet QoS performance monitoring shall provide both real-time and historical QoS information on a per subscription basis through measurement, logging, reporting and alarming.

SYS-42. NASPInet shall also provide statistical QoS information of the entire NASPInet using the logged per-subscription QoS information. The QoS information to be measured and logged shall include but not limited to latency (maximum and average), successful delivery rate, etc..

SYS-43. NASPInet shall provide accurate timing references for measuring the delivery latency for each subscription. NASPInet QoS performance monitoring shall also include the QoS performance monitoring of incoming data from registered publishing PGs.

SYS-44. NASPInet shall provide a QoS provisioning mechanism during the new subscription setup process. The QoS provisioning mechanism shall enable NASPInet to determine, once setup, if the QoS requirements of the new subscription could be satisfied based on the resource status, resource usage, and QoS performance of existing subscriptions and external publishing sources.

SYS-45. NASPInet shall provide a traffic management mechanism for QoS assurance under both normal and abnormal system conditions based on the traffic prioritization of different data service classes. NASPInet shall support data delivery based on the priority traffic levels, i.e. higher priority traffic shall always be delivered/processed before lower priority ones.

SYS-46. NASPInet shall provide means for setting the desired priorities of different types of traffic, such as the priorities for different class of data services, subscription requests/responses messages, network management traffic, control signals, etc..

SYS-47. The traffic management shall also provide means for setting traffic management policies of NASPInet for dealing with various normal and abnormal system conditions. The NASPInet shall be able to control the traffic based on the traffic management policies, resource availability, resource usage levels, and actual QoS performance measurement.

3.1.6 Security and System Resiliency

SYS-48. NASPInet shall implement a comprehensive cyber security framework to safeguard the reliable operation and the data exchange of NASPInet. The NASPInet security framework shall include secure mechanisms for identification and authentication, access control, information assurance, and security monitoring and auditing.

SYS-49. The NASPInet secure identification and authentication mechanism shall enable NASPInet to securely authorize, assign, and authenticate each and every device/equipment connected to the NASPInet and communicate through the NASPInet. The NASPInet secure identification and authentication mechanism shall enable NASPInet to securely authorize, assign, and authenticate each user who has access to NASPInet's resources.

SYS-50. The NASPInet access control mechanism shall enable NASPInet to set and enforce proper levels of access privileges and rights for each and every device/equipment connected to the NASPInet on an individual device/equipment basis. The NASPInet access control mechanism shall also enable NASPInet to set and enforce proper levels of access privileges and rights for each user of the NASPInet on an individual user basis. The objective of NASPInet access control is to ensure that only authorized and trusted users and device/equipment could gain access to the NASPInet PGs and DB components to utilize the NASPInet resources at a level that they are authorized to.

SYS-51. The NASPInet information assurance function shall enable NASPInet to guarantee the confidentiality and integrity of the data exchanged through NASPInet, which shall include secure subscription setup, subscription based data and control flow security, key management, and information integrity assurance. These functions serve two main objectives: keep data and control flows from any unauthorized access and at the same time ensure that data and control flows have not been tempered with or degraded when traveling through the NASPInet.

SYS-52. All data traffic going through NASPInet, including administrative traffic, data/control flow, network management data, etc., shall be actively monitored, logged, analyzed and audited. Any anomaly shall be reported, traced and analyzed to determine whether it is the results of NASPInet own degradations/failures or intentional/unintentional intrusion attempts by unauthorized entities (hackers, intruders, unauthorized equipment connection, unauthorized user logins, etc.).

SYS-53. NASPInet shall generate regular security audit reports in compliance with NERC CIP reporting requirement.

SYS-54. NASPInet shall ensure a secure and reliable end-to-end data exchange for every subscription of the data.

SYS-55. NASPInet shall be resilient to external intrusions and system failures.

SYS-56. More specifically, NASPInet shall, as a minimum, implement a cryptographic key generation and management mechanism for real-time streaming data and historical data publishing and subscriptions, and implement PKI for all other message exchange communications among PGs, between PGs and DB, and within DB.

SYS-57. NASPInet's subscription cryptographic key generation and management mechanism shall ensure that all active subscriptions of real-time streaming data and historical data have no duplicated keys.

SYS-58. NASPInet's cryptographic key generation and management mechanism shall support dynamic key generation and distribution for real-time streaming data publishing and subscriptions.

3.1.7 Logging and Audit Trail

SYS-59. For auditing purposes, NASPInet shall log all user activities (e.g. access requests and the outcome of each request), system administration activities (e.g. data source registration and connection, PG's DB access requests and outcome), data subscription related activities (e.g. subscription requests and outcome), QoS alerts, cyber security alerts, application errors, etc.. Each record shall be time stamped and securely stored.

SYS-60. The PG shall allow the PG administrator to generate reports from the log, or export data from the log to a common data format such as Excel.

SYS-61. The DB components shall allow their administrators to generate reports from the log, or export data from the log to a common data format such as Excel.

SYS-62. The NASPInet shall maintain accurate audit trails of all NASPInet activities, such as user activities, system administration activities, and data subscription and delivery activities.

3.1.8 Flexibility and Expandability

SYS-63. The design and implementation of NASPInet shall provide the flexibility and expandability needed to support incremental deployment of the NASPInet.

SYS-64. The design and implementation of DB shall allow it to gradually increase the capacities of its various components and services to support the gradually increased number of PGs connected to it, the publishing devices (e.g. PMUs, PDCs) connected to publishing PGs, and the subscribing devices/applications connected to subscribing PGs.

SYS-65. The design and implementation of PG shall facilitate customization and configuration to support different data publishing and subscription capabilities of each PG.

SYS-66. The design and implementation of PG shall allow expansion from initial limited data publishing and subscription capabilities to the full capabilities described in these specifications.

SYS-67. The design and implementation of PG shall enable the increase of the processing capacity for each class of data that it supports when needed.

SYS-68. The NASPInet WAN design and implementation shall also support incremental growth in the deployment process of the NASPInet.

3.1.9 Common Services

SYS-69. The DB and the PG shall utilize, shall be compatible with, and shall integrate within the Common Services of the enterprise IT infrastructures of the respective Requester, where available and applicable. Contrasting some of these services with equivalent services within the context of the DB and PG, such as System Management and Administration, the Common Services shall perform similar functions but on a broader scale throughout the Requester’s enterprise IT environment and shall integrate with it.

SYS-70. The Common Services shall include the logical components outlined below. These services may be grouped in a different set of product modules based on the commercial products used by the Requester for these services.

SYS-71. Security – this service shall provide enabling services and infrastructure to ensure the appropriate access to and usage of NASPInet resources and information. Key components typically include Authentication, Authorization, Access Control, Confidentiality, Auditing, Non-Repudiation and many others. Please see Section 7, Security Requirements, for details.

SYS-72. Management & Administration – this service shall enable the initial configuration and ongoing operation of NASPInet components and services, and will likely integrate or aggregate the analogous but more focused services within the Data Bus.

SYS-73. Name & Directory – this service shall enable the system-wide registry of Phasor Gateways, Phasor Measurement Units, and IED devices as well as the services, components, processes and other entities required by the Phasor Gateway and/or Data Bus components.

SYS-74. Resiliency – This service and infrastructure shall ensure critical system attributes such as Fault Tolerance, Availability, Disaster Recovery, Business Continuity and similar aspects.

SYS-75. Instrumentation – In concert with DB Management and Administration Services, this service shall provide visibility into key aspects of the NASPInet infrastructure, such as performance, utilization and general health indicators, for the DB network, hardware and software subsystems of DB and PG.

SYS-76. Data Management – this service shall enable the logical and physical architecture, storage, access and management of persistent and transient data within NASPInet. Key components typically include Relational Database Management engines, Storage Area Network infrastructure, Metadata Management, Hierarchical Storage Management, Information Lifecycle Management and other services.

3.2 NASPInet System Administration Functions

NASPInet shall include facilities that enable the PG administrators and DB administrators to perform system administration functions, such as registering a PG with the DB. As a minimum, the system shall provide the key System Administration functions that are described in the following subsections.

3.2.1 Register a PG with DB

SYS-77. The system shall include a function to enable the PG administrator to register a PG with the DB's NDS. PGs must be registered with the DB NDS before being allowed to publish or subscribe data on the DB and NASPInet. Attempts by an unregistered PG to publish and subscribe data on the DB of NASPInet shall be rejected by the DB of NASPInet. The DB shall generate an alarm message to alert the DB administrator to this occurrence.

SYS-78. After a PG has been installed and tested to function properly at an entity's facility for interacting with entity's own real-time streaming data devices/systems (PMUs, PDCs, etc.), historical data store, and/or applications, the PG shall be registered with NASPInet. The PG shall include a suitable function to assist the user in registering the new PG.

SYS-79. Only the PG administrator shall be allowed to register a PG with NASPInet. The PG shall prevent other users of the PG from accessing the PG registration process.

SYS-80. Following successful completion of the PG registration process, the PG shall receive a unique 128-bit PG identifier from the NASPInet administrator indicating that the PG has been registered in the DB NDS. The PG ID obtained via this process shall be required for all other system administration and operational functions to identify and authenticate a specific PG.

SYS-81. The PG ID supplied by NASPInet shall be encrypted to guard against any tempering and misuse.

SYS-82. Once a PG has been successfully registered with NASPInet, all streaming and historical data source devices/systems connected and registered with the PG shall also be registered with the NASPInet DB NDS before the PG can publish any data from these devices/systems to NASPInet.

SYS-83. After successful registration of a PG, the applications running on the PG owner's own network and PG administrator shall be able to inquire, subscribe and access available streaming and historical data from other PGs that are already registered with the NASPInet through the PG registration process.

SYS-84. A PG requesting registration shall also obtain the method from DB to authenticate identities of DB components and any messages that it receives from NASPInet DB.

SYS-85. A PG could have varied degrees of capabilities in terms of published/subscribed data classes, such as QoS requirements and support. A PG registered with NASPInet shall indicate its capabilities in terms of published/subscribed data classes.

SYS-86. The PG Registration function shall specify the PG throughput information for each class of published/subscribed data that the PG supports.

SYS-87. A PG's Registration shall provide information that is needed for other PG owners to identify the PG's owner and the PG capabilities. As a minimum, the information shall include:

- Owner information
- Location information
- PG capabilities information (e.g. classes of data services supported)

3.2.2 Update PG Registration with DB

SYS-88. The PG administrator shall be able to update the registration of a PG that has previously been registered to accurately inform NASPInet about changes in the functionalities and capabilities of the PG. For example, it shall be possible to change an existing publishing Class C data only PG to a publishing Class B and C data PG.

SYS-89. Only the PG administrator shall be permitted to update a PG's registration with NASPInet. The PG shall reject all attempts by persons other than the PG administrator to update the PG's registration.

SYS-90. The PG shall include a user interface function that shall enable the PG administrator to enter the updated registration information and send the requested changes to NASPInet. The PG administrator shall be validated locally by PG's security management logic (see Section 7 of the PG Technical Specifications).

SYS-91. The PG shall perform extensive validity checks of the inputs to ensure that the updated information is accurate and reasonable. The PG shall detect validity check failures and notify any errors to the PG administrator and allow the PG administrator to correct these errors. No registration update data shall be sent to the DB prior to successfully completing the validity checks.

SYS-92. After successful validation of the registration information, the PG shall send a registration update request message to the DB's NDS with the updated information.

SYS-93. If no errors are detected by the DB in the updated information, the PG shall receive a message from the DB indicating that the PG's registration with NASPInet has been successfully updated.

SYS-94. After the PG's registration with NASPInet has been successfully updated, the PG shall begin publishing data to NASPInet and/or subscribing data from NASPInet in accordance with the updated registration.

SYS-95. Data exchange of existing subscriptions shall be automatically stopped and resumed as needed during the PG registration update process.

SYS-96. The PG and DB shall ensure that all subscriptions to discontinued data services be terminated in an orderly way prior to updating the DB registration.

3.2.3 Remove a PG from DB

SYS-97. The PG shall include a function to enable the PG Administrator to remove a registered PG from NASPInet at any time.

SYS-98. The PG administrator shall be validated locally by PG's security management logic. Only the PG Administrator shall be allowed to remove a PG's registration with NASPInet; no other PG users shall have any access to the PG registration removal process.

SYS-99. The PG shall send a removal request message to the DB. Following successful authentication by the DB, the PG shall be prompted to confirm its intention for PG removal. If confirmation of the request for PG removal is not received within a user specified time period, the request shall be cancelled.

SYS-100. Following confirmation of its intention for PG removal by the requesting PG, the DB shall attempt to remove the registration. If the PG registration cannot be removed, the DB shall log and inform the PG of the reason for unsuccessful registration removal.

SYS-101. After the PG's registration with NASPInet is removed, the PG shall no longer be able to publish streaming and historical data to NASPInet and the PG shall no longer be able to subscribe to and receive data from streaming and historical data sources of other registered PGs on NASPInet.

SYS-102. The DB shall ensure that all subscriptions related to the removed PG be terminated in an orderly way in the PG removal process.

3.2.4 Register a Real-Time Streaming Data Source (RT-SDS)

SYS-103. All real-time streaming data sources (RT-SDS) that will serve as a streaming data source through the NASPInet must be connected to and registered with a PG that is registered with NASPInet.

SYS-104. All real-time streaming data sources shall be registered with the NASPInet through the data source owner's PG before the data source can publish data to NASPInet through the PG.

SYS-105. The PG shall not publish any data from an unregistered RT-SDS device/system to NASPInet.

SYS-106. Prior to registering the data source, the data source owner shall verify that the data source is operating and communicating successfully with the PG. The PG shall include suitable communication/test facilities to verify that each data source is installed, operating, and communicating properly with the PG.

SYS-107. To enable a registered RT-SDS device/system and its signals to be queried and accessed by NASPInet subscribing PGs, the registering PG shall provide all required information to NASPInet DB, including the following as a minimum:

- Physical location of the device (Country, State, Geo-coordinates, etc.)
- Location identification (substation name, building name, etc.)
- Type of device (PMU, PDC, etc.)
- Device identification (device name, sequence number, etc.)
- Device configuration (physical & logical)
- Complete signal description (type of signal, reporting rate, data format, etc.)
- Signal origin (e.g., original PMU signal that a PDC signal is derived from)
- Signal source (measurement CT/PT, source devices, etc.)
- Signal processing methods (if not original signal)
- Signal quality (data class – latency, reliability, etc.)

- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Ownership (entity name)
- Names according to PG owner naming convention
- Names according to NASPInet naming convention

SYS-108. It shall be possible to register an individual RT-SDS or small number of RT-SDSs interactively using the PG user interface.

SYS-109. The PG shall also include a convenient mechanism for registering a large number of RT-SDS devices/systems that frequently register/remove themselves with/from the NASPInet on a regular basis.

Human intervention to manage the timely registration and removal process of such RT-SDS devices/systems may be impractical. Requirements for interactive registration and automatic registration of a large number of RT-SDSs are described in the following subsections.

3.2.4.1 Interactive Registration

SYS-110. The PG shall include a function to allow interactively registering the RT-SDS with NASPInet. This function shall include display screens with data entry fields for entering information about the RT-SDS, such as device/system type, available signals, and other pertinent information about the RT-SDS.

SYS-111. The PG shall perform extensive error checking on the entered data shall inform the user if erroneous, invalid, or inconsistent data is entered. This function shall prevent erroneous, invalid, or inconsistent data from being submitted to NASPInet.

SYS-112. After the data errors have been corrected by the user, the registered PG shall send a RT-SDS Registration Request message to the DB with the pertinent RT-SDS information.

SYS-113. After authentication of PG and data source and validation of the data, DB shall send unique signal IDs (128-bit) and a RT-SDS device ID (128-bit) to the requesting PG along with a registration complete message. The requesting PG shall store the unique signal ID received from DB and acknowledge receipt of this information.

SYS-114. After successful completion of the interactive registration process, the PG shall be able to publish data from the registered RT-SDS device/system to other subscribing PGs registered with the NASPInet.

3.2.4.2 Automatic Registration

SYS-115. An alternative registration process that does not require PG administrator involvement shall be provided for RT-SDS devices that have been entered into the DB's NDS database via a registered PG, either through previous registration or other secure method. RT-SDS devices that satisfy this requirement shall receive secure unique IDs from NASPInet that shall be used to facilitate the automatic RT-SDS registration process.

SYS-116. The PG shall support automated registration of a RT-SDS device/system through the PG without PG administrator’s involvement. After a successful automated RT-SDS device/system registration with the PG, the PG shall automatically send a “RT-SDS registration request” message to DB’s NDS with the RT-SDS device/system’s information to DB’s NDS.

SYS-117. If no errors are detected by the DB in the registered RT-SDS device/system’s information, the PG will receive unique signal IDs for all signals of the registering RT-SDS device/system, along with a “RT-SDS registration complete” message.

SYS-118. The PG shall acknowledge the receipt of the confirmation and shall store the signal IDs to complete the registration process.

SYS-119. After successful completion of the automatic registration process, the PG shall be able to publish data from the registered RT-SDS device/system to other subscribing PGs registered with the NASPInet.

SYS-120. In the event that the RT-SDS registration process is unsuccessful for any reason or the PG does not receive assigned signal IDs or RT-SDS registration complete message from the DB within a user specified time period, the PG shall log the RT-SDS incomplete registration request process in its application error log.

3.2.5 Update a Real-Time Streaming Data Source

SYS-121. The PG shall include an administration function to change the configuration of an existing registered RT-SDS device or system that is currently publishing streaming data to the NASPInet. For example, it shall be possible to update the registration of a Phasor Data Concentrator (PDC) when PMUs are added or removed from the PDC, resulting in the PDC supplying more or fewer signals to the NASPInet.

SYS-122. The PG shall support interactive updates and automatic updates, as described in the following sections.

SYS-123. Updating RT-SDS registration with PG and DB shall ensure that all subscriptions related to the RT-SDS will be terminated in an orderly way prior to the start of the RT-SDS updating process.

3.2.5.1 Interactive Updates

SYS-124. The PG shall include a function to allow interactively updating of the existing registered RT-SDS with NASPInet. This function shall include display screens with data entry fields to enable the PG Administrator to enter the information needed to update the registration of the RT-SDS. This includes device/system type, available signals, and other pertinent information about the RT-SDS. The PG shall perform extensive error checking on the entered data and shall inform the user if erroneous, invalid, or inconsistent data is entered so that the data can be corrected. This function shall prevent erroneous, invalid, or inconsistent data from being submitted to NASPInet.

SYS-125. After any data errors have been corrected by the user, the registered PG shall send an RT-SDS registration update request message to the DB's NDS with the updated RT-SDS information to be stored by the DB's NDS.

SYS-126. If the data is correct, the requesting PG shall receive unique signal IDs along with a "RT-SDS registration update complete" message. The requesting PG shall store the unique signal IDs received from DB and acknowledge receipt of this information.

SYS-127. After successful completion of the interactive registration update process, PG shall be able to publish data from the registered RT-SDS device/system that is just updated to other subscribing PGs registered with the NASPInet.

SYS-128. In the event that the RT-SDS registration update process is unsuccessful for any reason or the PG does not receive assigned signal IDs or RT-SDS registration complete message from the DB within a user specified time period, the PG shall log the RT-SDS incomplete registration update request process in its application error log. In addition, the DB administrator shall be notified about the failed RT-SDS registration request.

SYS-129. The DB shall automatically stop any active publish/subscribe data activities involving the RT-SDS before the registration update process, informing all subscribing PGs of the interruptions. After the registration is complete, the DB shall send a message to the publishing and subscribing PGs to reinitiate the publishing and subscriptions of the data.

3.2.5.2 Automatic Registration Updates

SYS-130. An alternative registration process that does not require PG administrator involvement shall be provided for RT-SDS devices that have been entered into the DB's NDS database, either through previous registration or other secure method. RT-SDS devices that satisfy this requirement will receive secure unique IDs from NASPInet that shall be used to facilitate the automatic RT-SDS registration update process.

SYS-131. The PG shall support automated registration updates for a RT-SDS device/system with the PG without PG administrator's involvement. After a successful automated RT-SDS device/system registration update with PG, the PG shall automatically send a "RT-SDS registration update request" message to DB's NDS with the RT-SDS device/system's updated information to DB's NDS.

SYS-132. If the DB's data verification and validation process is successful, the PG will receive unique signal IDs for all signals of the updated RT-SDS device/system, along with a "RT-SDS registration updated complete" message to the requesting PG.

SYS-133. The PG shall acknowledge the receipt of the confirmation and shall store the unique signal IDs to complete the registration process.

SYS-134. After successful completion of the automatic registration update process, PG shall be able to publish data from the registered RT-SDS device/system that is just updated to other subscribing PGs registered with the NASPInet

SYS-135. In the event that the RT-SDS automatic registration update process is unsuccessful for any reason or the PG does not receive assigned signal IDs or RT-SDS registration complete message from the DB within a user specified time period, the PG shall log the RT-SDS incomplete registration update request process in its application error log. In addition, the DB administrator shall be notified about the failed RT-SDS registration request.

SYS-136. The DB shall automatically stop any active publish/subscribe data activities involving the RT-SDS before the registration update process, informing all subscribing PGs of the interruptions. After the registration is complete, the DB shall send a message to the publishing and subscribing PGs for the PGs to reinitiate the publishing and subscriptions of the data.

3.2.6 Remove a Real-Time Streaming Data Source

SYS-137. The system shall allow one or more registered and communicating RT-SDS devices to be taken offline in a planned and orderly manner for various reasons, such as testing, firmware upgrade, and other maintenance activities. No real-time streaming data will be published from phasor measurement devices that are offline.

SYS-138. After the RT-SDS is taken offline, it shall be possible to disconnect the RT-SDS from the PG for performing various work activities, such as firmware update, testing, and other maintenance activities.

SYS-139. The system shall facilitate return an RT-SDS that has been taken offline from the service. If no change to its registration is needed, PG and DB shall be notified of the RT-SDS returning to service, and confirmation shall be received before it can publish data again. If change to its registration is needed, then either a normal registration process or a registration update process must be conducted before it can publish data again.

SYS-140. The system shall support interactive removal and automatic removal of RT-SDS services, as described in the following requirements.

SYS-141. Removing a RT-SDS registration or service from DB shall ensure that all subscriptions related to the RT-SDS will be terminated in an orderly way prior to the start of the RT-SDS removing process.

SYS-142. The PG shall include a user interface function that shall enable the PG administrator to remove a registered, active RT-SDS device from service, or remove its registration. Upon request from the PG administrator, the PG shall send an RT-SDS removal request message to DB's NDS to initiate and complete the RT-SDS removal process.

SYS-143. The system shall include a function to support automatic removal of a RT-SDS from service. After confirming a removal request from a RT-SDS device/system, the PG shall automatically send an RT-SDS removal request message to DB's NDS to initiate and complete the RT-SDS removal process. Registration shall not be removed automatically through this process; the PG administrator will need to use the interactive method stated above to remove the registration when needed.

3.2.7 Register a Historical Data Source (HDS)

SYS-144. The PG shall be able to acquire data from historical data sources (HDS) external to the NASPInet such as phasor data concentrators (PDCs) that have data storage capabilities. As with streaming data sources, historical data sources can publish their data to NASPInet via a PG. Any HDS that supplies data to NASPInet subscribers shall be registered through the HDS owner's PG.

SYS-145. The PG shall include a user interface function to facilitate registering an HDS with NASPInet.

SYS-146. To register with NASPInet, each HDS shall be required to meet the minimum requirements listed below. The PG shall verify that these capabilities exist before attempting to register the HDS with NASPInet.

- Each HDS shall include a mechanism to enable PGs and subscribers to query, request, and obtain the stored data for selected signals for a specific period of time.
- Each HDS shall be able to provide on demand to any authorized PG or subscriber a complete description of the types of stored data (measurement points list, sampling rates, length of storage, maximum data file size per request, etc.) that it provides and the format of this data.
- Each HDS shall be able to accept and store the unique device and signal IDs assigned by the DB for all stored synchro-phasor data points originated from RT-SDSs as part of the data storage.

SYS-147. The PG of an HDS shall be able to provide access to phasor measurements that were originally supplied by the RT-SDSs of the PG's and HDS's owning entity. The PG of the HDS shall not provide access to phasor measurements supplied by RT-SDSs of other publishing entities (P-PGs) without the permission of the owning entities of these RT-SDSs.

SYS-148. Prior to registering the HDS with NASPInet, the PG shall confirm that the HDS has been installed, operating, and communicating properly with the PG.

SYS-149. The PG shall include suitable facilities to verify that the HDS is operating and communicating properly.

SYS-150. All RT-SDS devices that supply data to the HDS shall be registered with the HDS. The HDS shall store the unique signal IDs assigned by NASPInet to signals published by the RT-SDS devices/systems to NASPInet.

SYS-151. To initiate registration of a historical data source, the PG shall send an HDS registration request message to DB's NDS with the necessary HDS information, such as RT-SDS device IDs and signal IDs for publishable data points when prompted.

SYS-152. It shall be possible to register the HDS interactively or automatically, as described in the following sections.

3.2.7.1 Interactive Registration

SYS-153. The PG shall include a function to allow the PG administrator to register the HDS using interactive display screens. The PG shall include security management logic to validate the administrator locally. Once validated by the PG's security management logic, the PG administrator shall be able to initiate an HDS registration request message to the DB's NDS.

SYS-154. Upon successful authentication by DB's NDS, the PG shall be able to enter and send the HDS registration information. The PG's registration function for HDS devices shall include display screens with suitable data entry field for inserting the necessary registration information to register the HDS and the data it can provide. Following completion of data entry, the PG administrator shall be able to send this information to the DB's NDS.

SYS-155. If data verification and validation checks performed by the DB's NDS on the PG-supplied data are not successful, the DB shall send the PG an error message and log the error in its error log.

SYS-156. If the data verification and validation checks are successful, the PG shall receive the unique device and signal IDs of registered RT-SDSs for all signals of the registering HDS device/system, along with a unique ID for the HDS and an "HDS registration complete" message.

SYS-157. The PG shall acknowledge the receipt of the confirmation message and shall store the received device and signal IDs and forward them to HDS. After successful completion of the interactive registration process, the PG shall be able to publish historical data from the registered HDS device/system to other subscribing PGs registered with the NASPInet.

3.2.7.2 Automatic Registration

SYS-158. The system shall provide an automatic registration function for HDS devices/systems that support the automatic registration. To be accepted for automatic registration, the HDS device/system must have obtained a secure unique ID through previous registration with DB's NDS database or other secure method. The PG shall be configurable to support registration of an HDS device/system with or without the PG administrator's involvement.

SYS-159. The PG shall support automated registration of HDS device/system registration with PG without PG administrator's involvement. After a successful automated HDS device/system registration with PG, the PG shall automatically send an "HDS registration request" message to DB's NDS. Upon successful authentication by the DB's NDS, the PG shall send the registered HDS device/system's information to DB's NDS.

SYS-160. If the data verification and validation checks are successful, the PG shall receive the unique device and signal IDs of registered RT-SDSs for all signals of the registering HDS device/system, along with a unique ID for the HDS and an "HDS registration complete" message.

SYS-161. PG shall acknowledge the receipt of the confirmation and shall store the received device and signal IDs and forward them to HDS to complete the registration process.

SYS-162. After successful completion of the automatic registration process, the PG shall be able to publish data from the registered HDS device/system to other subscribing PGs registered with the NASPInet.

SYS-163. In the event that the automatic HDS registration process is unsuccessful for any reason, e.g. the PG does not receive assigned device IDs or HDS registration complete message from the DB within a user specified time period, the PG and DB shall log the HDS incomplete registration request process in its application error log and notify PG and DB administrators.

3.2.8 Update an Historical Data Source

SYS-164. The PG shall include an administration function to allow the update of changes in the configuration and/or available historical data points of an existing registered HDS device or system that is currently publishing historical data to the NASPInet. For example, it shall be possible to add or delete HDS stored data points resulting in the PG supplying more or fewer historical data points to the NASPInet.

SYS-165. The PG shall support both interactive updates and automatic updates, as described in the following sections.

SYS-166. Updating HDS registration with PG and DB shall ensure that all subscriptions related to the HDS will be completed or terminated in an orderly way prior to the start of the HDS registration updating process.

3.2.8.1 Interactive Updates

SYS-167. The PG shall include a function to allow interactive update of the existing registered HDS systems and devices with NASPInet. This function shall include display screens with data entry fields to enable the PG Administrator to enter the information needed to update the registration of the HDS. This includes device/system type, available signals, and other pertinent information about the HDS. The PG shall perform extensive error checking on the entered data and shall inform the user if erroneous, invalid, or inconsistent data is entered so that the data can be corrected before submitting this data to NASPInet. This function shall prevent erroneous, invalid, or inconsistent data from being submitted to NASPInet.

SYS-168. After any data errors have been corrected by the user, the registered PG shall send an HDS registration update request message to the DB's NDS with the updated HDS information when prompted.

SYS-169. If the registration update is successful, the PG shall receive the unique device and signal IDs for new devices and signals added to the HDS along with an "HDS registration update complete" message. The requesting PG shall acknowledge the receipt of this information, and store and pass the unique device and signal IDs for new devices and signals to HDS to complete the registration update process.

SYS-170. After successful completion of the interactive registration update process, PG is ready to publish data from the registered HDS device/system that has just been updated to subscribing PGs registered with the NASPInet.

SYS-171. If the registration update is not successful, the DB shall send the PG an error message and log the error in its error log.

3.2.8.2 Automatic Registration Updates

SYS-172. The system shall provide an automatic registration update function for HDS devices that support automatic registration update. To be able to perform automatic registration update, the HDS device/system must have obtained a secure unique ID either through previous registration or other secure method. HDS devices that satisfy this requirement shall receive a secure unique ID from NASPInet that shall be used to facilitate the automatic HDS registration update process. The PG shall be configurable to support registration of an HDS device/system with or without the PG administrator's involvement.

SYS-173. The PG shall support automated registration updates for a HDS device/system with the PG without PG administrator's involvement. After a successful automated HDS device/system registration update with PG, the PG shall send the registered HDS device/system's updated information to DB's NDS.

SYS-174. Following successful verification and validation of the information sent by the PG, the DB NDS shall send device and signal IDs for all affected signals of the HDS device/system to PG and the PG shall receive a "HDS registration update complete" message.

SYS-175. The PG shall acknowledge the receipt of this information, and store and pass the unique device and signal IDs for new devices and signals to HDS to complete the registration process.

SYS-176. After successful completion of the automatic registration update process, the PG shall be able to publish data from the registered HDS device/system that has just been updated to subscribing PGs registered with the NASPInet.

SYS-177. In the event that the automatic HDS registration process is unsuccessful for any reason, the PG shall log the HDS incomplete registration request process in its application error log. In addition, the DB and PG administrator shall be notified about the failed HDS registration update request.

3.2.9 Remove an Historical Data Source

SYS-178. The system shall allow one or more registered and communicating HDS devices to be taken off-line in a planned and orderly manner for various reasons, such as testing, software upgrade, and other maintenance activities. No historical data shall be published from HDS systems/devices that are off-line.

SYS-179. After the HDS is taken off line, it shall be possible to disconnect the HDS from the PG for performing various work activities, such as software update, testing, and other maintenance activities.

SYS-180. An HDS that has been taken off-line shall take steps as needed to return it to the service. If no change to its registration is needed, PG and DB shall be notified and confirmation shall be received before it can publish data again. If change to its registration is needed, then either a normal registration process or a registration update process must be conducted before it can publish data again.

SYS-181. The system shall support interactive removal and automatic removal of HDS devices.

SYS-182. Removing a HDS registration from DB shall ensure that all subscriptions related to the HDS will be completed or terminated in an orderly way prior to the start of the HSDS removing process.

SYS-183. The PG shall include a user interface to allow the PG administrator to remove a registered HDS device from service, or remove its registration. Upon request from the PG administrator, the PG shall send an HDS removal request message to DB's NDS to initiate and complete the removal process. Registration shall not be removed automatically through this process; the PG administrator will need to use the interactive method stated above to remove the registration when needed.

SYS-184. The system shall support automatic removal of an HDS from service. Upon receiving a request from an HDS device/system, the PG shall automatically send an HDS removal request message to DB's NDS to initiate and complete the automatic HDS removal process to remove it from the service.

3.3 NASPInet Operational Functions

3.3.1 Query Available Real-Time Streaming Data Sources

SYS-185. The PG with subscribing capability shall enable its user/application/subscriber to query the active registered RT-SDS devices/systems on NASPInet to determine what streaming data is available that it can access. Only subscribing PGs (S-PG) that are currently registered with the NASPInet DB NDS shall be able to query the active real-time streaming data sources. The S-PG shall be able to use the data obtained via the query process to select the proper signals for subscription.

SYS-186. The publishing PG (P-PG) shall have full control over the access rights to the data it publishes. The P-PG shall be able to grant or deny access to all or part of its data to the subscribing PGs.

SYS-187. To allow the P-PG full control of access to its data, all inquiries for a P-PG's published data shall be routed to the P-PG with S-PG's identification.

SYS-188. Only RT-SDS signals that can be accessed by the S-PG with access right granted by P-PG will be shown to the S-PG. The P-PG shall supply, as a minimum, the unique signal IDs, and part or all of the following RT-SDS signal information of accessible RT-SDS signals to the inquiring S-PG:

- Physical location of the device (Country, State, Geo-coordinates, etc.)
- Location identification (substation name, building name, etc.)
- Type of device (PMU, PDC, etc.)
- Device identification (device name, sequence number, etc.)
- Device configuration (physical & logical)
- Complete signal description (type of signal, reporting rate, data format, etc.)
- Signal origin (e.g., original PMU signal that a PDC signal is derived from)
- Signal source (measurement CT/PT, source devices, etc.)
- Signal processing methods (if not original signal)
- Signal quality (data class – latency, reliability, etc.)
- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Ownership (entity name)
- Names according to PG owner naming convention

SYS-189. To inquire about available RT-SDS data sources, the inquiring S-PG shall send an RT-SDS data source inquiry request message to DB.

SYS-190. It shall be possible for the S-PG to submit either generic inquiries to all P-PGs or inquiries that are targeted to specific P-PGs.

SYS-191. Following successful authentication of the requesting S-PG, the DB shall forward the S-PG's request, its ID and pertinent registration information to targeted or all registered P-PGs.

SYS-192. The targeted or all registered P-PGs shall return to DB a list of the signal IDs that the inquiring S-PG is allowed to access. The DB shall, in turn, forward the information received from the P-PGs, including the available signal IDs, to the inquiring S-PG.

3.3.1.1 Interactive Query of P-PGs for Aavailable RT-SDS Signals

SYS-193. The S-PG shall include a function that shall enable the S-PG administrator to submit inquiries about available streaming data sources to either targeted or all P-PGs. The function shall enable the PG administrator to send a "show me the available RT-SDS signals" request to DB with or without a list of targeted P-PGs.

SYS-194. After the requesting S-PG's ID has been authenticated, DB shall forward the inquiry to the either targeted P-PGs or all P-PGs with requesting S-PG's ID and information.

SYS-195. The administrators of the targeted P-PGs shall identify RT-SDS signals that the requesting S-PG is allowed to access, and shall send a list of signal IDs and detailed signals information for those signals that S-PG is allowed to access (if any) to the S-PG via the DB.

SYS-196. The S-PG administrator shall be able to select from the available RT-SDS signals and shall be able to store available signal IDs and other necessary information in S-PG.

3.3.1.2 Automated Querying of P-PGs for Available RT-SDS Signals

SYS-197. An S-PG shall be able to query NASPInet periodically without the S-PG administrator's involvement to update the list of RT-SDS signals that it can access. The S-PG shall automatically send an inquiry request to all P-PGs or a select subset of P-PGs that are known to S-PG and are currently registered with NASPInet.

SYS-198. The S-PG shall be able to send a "show me the available RT-SDS signals" request to either all P-PGs or targeted P-PGs via the DB. The DB shall authenticate the S-PG before sending the request along with the S-PG ID and pertinent registration information to the P-PGs.

SYS-199. The P-PG shall examine the request to determine which signals that S-PG is allowed to access. The list of signal IDs for those signals that the S-PG is allowed to access (list may be empty) shall be sent to DB, which, in turn, will forward detailed signals information and along with the P-PG's ID to the requesting S-PG.

SYS-200. The S-PG shall then be able to store signal IDs, signals' information, and P-PG's ID. The stored data shall allow the PG administrator or authorized/authenticated application to select signals to subscribe to at a later time.

3.3.2 Subscribe to a Real-Time Data Stream

SYS-201. The S-PG shall include facilities to enable the S-PG and S-PG administrator to subscribe to real-time data streams that are available to it from NASPInet publishers (P-PGs). The S-PG and S-PG administrator shall first use the query function (Section 3.3.1) to discover the available signals and obtain detailed information about the available signals.

SYS-202. DB shall provide S-PG and S-PG administrator with data stream start and stop methods for subscribed signals as part of the subscription setup process.

SYS-203. DB shall provide subscription management and cryptographic key management to support RT subscription setup between an S-PG and a P-PG. DB shall ensure that there is no duplicated subscription IDs and security keys for all active subscriptions.

SYS-204. The DB cryptographic key management shall include various mechanisms, such as dynamically changing keys, to keep RT-SDS data secure from non-subscribers.

SYS-205. To subscribe to real time streaming data, registered S-PG shall send a "RT-SDS signals subscription request" message to the P-PG that publish the signals via the DB.

SYS-206. The DB shall authenticate the S-PG. After successful authentication, the DB shall send a subscription ID to S-PG and request the S-PG to send the signal IDs of the subscription and forward the information to the corresponding P-PG along with the subscription ID.

SYS-207. The DB and P-PG shall store the subscription ID, the requested signal IDs and S-PG ID as part of setting up the subscription. Once complete, the P-PG shall be able to send subscription related information, via DB, such as real time streaming data start/stop methods, to the S-PG.

SYS-208. The S-PG shall store the received information and shall at this point be able to start and stop receiving the subscribed data.

3.3.3 Start Receiving a Subscribed Real-Time Data Stream

SYS-209. Real-time data may only be received by a S-PG after obtaining authorization for a subscription as described in 3.3.2. Once an S-PG has a subscription, it shall be able to start and stop the data flow from a P-PG according to its data needs.

SYS-210. To start the data flow, the S-PG shall send the start data flow command to the P-PG via the DB with appropriate authentication information including its subscription number.

SYS-211. Once the P-PG has received the request, it shall send a response to the S-PG, via the DB, to acknowledge the command with a time that it will start sending data or a denial with a reason as to why it will not send data.

SYS-212. If the start request failed, the S-PG shall log the occurrence and take appropriate action, depending on the response. The P-PG shall also log the transaction.

SYS-213. If the start request succeeded, the S-PG shall prepare to receive the data and log the activity. The P-PG shall also log the transaction.

SYS-214. The PG shall also allow the PG administrator to schedule the start of the real-time data stream request, i.e., setting a time when the S-PG will send the signal to start receiving the subscribed real-time data.

SYS-215. The PG shall support manual request by the S-PG administrator to initiate real-time data flow by sending a signal to the P-PG, on demand via the DB, to request real-time data.

3.3.4 Stop a Subscribed Real-Time Data Stream

SYS-216. Real-time data will only be received from a publishing PG (P-PG) by a subscribing PG (S-PG) that has a valid subscription. After an S-PG has started receiving data, the data flow can be stopped by either the P-PG or the S-PG.

3.3.4.1 Stopping by P-PG Request

SYS-217. The P-PG shall be able to stop the real-time data flow by sending a stop data advisory to the S-PG via the DB. This advisory shall include reason for stopping including PG shutdown, PG maintenance, subscription change, access revocation, and loss of data input to PG, etc.

SYS-218. After sending a stop data advisory, the P-PG shall wait an administrator-configurable time for a reply acknowledgement (if possible) before stopping the data flow.

SYS-219. The PG shall allow the P-PG administrator to schedule the stop real-time data stream request, i.e., setting a time when the P-PG will send the stop data advisory and stop publishing the real-time data.

SYS-220. The PG shall support manual request by the P-PG administrator to stop the real-time data flow.

SYS-221. The data stop advisory may also be triggered automatically by certain events. The P-PG shall detect loss of data ingest from the RT-SDS and internal errors that could affect the publishing of the real-time data stream. When such conditions are detected, the P-PG shall send a stop data advisory to S-PGs that subscribe to the data, via the DB, and stop sending data.

SYS-222. The DB, S-PG, and P-PG shall all log the transaction.

3.3.4.2 Stopping by S-PG Request

SYS-223. An S-PG shall be able to stop the data flow at any time by sending a stop data command to the P-PG, via the DB, with appropriate authentication information including the subscription number. Once the DB receives the P-PG confirmation of the request, it shall send a response to the S-PG to acknowledge the command with a time that it will stop the data flow or a failed message with a reason as to why it could not stop the data.

SYS-224. If data flow will be stopped successfully, the S-PG shall prepare to stop receiving data , send a notice to connected applications, and log the activity.

SYS-225. The PG shall allow the S-PG administrator to schedule the stop real-time data stream request, i.e., setting a time when the S-PG will send the stop data request and stop receiving the real-time data.

SYS-226. The PG shall support manual request by the S-PG administrator to stop the real-time data flow.

SYS-227. The DB, S-PG, and P-PG shall all log the transaction.

3.3.5 Unsubscribe From a Subscribed Real-Time Data Stream

Both S-PG and P-PG shall be able to terminate a RT data subscription. This procedure assumes there is already a data subscription in place between the two PGs.

3.3.5.1 Subscription Revocation by P-PG

SYS-228. The P-PG shall allow the P-PG administrator to revoke a subscription. The P-PG shall send a subscription revocation notification to the targeted S-PG via the DB.

SYS-229. The S-PG shall send an acknowledgement of the notification.

SYS-230. The P-PG shall wait an administrator-configurable period of time for the acknowledgement. Whether a response is received or not within the waiting period, the P-PG shall revoke the subscription and send confirmation notice of the revocation to the S-PG.

SYS-231. The S-PG shall take appropriate action with connecting applications such that the data would be stopped gracefully.

SYS-232. If there is an active data flow under the subscription in question, the P-PG shall stop the real-time data flow using the Stop Real-Time Data Stream function outlined above.

SYS-233. If there is no more subscription to the data from any PGs after the removing the requested subscription, the P-PG shall stop ingesting the real-time data to NASPInet.

SYS-234. The DB, the P-PG and the S-PG shall all log the transaction and notify the PG administrator as needed.

3.3.5.2 Un-subscription Initiated by S-PG

SYS-235. The S-PG shall be able to unsubscribe from a RT data stream. The S-PG shall send a notification to unsubscribe a subscription to the appropriate P-PG, via the DB, with the subscription number. The DB shall authenticate the S-PG and confirm its intention to end the subscription before forwarding the request to the P-PG.

SYS-236. If there is an error in processing the unsubscribe request, the DB shall send a notice of failure with the reason for failure to the requesting S-PG. If there is a current data flow, the current data flow shall continue unaltered.

SYS-237. If the request is successful, the P-PG shall send an acknowledgement of success for the request to the S-PG via the DB, and remove the subscription from its list.

SYS-238. If there is an active data flow under the subscription in question, the S-PG shall stop the real-time data flow using the Stop Real-Time Data Stream function outlined above.

SYS-239. If there is no more subscription to the data from any PGs after the removing the requested subscription, the P-PG shall stop ingesting the real-time data to NASPInet.

SYS-240. Both the P-PG and the S-PG as well as the DB shall log the transaction and notify the PG administrator as needed.

SYS-241. The PG shall support manual request by the S-PG or P-PG administrator to cancel the subscription and stop the real-time data flow.

3.3.6 Inquiry for Available Historical Data Sources

SYS-242. The S-PG shall enable its user/application/subscriber to initiate a query to determine the availability of historical data available via the NASPInet.

SYS-243. Only S-PGs that are currently registered with the NASPInet shall be able to initiate a query to determine the availability of a historical data source (HDS).

SYS-244. The S-PG shall be able to use the data obtained via the query process to request a block of historical data.

SYS-245. The P-PGs for the underlying RT-SDS corresponding to the signals requested in the historical data query shall have full control over the access rights to the historical data, regardless where the historical data resides. The P-PG for the underlying RT-SDS shall be the only one to grant or deny access to all or part of the historical data that originate from its RT-SDS.

SYS-246. To allow the P-PGs for the underlying RT-SDS maintaining full control of access to their data, DB shall route all inquiries for historical data to the P-PGs associated with the corresponding registered RT-SDS signal of an HDS.

SYS-247. Historical data queries for a signal (data point) not associated with a corresponding registered RT-SDS signal shall be disallowed by the DB.

SYS-248. To inquire about available historical data sources, the inquiring S-PG shall send a historical data source inquiry request message to DB.

SYS-249. It shall be possible for the S-PG to submit either generic inquiries to all P-PGs or inquiries that are targeted to specific P-PGs.

SYS-250. Following successful authentication by the DB, the DB shall forward the S-PG request and its ID to targeted or all registered P-PGs. Each P-PG shall return to DB a list of the historical data sources that the inquiring S-PG is allowed to access.

SYS-251. The DB shall, in turn, forward the information received from the P-PGs, including the available historical data, to the inquiring S-PG. Information supplied to the S-PG shall include as a minimum:

- Location identification (substation name, building name, etc.)
- Type of device (PDC, Data Archiving Device, an operation data warehouse, etc.)
- Device identification (device name, sequence number, etc.)
- Signal origin (e.g., original PMU signal that a PDC signal is derived from)
- Signal processing methods (if not original signal)
- Signal quality (data class – latency, reliability, etc.)
- Ownership (entity name)
- Names according to PG owner naming convention
- Names according to NASPInet naming convention
- Time periods of data stored

SYS-252. The S-PG shall enable the PG administrator or authorized applications to submit inquiries about available historical data sources to a select set of P-PGs, including a list of targeted P-PGs or all P-PGs registered with the DB.

SYS-253. After authenticating the administrator or external application, the S-PG shall send a "show the available HDS data" request to the selected P-PGs via the DB.

SYS-254. After successful authentication and authorization of the requesting S-PG, the DB shall forward the inquiry to the select set of P-PGs. Each P-PG shall respond to the DB with a list of historical data available to the S-PG; the list could be null.

SYS-255. The DB shall forward available historical data sources that are accessible by the S-PG to the S-PG.

SYS-256. If the inquiry fails, the requesting S-PG shall be notified with a reason for failure and all PGs as well as the DB shall log the transaction.

SYS-257. The S-PG administrator shall be able to store HDS IDs and available historical data information in S-PG.

3.3.7 Request Historical Data

SYS-258. An S-PG shall allow an authorized user or application to request a block of historical data from a P-PG via DB. The signals to be requested shall first be identified using the historical data query function outlined above. The S-PG shall send the historical data request to the P-PG via DB. As a minimum, this request shall include the S-PG ID, the IDs of all signals requested and the start and stop times (in UTC time to an even second) of the interval of data requested.

SYS-259. The P-PG shall, via DB, authenticate the request and respond with an affirmative if the requested data will be sent or a denial if it will not be sent with the reason for denial.

SYS-260. If affirmative, the P-PG shall also send to the S-PG, via DB, information regarding the data that will be sent including a request ID, information for decoding the signals from the data transmission, scaling, data format, data rate, approximate volume (in bytes) of data, and any other available information required for reception and use of the data.

SYS-261. The S-PG shall provide the information regarding the requested historical data to the user or application for confirmation, and send the confirmation to the P-PG.

SYS-262. The P-PG shall discard the request if the confirmation is not received within a administrator-configurable time period.

SYS-263. Both the P-PG and the S-PG as well as the DB shall log the transaction and notify the PG administrators as needed.

3.3.7.1 Manual and Scheduled Start of Historical Data Transmission

SYS-264. The S-PG shall allow the S-PG administrator to schedule the start the historical data transmission, i.e., setting a time when the S-PG will send the start command to the P-PG.

SYS-265. The PG shall support manual request by the S-PG user or authorized application to start the historical data transmission on demand.

3.3.8 Start Receiving a Block of Historical Data

SYS-266. Once a request for historical data has been processed and approved, the S-PG shall send a start command which includes the historical data request ID to each P-PG of the historical data request within a requested data available period.

SYS-267. The S-PG shall allow sending of the start command to the P-PGs at different times.

SYS-268. The P-PG shall discard the historical data request if a start of data transmission request is not received within a requested data available period from the time of the historical data request. The requested data available period is configurable by the P-PG administrator.

SYS-269. When a P-PG receives the start data command it will first authenticate the S-PG and data request ID. If the P-PG will not grant the request, it shall respond to the S-PG with a reason for the denial.

SYS-270. If the P-PG will grant the request, it shall start sending the data and continue until the data transfer is complete or until it receives a request to stop the transmission.

SYS-271. If the P-PG received a start command after the data transfer has been paused (see below), it shall start the data transfer from the beginning of the data block rather than the point at which the transfer was paused.

3.3.9 Pause the Receipt of Historical Data

SYS-272. When historical data is being transmitted from a P-PG to an S-PG, either PG, and the DB shall be able to pause the receipt of data.

3.3.9.1 Historical Data Transmission Pause Initiated by S-PG

SYS-273. If the S-PG wishes to pause the transmission, the S-PG shall send a pause request including the historical request ID to the P-PG. When the P-PG receives a pause request, it shall authenticate the IDs of the data request and the S-PG.

SYS-274. If the request fails, the P-PG shall send a failure notice to the S-PG with a reason for the failure.

SYS-275. If request succeeds, the P-PG shall stop the data flow with appropriate information to be able to resume the transmission at the point of pause. It shall also send a reply to the S-PG that the data has been paused.

SYS-276. The P-PG shall be able to discard the historical data request if the S-PG does not resume or restart the transmission within a requested data available period (e.g. 24 hours) of the pause. The period is configurable by the P-PG administrator.

3.3.9.2 Historical Data Transmission Pause Initiated by P-PG

SYS-277. During transmission of historical data, the P-PG shall be able to pause transmission at any time. The P-PG shall send a pause notification which includes the historical data request ID, a reason for pausing, and an estimated availability time to the S-PG.

SYS-278. Once paused by the P-PG, the transmission of historical data shall not be resumed until the P-PG receives a resume or restart command from the S-PG. The P-PG shall determine if data transmission is allowed at the time of the resume/start request. If yes, it shall restart the data transmission.

SYS-279. The P-PG shall discard the historical data request if the S-PG does not resume or restart the transmission within a requested data available period of the pause. The period is configurable by the P-PG administrator.

3.3.9.3 Historical Data Transmission Pauses Initiated by DB

SYS-280. During transmission of historical data, the DB shall be able to pause transmission at any time. The DB shall send a pause notification which includes the historical data request ID, a reason for pausing, and an estimated availability time to the affected P-PG and S-PG.

SYS-281. Once paused by the DB, the transmission of historical data shall not be resumed until the P-PG receives a resume or restart command from the DB or S-PG. The P-PG shall determine if data transmission is allowed at the time of the resume/start request. If yes, it shall restart the data transmission.

SYS-282. The P-PG shall discard the historical data request if the DB or S-PG does not resume or restart the transmission within a requested data available period of the pause. The period is configurable by the P-PG administrator.

3.3.9.4 Support of Manual and Automated Operation

SYS-283. This function shall support both manual operation by the PG and DB administrators and automated operation. Automated operation shall include both timed and signaled operations. Timed operation shall allow the PG and DB administrator to set a time when a request shall be sent to pause a historical data transfer. Signaled operation shall allow the transfer of historical data to be paused by signals generated from predefined conditions, which are configurable by PG and DB administrators.

3.3.10 Resume the Receipt of Historical Data

SYS-284. After the transmission of historical data has been paused during transfer from P-PG to a S-PG, the S-PG (or DB) shall be able to resume the data transmission. When the S-PG (or DB) wishes to resume or restart a transmission, it shall send a resume or start request including the historical request ID to the P-PG (and S-PG if initiated by DB).

SYS-285. When the P-PG receives a resume or start request, it shall authenticate the IDs of the data request and the S-PG (or DB). If the authentication fails, it shall send a failure notice to the S-PG (or DB) with a reason for the failure.

SYS-286. If authentication succeeds, the P-PG shall resume the data flow from the point of pause, or restart from the beginning depend upon whether a resume or a start request is received. The P-

PG shall also confirm to the S-PG (and DB) that the data transmission has been resumed or restarted.

SYS-287. The P-PG shall continue sending data until the request is fulfilled, the transmission is paused again, or the request is canceled.

SYS-288. The system shall allow the S-PG administrator or DB administrator to schedule the resume or restart request at a specific time and send the resume or start command to the P-PG at that time.

SYS-289. The PG shall support manual request by the S-PG user or authorized application to resume the historical data transmission on demand.

SYS-290. This function shall support both manual operation by the PG and DB administrators and automated operation. Automated operation shall include both timed and signaled operations. Timed operation shall allow the PG and DB administrator to set a time when a request shall be sent to pause a historical data transfer. Signaled operation shall allow the transfer of historical data to be paused by signals from connected devices or generated from predefined conditions, which are configurable by PG and DB administrators.

3.3.11 Cancel the Historical Data Request

SYS-291. The P-PG or the S-PG shall be able to cancel a historical data request at any time.

SYS-292. It shall be possible to cancel a historical data request during transmission, if necessary.

SYS-293. If there is a data transfer in progress when an authorized and authenticated cancellation request is received, the P-PG shall discontinue the transmission.

3.3.11.1 Historical Data Request Cancelation Initiated by S-PG

SYS-294. When the S-PG wishes to cancel the request, the S-PG shall send a cancellation request including the historical request ID to the P-PG.

SYS-295. When the P-PG receives the request, it shall authenticate the IDs of the data request and the S-PG. If the authentication fails, it shall send a failure notice to the S-PG with a reason for the failure.

SYS-296. If authentication succeeds, the P-PG shall cancel the data request and stop the data flow if it is currently occurring. It shall also send a reply to the S-PG that the data request has been canceled.

3.3.11.2 Historical Data Request Cancellation Initiated by P-PG

SYS-297. It shall be possible for the P-PG to cancel a historical data request. To do this, the P-PG shall send to the S-PG a cancellation notification which includes the historical request ID and a reason for canceling. A cancellation notice shall be sent any time the P-PG cancels a request, including timeout of the requested data available period.

3.3.11.3 Manual and automated historical data request cancellation

SYS-298. This function shall support for both manual operation by the PG administrators and automated operation. Automated operation shall include both timed and signaled operations. Timed operation shall allow the PG administrator to set a time when a request shall be sent to pause a historical data transfer. Signaled operation shall allow the transfer of historical data to be paused by signals generated from predefined conditions, which are configurable by PG administrators.

4 Phasor Gateway Functional Requirements

This section describes the major functions to be performed by the Phasor Gateway (PG) in concert with the overall NASPInet requirements described in the last section. The functional requirements in this section describe what functions that the PG is expected to perform, not how the function will be designed and implemented. PG_SUPPLIERs are encouraged to propose a design that satisfies the functional requirements while making the best use of PG_SUPPLIER's standard offerings and commercial off-the-shelf products.

The NASPInet Phasor Gateway's functional requirements are divided into two groups:

- **Phasor Gateway General Functional Requirements:** This subsection provides the overall functional requirements of a Phasor Gateway with FULL capability to serve ALL synchrophasor data service classes. The PG's overall functional requirements in this subsection are for supporting PG's and NASPInet's system administration and operation functions.
- **Phasor Gateway Detailed Functional Requirements:** This subsection provides detailed functional requirements of a Phasor Gateway with FULL capability to serve ALL synchrophasor data service classes. The PG's functional requirements in this subsection are for supporting PG's and NASPInet's system administration and operation functions.

A requirement applicability check list is included in this specification as Appendix A, which clearly indicates the data service capabilities of and the applicable requirements for PG_REQUESTER's Phasor Gateway to be supplied by the PG_SUPPLIER.

As Section 1 indicated, the PG system integration and interface requirements are detailed in Section 5; networking and communications requirements in Section 6; security requirements in Section 7; and sizing, performance, and availability requirements in Section 8. PG_REQUESTER should tailor the sample texts in Attachment II to its specific IT governance and resource availability, including hardware and software technical requirements in Sections 9 and 10 respectively; and project implementation and system sustainability services in Section 11.

4.1 General System Functions

This section describes the overall functional requirements of a Phasor Gateway that supports the publication and subscription of all data service classes (full functional PG). For overall functional requirements that apply to PG_REQUESTER's PG to be supplied by PG_SUPPLIER, please consult the PG_REQUESTER's Phasor Gateway Overall Functional Requirement Check List in Appendix A of this specification.

The section describes what functions the full functional PG shall supply to enable it to work seamlessly with DB and other PGs within the NASPInet system. As illustrated in Figure 1.1, every PG connecting to NASPInet's DB shall have two types of interfaces: one type is to interface PG with DB of NASPInet through DB's NASPInet WAN (Network interface 1 – NI1) and the other type is to interface PG with PG_REQUESTER's devices/applications through PG_REQUESTER's own network (Network interface 2 – NI2).

The PG NI2, which communicates with the local PG_REQUESTER equipment/applications, may consist of several physical interfaces to communicate with different PG_REQUESTER's equipment/applications.

The PG shall have a physically separate NI1 that will connect PG with the DB. The NI1 may be comprised of more than one physical interface, but all DB physical interfaces of the PG for DB access shall be physically separate from all physical connections to the external interfaces of PG's NI2.

Detailed networking and communication requirements for PG's NI1 and NI2 are provided in Section 1, "Networking and Communication Requirements".

4.1.1 Phasor Gateway Components Functional Requirements

A full functional PG shall provide the following major logical components in accordance with the NASPInet architectural design framework:

- Phasor Gateway Access (PG-A)
- Phasor Gateway Device Management (PG-DM)
- Phasor Gateway Ingest (PG-I)
- Phasor Gateway Distributor (PG-D)
- Phasor Gateway Historian (PG-H)

Detailed PG components functional requirements are described in the following subsections.

4.1.1.1 PG Access Component Functional Requirements

PG Access shall provide two separate access controls for PG NI1 and PG NI2.

PG NI1 shall only be accessible by PG administrator. PG NI2 shall be accessible by PG administrator and the authorized PG users.

PG Access for NI1 access control shall provide system administration functions for PG administrator to configure, operate, diagnose, and control the PG NI1. PG Access for NI1 access control shall also enable

PG administrator to perform NASPInet internal system administration related functions, such as PG registration, PG registration update, PG registration cancellation, and so on.

PG Access for NI2 access control shall provide system administration functions for PG administrator to configure, operate, diagnose, and control PG NI2. PG Access for NI2 access control shall enable PG administrator to add, edit, and remove PG NI2 users, as well as control each user's access rights. PG Access for NI2 access control shall also enable PG administrator to perform NASPInet external system administration related functions, such as external device/application registration, external device/application registration update, external device/application registration cancellation, and so on with the PG.

PG Access shall meet all applicable security requirements specified in Section 7.

Details for PG NI2 user access control functional requirements are specified in subsection 4.2.1.3.

4.1.1.2 PG Device Management Component Functional Requirements

PG shall provide device management component functions for managing both NASPInet internal devices/services and NASPInet external devices/applications.

PG internal device management shall provide functions for entering, obtaining, authenticating, validating, storing, and retrieving of NASPInet internal device information, such as DB component/services information, other PGs' information, and so on. NASPInet internal device include all registered PGs and DB components.

PG external device management shall provide functions for entering, obtaining, authenticating, validating, storing, and retrieving of NASPInet external device information, such as PMU metadata information, PDC metadata information, application metadata information, and so on. The PG external devices include those residing within the PG_REQUESTER's own network and those that reside on other PG owners' networks.

Specific functional requirements for these functions are detailed in subsection 4.2.1.1 and 4.2.1.2.

4.1.1.3 PG Ingest Component Functional Requirements

PG shall provide Ingest component functions for receiving data from PG NI2 and distributing data to PG NI1.

PG Ingest shall provide functions for incoming traffic monitoring, QoS performance logging, and abnormality logging, alarming, and reporting.

PG Ingest shall provide functions to pass the data received from PG NI2 to PG NI1 either unchanged or converted (protocol conversion, data disaggregation/aggregation, etc.).

4.1.1.4 PG Distributor Component Functional Requirements

PG shall provide Distributor component functions for receiving data from PG NI1 and delivering data to PG NI2.

PG Distributor shall provide functions for outgoing traffic prioritization, PG performance monitoring, and traffic abnormality logging, alarming, and reporting.

PG Distributor shall provide functions to deliver the data received from PG NI1 to PG NI2 either unchanged or converted (protocol conversion, data masking, data disaggregation/aggregation, etc.).

4.1.1.5 PG Historian Component Functional Requirements

The PG shall provide virtual access to historical data that may be stored locally in the PG or another PG or data store via the NASPInet Data Bus. The PG shall provide a Graphical User Interface (GUI) for the PG user and an Application Programming Interface for an external application to request historical data by specifying the device ID, data type, time period of the data, and desired file format (e.g. Excel, Access, ASCII flat file, etc.). The PG shall determine if the requested data is locally available. If yes, the PG shall retrieve the data stored in the PG or another database on the request PG’s LAN/WAN and provide the data in the requested format. If not, the PG shall relay the request to the DB and provide the requested data obtained via the DB in the requested format, or an error message as appropriate (e.g. data not available, format not available, device ID not found, etc.)

4.1.2 Phasor Gateway System Administration Functional Requirements

The PG shall provide appropriate Graphical User Interfaces (GUI) for handling all NASPInet administrative requirements. The PG shall also allow administrative functions to be carried out using its native access if the GUI is not available.

4.1.2.1 User account management

The PG shall provide user account management capability for authorized system users. These shall include providing and restricting the access rights to PG administrative account access, PG NI2 user account creation and access control, PG registration and PG NI1 configurations to PG administrator only. These shall also include providing access to register device and signals for publication (both streaming and historical), query, request, and subscribe to streaming and historical data, and perform any administrative functions, both for the local PG and for the overall DB by PG administrator and by PG NI2 users with varied authorized access rights.

4.1.2.2 PG administrative communication with the DB

The PG shall conform to the methods and protocols of DB API specified by the DB_SUPPLIER for all administrative communication with the DB. The DB API specification will include all protocols and messages necessary to carry out the functions described in these sections. The PG_SUPPLIER shall work with DB_SUPPLIER to resolve all interface issues prior to PG delivery.

4.1.2.3 Registration, update, and removal of the PG from the DB

The PG shall provide a means for PG registration with the DB NDS in accordance with Section 3.2.1. The PG shall also have means to allow an update of registration and removal PG registration from the DB NDS in accordance with Sections 3.2.2 and 3.2.3. PG registration, update, and removal processes shall be interactively performed by the PG administrator, not automatic.

4.1.2.4 Registration, update, and removal of streaming data ingest for publication

The PG shall provide means to register streaming data signals input to NASPInet DB NDS using both interactive and automatic methods as described in section 3.2.4. The signal registration shall be first entered into the PG which shall perform data integrity checks. The actual streaming signal source shall be tested against the registration to assure the registration is accurate. Streaming signal ingest shall be able to receive and deliverg, as a minimum, IEEE C37.118-2005, which provides a configuration frame which should match the signal registration. The PG administrator shall correct any errors before proceeding. Once the registration with PG is validated, the PG shall attempt to register the signals with the DB NDS for publication. Once the DB validates the signals' registration, it shall provide the PG with assigned signal IDs that are unique across the entire NASPInet and the authorization to publish. Automated registration shall be provided for signals previously registered by the PG administrator. The PG shall also provide for streaming data source registration updates and removal as detailed in sections and SYS-136. The PG shall provide a means for PG administrator to configure the automatic registration, updates, or removal of a streaming data source.

4.1.2.5 Registration, update, and removal of historical data ingest for publication

The PG shall provide for registering a historical data source using both interactive and manual means as described in section 3.2.7. This registration shall include all elements detailed in section 3.2.4. Historical data may reside in a variety of formats and systems with differing access methods. The PG_SUPPLIER shall provide means to enable the access of these data source through interface adapters.

The PG shall perform historical data ownership checks on registration. Historical data publication is limited to only those signals that are already registered with DB NDS for publication. As historical data offered by the PG for publishing may not be the published real-time stream data of the PG but from other PGs, PG shall validate data ownership to the extent possible, at a minimum by identifying real-time streaming signal sources of the historical data offered for publication. Since historical data availability may differ over time, the PG shall be capable of communicating with the historical archive or maintaining a signal database to enable proper responses to historical data queries. The PG administrator shall correct any inconsistencies before proceeding with registration. Once a historical data source has been successfully registered with the PG, the PG shall attempt to register it with the DB. Once the DB validates the signals, it shall provide the PG with linked signal IDs and authorization to publish. The PG shall also provide for interactive and automatic updates and removal of historical data sources as provided in 3.2.8 and 3.2.9. The PG shall provide a means for disabling automatic registration, updates, or removal of a data source.

4.1.3 Phasor Gateway System Operation Functional Requirements

PG shall provide means for supporting both streaming data and historical data publishing and subscribing.

4.1.3.1 Real-time Streaming Data Publishing Functions

The PG shall have means to respond to data discovery inquiries, subscription setup/update/removal requests, and start/stop data streaming requests of active subscriptions of streaming data from other PGs, and interact with the requesting PGs and DB to complete the response. It shall support both interactive and automatic methods. The streaming data query and subscription setup processes are detailed in 3.3.1 and 3.3.2. Once a subscription process is successful, the PG shall be able to start and stop the stream as described in Sections 3.3.3 and 3.3.4, or terminate the subscription as described in Section 3.3.5 in response to subscribing PGs' requests. The PG shall provide a means for configuring automatic response to subscription, updates, start, stop, or cancellation of a subscription.

4.1.3.2 Real-time Streaming Data Subscribing Functions

The PG shall provide means to initiate the data discovery inquiries, subscription setup/update/removal requests, and start/stop data streaming requests of active subscriptions of streaming data to publishing PGs, and interact with publishing PGs and DB to complete these inquiries/requests. It shall support both interactive and automatic methods. The query and subscription processes are detailed in 3.3.1 and 3.3.2. Once a subscription process is successful, the PG shall be able to start and stop the stream as described in sections 3.3.3 and 3.3.4, or terminate the subscription as described in section 3.3.5. The PG shall provide a means for configuring automatic initiation of subscription, updates, start, stop, or cancellation of a subscription.

4.1.3.3 Historical Data Publishing Functions

The PG shall provide means to respond to the data discovery inquiries, subscription setup/update/removal requests, and start/pause/resume data delivery of active subscriptions of historical data of other PGs, and interact with the requesting PGs and DB to complete the response. It shall support both interactive and automatic methods. The historical data query and subscription setup processes are detailed in 3.3.6 and 3.3.7. Once a request is granted, the PG shall be able to start, pause, and resumption of the data transfer as described in sections 3.3.8, 3.3.9, and 3.3.10. It shall be able to cancel the subscription as in section 3.3.11. Historical data requests and delivery are by nature temporal, and shall always be terminated when complete. The PG shall provide a means for configuring automatic initiation of query, request, start, pause, resume, or cancel functions.

4.1.3.4 Historical Data Subscribing Functions

The PG shall provide the means to initiate the data discovery inquiries, subscription setup/update/removal requests, and start/pause/resume data delivery of active subscriptions of historical data of other PGs, and interact with the publishing PGs and DB to complete the inquiries/requests. It shall support both interactive and automatic methods. The query and request processes are detailed in 3.3.6 and 3.3.7. Once a request is granted, the PG shall be able to start, pause, and resume the data transfer as described in Sections 3.3.8, 3.3.9, and 3.3.10. It shall also be able to cancel the request as described in section 3.3.10. Historical data requests and delivery are by nature temporal, and shall always be terminated when complete. The PG shall provide a means for configuring automatic query, request, start, pause, resume, or cancel functions.

4.1.4 Phasor Gateway Instrumentation and Traffic Management

PG shall provide means for monitoring the QoS of the data traffic going through PG and managing the traffic according to traffic management polices.

4.1.4.1 PG Ingest traffic monitoring

The PG shall monitor input data for errors and conformance with the data service class specifications. Data received with errors shall be marked before forwarded to the DB. The PG administrator shall be notified of excessive data errors. The level of errors causing notification shall be configurable by the PG administrator to prevent nuisance alarms. If the input data does not conform to the data service class specification and the mismatch cannot be resolved as a configuration change, the PG shall notify the PG administrator and not forward the data.

The PG ingest shall perform quality assurance checks on all input data. The PG shall provide statistics that include:

- Number of missing packets & missing packet rate
- Number of packets with data integrity check, such as CRC check, for detecting errors & data error rate

- Data stream interruptions
- Data stream delays (as detected by class of service instrumentation described below)
- Changes in input data configuration

These and other statistics counters shall be configurable by the PG administrator and provided with timers to keep track of reset events.

4.1.4.2 PG Distributor Traffic monitoring

The PG distributor shall monitor data received from the DB for errors and conformance with the data service class specifications. Data received with errors shall be discarded and not forwarded for distribution. The PG administrator shall be notified of excessive data errors. The level of errors causing notification shall be configurable by the PG administrator to prevent nuisance alarms. If the input data does not conform to the data service class specification and the mismatch cannot be resolved, the PG shall notify the PG administrator and stop distributing the data.

The PG distributor shall instrument data received from the DB for quality assurance. The PG shall provide statistics that include:

- Number of missing packets & missing packet rate
- Number of packets with data integrity check, such as CRC check, for detecting errors & CRC error rate
- Data stream interruptions
- Data stream delays (as detected by class of service instrumentation described below)
- Changes in input data configuration

These and other statistics counters shall be configurable by the PG administrator and provided with timers to keep track of reset events.

4.1.4.3 Streaming data instrumentation

Streaming data is continuous and in many cases high speed. A small rate of lost packets and delays may not be acceptable. Therefore it is important that the PG administrator shall be able to set alarm and reporting limits for each data stream individually.

Quality-of-service assurance for streaming data shall include timing instrumentation. The PG ingest shall check the time tag of the arriving streaming data packets from user equipment, and add a new time stamp to the packet before pass it to DB. The PG ingest shall use the time difference between these two time tags to determine the latency of the received data stream. The PG distributor shall check the added time stamp of the departing streaming data of the PG and use PG own time reference to determine the total latency of the data stream (an important QoS metric) through the NASPInet. The measurement interval shall be configurable by PG administrator. In addition, the PG shall include a function that can time the transmission time of packets from the PG ingest input to output into the DB or from DB to PG distributor output into the user equipment to determine delays within the PG. These functions shall be configurable for normal operation.

Class A and B data service class shall meet millisecond-level delivery latency requirement as specified in 8.2.2. Instrumentation to assure this level of performance shall, as a minimum, include sub-millisecond synchronization accuracy with UTC. A PG equipped for class A and B data service shall have an accurate timing reference source for time measurement and tagging with accuracy within ± 1 μs of UTC.

Class C data service shall meet data delivery latency requirement within 1-2 seconds as specified in 8.2.2. This level of timing for a PG could be supplied by several network services that supply more accurate time reference than internal clock timing. A PG equipped for providing class C streaming data service only shall be allowed to have a timing reference source for time measurement and tagging with accuracy within ± 100 ms of UTC.

4.1.4.4 Class D & E historical data instrumentation

Historical data is discontinuous and has no timing delivery requirements. The PG shall record rate of delivery, communication errors, and delivery failures for blocks of historical data.

4.2 Detailed Functional Requirements

This subsection describes detailed functional requirements of a Phasor Gateway with FULL capability to serve ALL data service classes. The PG's functional requirements in this subsection are for supporting PG's and NASPInet's system administration and operation functions.

PG-1. The PG supplied by PG_SUPPLIER shall meet all PG mandatory requirements listed in this section in accordance to the PG capability requirement matrix. For non-compliance items, PG_SUPPLIER shall provide details and explanations for each non-compliant item.

PG-2. PG_SUPPLIER's proposal shall respond to all highly desirable PG requirements listed in this section in accordance to the PG capability requirement matrix, indicating whether the PG_SUPPLIER will provide the function and meet the functional requirement, or not provide the function.

PG-3. PG_SUPPLIER's proposal shall include responses to desired requirements listed in this section that PG_SUPPLIER elected to provide and meet the requirements.

PG-4. PG_SUPPLIER's proposal shall include responses to optional requirements listed in this section that the PG_SUPPLIER elected to provide and meet the requirements.

PG-5. PG_SUPPLIER shall supply a Phasor Gateway that provides the required data exchange capabilities listed in the PG capability requirement matrix (Table 4-1) below.

Table 4-1 PG Data Exchange Capability Requirement Matrix

Function	Data Group	Class	Required (Initial)	Required (Final)
Publishing	**Streaming data**	A		
		B		
		C		
	Historical data	D		
		E		
Subscribing	**Streaming data**	A		
		B		
		C		
	Historical data	D		
		E		

4.2.1 Phasor Gateway administration

PG supplied by the PG_SUPPLIER shall meet the following PG system administration functional requirements.

4.2.1.1 NASPInet internal devices/services administration

PG-6. PG shall provide GUIs and other supporting system administration functions to enable PG administrator to register, update and remove PG registration information of this PG with DB interactively.

PG-7. PG shall provide registration functions for generating registration request, sending request to DB NDS, sending registration information to DB NDS upon receiving DB NDS approval for registration, and setting PG registration status to “Registered” after DB NDS’ confirmation of a successful registration.

PG-8. PG shall provide GUI/functions to enable PG to update its registration with DB each time its registration information has been changed, either manually by PG administrator or automatically.

PG-9. PG shall provide functions to enable the PG to remove its own registration with DB NDS by PG administrator manually.

PG-10. PG shall provide authentication functions as part of its security component that meet security requirements specified in Section 7 to authenticate all requests and responses received from DB components/services and other PGs.

PG-11. PG authentication functions shall enable PG to authenticate DB component/service through its locally stored information, and/or through further interaction with DB NDS and security services

PG-12. PG authentication functions shall enable PG to authenticate other PGs either through its locally stored information, through further interaction with other PGs, and/or through further interaction with DB NDS and security services

PG-13. PG shall provide a secure local storage for storing PG identification information of this PG and other PGs. PG identification information shall include, as a minimum, PG ID, PG IP addresses, PG capability matrix, PG capabilities, and PG status. Retrieval of such data shall be restricted to PG administrator and related security service functions (e.g. authentication function) only.

PG-14. PG shall provide a secure local storage for storing DB components and services identification information of the DB. DB components identification information shall include, as a minimum, DB component/service ID, DB component/service IP addresses, DB component capabilities matrix, and DB component/service status. Retrieval of such data shall be restricted to PG administrator and related functions (e.g. authentication function) only.

PG-15. PG shall provide a function to automatically notify DB NDS of its status change each time a change occurs.

PG-16. PG shall provide a function to respond to DB status query with its current status.

PG-17. PG shall provide functions to log its interactions with other PGs and DB component/service. Logged information shall be stored locally and securely. Logged information shall not be editable by anyone, including PG administrator, but shall be able to be copied and exported by PG administrator.

4.2.1.2 NASPInet external devices/applications administration

PG-18. PG shall provide GUIs and functions for registering devices/applications with this PG that are external to NASPInet, such as PMUs, PDCs, phasor applications, etc., either manually by PG administrator or automatically by responding to device/application’s registration request.

PG-19. PG shall provide GUIs and functions for PG administrator to setup the PG for automatic external devices/applications registration (such as assign/setup device/application ID, enter key information of a device/application for authentication, etc.), so that it will be able to respond to device/application’s registration request directly.

PG-20. PG shall provide GUIs and functions for updating device/application's registration information with this PG for registered devices/applications interactively by PG administrator. Registration information update shall include the status update of external device/application, such as from "online" to "offline".

PG-21. PG shall provide functions for updating device/application's registration information with this PG for registered devices/applications automatically by responding to device/application's registration request. Registration information update shall include the status update of external device/application, such as from "online" to "offline". PG shall provide GUIs and functions for PG administrators to configure the automated registration updating function.

PG-22. PG shall provide GUIs and functions for canceling device/application's registration with this PG for any registered device/application interactively by PG administrator. Cancellation shall be used for removing a device/application permanently out of service.

PG-23. Register Device/Application with DB manually: PG shall provide GUIs and functions for registering a device/application with DB NDS that have been registered with this PG manually by PG administrator upon the completion of device/application's registration with this PG. The registration process shall include sending registration request to DB NDS, supplying registration metadata to DB NDS, receiving and storing assigned device/application ID and signals IDs for the device/application, and confirming the successful completion of the registration process.

PG-24. Register Device/Application with DB automatically: PG shall provide functions for automatically registering a device/application with DB NDS that have been registered with this PG by initiating the DB NDS registration process immediately upon the completion of device/application's registration with this PG. The registration process shall include sending registration request to DB NDS, supplying registration metadata to DB NDS, receiving and storing assigned device/application ID and signals IDs for the device/application, and confirming the successful completion of the registration process. PG shall provide GUIs and functions for PG administrators to configure the automated functions for registering device/application with DB.

PG-25. Update Device/Application Registration with DB manually: PG shall provide GUIs and functions for updating a device/application's registration with DB NDS that have been registered with DB NDS manually by PG administrator. The updating process shall include sending updating request to DB NDS, supplying updated registration metadata to DB NDS, receiving and storing updated device/application ID and signal IDs for the device/application, and confirming the successful completion of the registration updating process. Registration information update shall include the status update of external device/application, such as from "online" to "offline".

PG-26. Update Device/Application Registration with DB automatically: PG shall provide GUIs and functions for updating a device/application's registration with DB NDS that have been registered with DB NDS automatically by initiating the corresponding updating process immediately upon the completion of device/application's updating with this PG. The updating process shall include sending updating request to DB NDS, supplying updated registration metadata to DB NDS, receiving and storing updated device/application ID and signal IDs for the device/application, and confirming the successful completion of the registration updating process. Registration information update shall include the status update of external device/application, such as from “online” to “offline”. PG shall provide GUIs and functions for PG administrators to configure the automated functions for updating device/application registration with DB.

PG-27. Cancel Device/Application Registration with DB manually: PG shall provide GUIs and functions for canceling a device/application’s registration with DB NDS that have been registered with DB NDS manually by PG administrator. The canceling process shall include sending canceling request to DB NDS, confirming its intention to cancel the registration to DB NDS, acknowledging the receipt of DB NDS’ confirmation of the registration cancellation. Cancellation shall be used for removing a device/application permanently out of service.

PG-28. PG shall provide a secure local storage for storing the registration metadata for devices/applications registered with this PG. The stored metadata shall include if the device/application has been registered with DB NDS, and the assigned device/application ID and signal IDs if the device/application is already registered with DB NDS.

PG-29. PG shall provide functions for logging the status of devices/applications it has registered.

PG-30. PG shall provide functions for automatically sending the device/application status to DB NDS for devices/applications registered with the DB NDS each time a status change occurs.

PG-31. PG shall provide a function to respond to DB status query for any device/application that is registered with the DB NDS with its current status.

4.2.1.3 PG user administration

PG-32. PG shall provide a default PG administrator account for PG administrator to perform PG administration functions of the PG on PG_REQUESTER side, such as external device registration/update/cancel, for which the default login information (user ID and password) shall be changed at the first login process.

PG-33. PG shall provide GUIs and the related functions for PG administrator to setup/delete and manage PG_REQUESTER’s PG user accounts for users accessing PG on the PG_REQUESTER’s own network side.

PG-34. PG shall provide means for PG administrator to set access policy for PG_REQUESTER’s user account on an individual user basis. PG should also provide means for PG administrator to set access policy for PG_REQUESTER’s user accounts on other basis, such as type of users.

PG-35. PG shall provide GUIs and the related functions for PG administrator to administer the PG configurations, access policy for other PGs on an individual PG basis, and access policy for DB components/services, on the DB network side on an individual component basis.

PG-36. PG shall provide a separate default PG administrator account for PG administrator to perform system administration functions on DB network side, such as registering/updating/canceling the PG, for which the default login information (user ID and password) shall be changed at the first login process.

PG-37. PG general users shall not be able to log into user accounts through NASPInet WAN to access PG.

PG-38. It shall not be possible to access PG administration functions for DB network side by logging into PG administrator's account and PG_REQUESTER users' accounts from PG_REQUESTER's network.

PG-39. PG shall provide user authentication functions as part of its security component that meets security requirements specified in Section 7.

PG-40. PG shall provide functions for logging user account activities of the PG. It shall not be possible for PG administrator and users to alter the logged information. It shall be possible to make a copy of the logged information and export it.

PG-41. PG shall provide GUIs and related function for PG administrator to set the time period that the logged information shall be kept before discarded by the PG. It shall not be possible to set the time period below the minimum time period that the logged user activities shall be kept in the PG.

4.2.2 Phasor Gateway publish/subscribe operations

PG supplied by the PG_SUPPLIER shall meet the following PG publish/subscribe operation functional requirements.

4.2.2.1 PG publishing/subscribing general requirements

PG-42. PG shall implement standard APIs for interfacing PG ingest and distributor components with DB per DB API specifications

PG-43. PG shall implement default/customizable APIs for interfacing PG ingest and distributor components to devices and applications (PMUs, PDCs, historians, EMS/SCADA systems, various applications, etc.) on PG_REQUESTER network side.

PG-44. PG shall provide GUIs and related functions for PG administrator to manually configure APIs to connect the PG with devices and applications on PG_REQUESTER network side.

PG-45. PG shall provide an API to allow for automated connection of the PG ingest and distributor components with the devices and applications that are on the PG_REQUESTER network side and are already registered with PG. The API shall be able to respond to device/application's "request for connection" to authenticate the requested device/application, validate the request, establish the connection, and test the connection to complete the connection process. The API shall also be able to initiate the connection process by issuing a "request for connection" to a registered device/application.

PG-46. PG ingest APIs shall include both real-time streaming data ingest API and historical data ingest API components.

PG-47. PG real-time streaming data ingest API shall be able to handle multiple real-time data streams with different data classes and different data rates concurrently.

PG-48. PG ingest APIs shall enable the integration of various QoS instrumentation and performance monitoring functions.

PG-49. PG distributor APIs shall include both real-time streaming data distributor API and historical data distributor API components.

PG-50. PG real-time streaming data distributor API shall be able to handle multiple real-time data streams with different data classes and different data rates concurrently.

PG-51. PG distributor APIs shall enable the integration of various QoS instrumentation and performance monitoring functions.

PG-52. PG shall include protocol conversion functions for converting ingest input data protocols to distributor input data protocols. The protocol conversion shall include, as a minimum, simple data masking without change data protocol.

PG-53. PG shall provide GUIs and related functions for PG administrator to configure the protocol conversion functions.

PG-54. PG shall also provide GUIs and related functions for PG administrator to setup predefined protocol conversion configurations.

PG-55. PG distributor APIs shall enable the integration of data decryption functions for decrypting data received from DB network side. The decryption functions shall be able to decrypt the received data using the key provided by the DB key generation and management functions through subscription setup process.

PG-56. PG ingest APIs shall enable the integration of data encryption functions for encrypting data sending to DB network side. The encryption functions shall be able to encrypt the published data using the publishing key provided by the DB key generation and management functions through subscription setup process.

PG-57. PG shall provide a function for securely storing the subscription IDs and detailed subscription information for each subscription. The subscription IDs shall be used for all subscription related communications, such as initiate a "stop" request for the data transfer to subscribing PGs either by P-PG or S-PG.

PG-58. For publishing data, PG shall provide functions for PG administrator to administer the access rights to different data service classes on a per PG and per signal basis.

4.2.2.2 Real-time streaming data publishing

PG-59. PG shall provide a function for responding to DB relayed real-time streaming data discovery requests from other PGs. The function shall respond to DB relayed real-time streaming data discovery requests from UNKNOWN PGs by authenticating DB, validating the request with DB, obtaining (and storing) PG identification information from DB for determining its access rights of the requesting PG, and sending all real-time streaming signal IDs that the requesting PG is allowed to subscribe to DB for relaying to the requesting PG. The function shall respond to DB relayed real-time streaming data discovery requests from KNOWN PGs by authenticating DB and PG, validating the request with the requesting PG, sending all real-time streaming signal IDs that the requesting PG is allowed to subscribe to the requesting PG, and informing DB that the request has been processed.

PG-60. PG shall provide GUIs and related functions for the PG administrator to set real-time streaming data access policy for previously unknown PGs according to their identification information obtained from DB. The GUIs and functions for setting real-time streaming data access policy shall allow PG administrator to set the access policy on an individual PG basis with a signal granularity. The GUIs and functions for setting real-time streaming data access policy shall also allow PG administrator to update the access policy on an individual PG basis with a signal granularity.

PG-61. PG shall provide GUIs and related functions for PG administrator to review/validate the real-time streaming data discovery request, and manually select and send real-time streaming data signals that other PGs are allowed to access.

PG-62. PG shall provide a function for responding to real-time streaming data subscription requests from other PGs via DB. The function shall only respond to requests from known PGs. The function shall respond to data subscription requests from known PGs by authenticating PG, validating the request with the requesting PG, setting up the subscription with the requesting PG, and sending subscription access methods to subscribing PG that made the request. The subscription access methods shall include subscription number, cryptographic key, and real-time data stream start/stop methods of the subscription. The function shall send a “PG unknown” message to DB along with the requests for all the requests from unknown PGs.

PG-63. PG shall provide supporting functions for setting up real-time streaming data publishing in response to subscribing PG’s subscription request.

PG-64. PG subscription supporting functions for setting up real-time streaming data publishing shall respond to subscribing PG’s subscription request by working with DB subscription management functions on QoS provisioning, subscription ID generation and management, and cryptographic key generation and management.

PG-65. The PG subscription supporting functions for setting up real-time streaming data publishing shall provide source data QoS statistics and PG loading information in response to DB subscription QoS provision function's request to enable it to determine whether a new subscription can be supported and its QoS requirements can be met based on the DB components loading, NASPInet WAN network component loading, and PG loading of involved PGs.

PG-66. The PG subscription supporting functions for setting up real-time streaming data publishing shall store subscription ID generated by DB subscription ID generation and management functions for real-time streaming data subscription management and obtained from subscribing PG's subscription request. PG shall use subscription ID in all future communications with subscribing PG and DB related to this subscription.

PG-67. The PG subscription supporting functions for setting up real-time streaming data publishing shall store publishing cryptographic encryption key generated by DB cryptographic key generation and management functions for real-time streaming data subscription management and obtained from DB at the completion of subscription setup when the data stream is to be published the first time. PG shall use the key to encrypt the data packets of the published stream.

PG-68. The PG subscription supporting functions for setting up real-time streaming data publishing shall initialize the subscription instrumentation function to monitor the data publishing performance.

PG-69. The PG cryptographic key management function for real-time streaming data publishing shall be able to work in concert with DB cryptographic key management function to support dynamic key management scheme, which as a minimum shall be changed periodically.

PG-70. PG shall provide a function for responding to "real-time streaming data subscription cancellation" requests from the subscribing PGs. The function shall only respond to requests from known PGs with valid subscriptions. The function shall respond to data subscription cancellation requests from known PGs by authenticating PG, validating the request with the requesting PG, and confirming the cancellation of the subscription with the requesting PG. The function shall send a "PG unknown" message to DB along with the request for all the requests from unknown PGs and/or with invalid subscriptions. In the case that this is the last subscription of the stream to be cancelled, PG shall retire the publishing key and stop the publishing of the stream.

PG-71. PG shall provide GUIs and related functions for PG administrator to cancel an active real-time streaming data subscription. The GUIs and functions shall allow PG administrator to cancel a subscription by selecting the real-time streaming data subscription to be cancelled, sending a message to subscribing PG and DB notifying its intention to cancel the subscription, and set the status of the subscription to "cancelled" once received acknowledgement from the subscribing PG and DB. In the case that this is the last subscription of the stream to be cancelled, PG shall retire the publishing key and stop the publishing of the stream.

PG-72. PG shall provide a function for responding to “start real-time data streaming” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscription IDs. The function shall respond to “start real-time data streaming” requests from known PGs by authenticating PG and subscription ID, validating the request, and starting the data streaming to the requesting PG. The function shall start the data streaming based on the traffic management policy and the actual traffic through the PG and DB. The function shall set the status of the subscription to “data streaming started” after received the confirmation that the subscribing PG is starting to receive the data correctly. The function shall provide means to alert PG administrators of publishing and subscribing PGs and DB administrator for any unsuccessful starting of the data streaming. The function shall send a “PG unknown” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscription IDs.

PG-73. PG shall provide a function for responding to “stop real-time data streaming” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscription IDs. The function shall respond to “stop real-time data streaming” requests from known PGs by authenticating PG and subscription ID, validating the request, and stopping the data streaming to the requesting PG. The function shall set the status of the subscription to “data streaming stopped” after received the confirmation that the subscribing PG is no longer receiving the data stream. The function shall provide means to alert PG administrators of publishing and subscribing PGs and DB administrator for any unsuccessful stopping of the data streaming. The function shall send a “PG unknown” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscriptions. DB shall stop sending the subscribed data stream to subscribing PG upon the completion of the process and retire the subscription cryptographic key. PG shall stop publishing the data stream if it is the last subscription to stop. Otherwise, PG shall continue to publish the data stream for other active subscriptions.

PG-74. PG shall provide a function for stopping the data stream to a subscribing PG. the function shall notify subscribing PG and DB for its intention to stop the data streaming. DB shall stop sending the subscribed data stream to subscribing PG upon the completion of the process and retire the subscription cryptographic key. PG shall stop publishing the data stream if it is the last subscription to stop. Otherwise, PG shall continue to publish the data stream.

4.2.2.3 Real-time streaming data subscription

PG-75. PG shall provide a function for inquiring accessible real-time streaming data from other PGs through DB NDS. The function shall be able to obtain accessible real-time streaming data information from publishing PGs by sending an “accessible real-time streaming data” request to

DB either as a general query or as a targeted query with the targeted PGs' IDs, and receiving and storing signal IDs of the accessible real-time streaming data from publishing PGs along with publishing PGs' IDs. For unknown PGs, the function shall obtain PG identification information of those PGs from DB NDS and store them for future PG authentication purpose.

PG-76. PG shall provide GUIs and related functions for PG administrator to initiate "accessible real-time streaming data" queries to DB. The GUIs and functions for initiating the queries shall enable PG administrator to include a list of PGs included/excluded in a query.

PG-77. PG shall provide a function for PG to automatically initiate the "accessible real-time streaming data" query to DB, and receiving and storing signal IDs for accessible real-time streaming data from publishing PGs. For unknown PGs, the function shall obtain PG identification information from DB NDS and store them automatically for future PG authentication purpose.

PG-78. PG shall provide GUIs and functions for PG administrator to configure the automated initiation of "accessible real-time streaming data" queries to DB. The GUIs and functions shall enable PG administrator to enable/disable the automated initiations, set time interval that PG shall generate a query if enabled for timed query, and set various conditions of the queries, such as included/excluded PGs lists, abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up multiple automated queries initiation for multiple known PGs.

PG-79. PG shall provide GUIs and related functions for PG administrator to obtain detailed signal information using obtained signal IDs from DB NDSy.

PG-80. PG shall provide a function for PG to automatically obtain detailed signal information using obtained new signal IDs from DB NDS and store these information for future use.

PG-81. PG shall provide functions for setting up subscriptions of selected real-time streaming data signals with the publishing PGs.

PG-82. PG shall provide GUIs and related functions for PG administrator to create subscription requests for real-time streaming data signals and send the requests to publishing PGs. The GUIs and functions shall enable PG administrator to select signals for a subscription, and set the data service class and specific QoS requirements for the subscription. PG shall also provide a function for obtaining a subscription ID for the subscription from DB's subscription ID generation and management function, communicating with publishing PG to setup the subscription, and confirming to DB subscription management function of the successful setup. It shall also receive a cryptographic subscription key from DB which is different from all publishing and subscription keys of the active subscriptions.

PG-83. PG shall provide a function to automatically create subscription requests for real-time streaming data signals and send the requests to publishing PGs. The function shall enable PG to automatically select signals for a subscription, and set the data service class and specific QoS requirements for the subscription. PG shall also provide a function for obtaining a subscription ID for the subscription from DB subscription ID generation and management functions, communicating with publishing PG to setup the subscription, and confirming to DB subscription management function of the successful setup. It shall also receive a cryptographic subscription key from DB which is different from all publishing and subscription keys of the active subscriptions.

PG-84. PG shall provide GUIs and functions for PG administrator to configure the automated subscription request generation function. The GUIs and functions shall enable PG administrator to enable/disable the subscription request generation, and to set various conditions for creating a request, such as creating a request upon receiving subscription request from connected devices/applications on PG_REQUESTER's own network side, etc., and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated generation of multiple subscription requests for different external devices/applications.

PG-85. PG shall provide GUIs and related functions for PG administrator to test and confirm the proper setup of a subscription for real-time streaming data signals. The GUIs and functions shall enable PG administrator to start and then stop the real-time streaming data using the start/stop methods provided by the publishing PG to ensure that the subscription was set up correctly and all QoS requirements are met. The GUIs and functions shall enable PG administrator to confirm to the publishing PG that the subscription has been successfully set up.

PG-86. PG shall provide a function to automatically test and confirm the proper setup of a subscription for real-time streaming data signals. The function shall enable PG to automatically start and then stop the real-time streaming data using the start/stop methods provided by the publishing PG for the subscription to ensure that the subscription was set up correctly and all QoS requirements are met. The function shall enable PG to automatically send a confirmation to the publishing PG that the subscription has been successfully set up.

PG-87. PG shall provide GUIs and functions for PG administrator to configure the automated subscription test and confirmation. The GUIs and functions shall enable PG administrator to enable/disable the automated subscription test and confirmation, and set various conditions for conducting the test, handling abnormal conditions, and make the final confirmation. The GUIs and functions shall enable PG administrator to configure multiple automated test and confirmation processes for different types of subscriptions.

PG-88. PG shall provide GUIs and related functions for PG administrator to start the data streaming of an established subscription for real-time streaming data signals by sending a “start” request with the subscription's ID to the publishing PG using the method provided by the publishing PG through the subscription setup process. The GUIs and functions shall enable PG administrator to select a particular subscription to request starting, confirm to publishing PG that it is receiving the data, and set the status of the subscription to “streaming”.

PG-89. PG shall provide a function to automatically start the data streaming of an established subscription for real-time streaming data signals by automatically sending a “start” request with the subscription’s ID to the publishing PG using the method provided by the publishing PG through the subscription setup process. The function shall enable PG to start a particular subscription, confirm to publishing PG that it is receiving the data of the subscription, and set the status of the subscription to “streaming”.

PG-90. PG shall provide GUIs and functions for PG administrator to configure the automated start of the data streaming of an established subscription. The GUIs and functions shall enable PG administrator to enable/disable the automated start function, and to set various conditions for creating the request, such as creating a request upon receiving a “start” request of the subscription from connected devices/applications on PG_REQUESTER’s own network side, etc., and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated start of multiple subscriptions.

PG-91. PG shall provide GUIs and related functions for PG administrator to stop the data streaming of an established subscription for real-time streaming data signals by sending a “stop” request with the subscription ID to publishing PGs using the method provided by the publishing PG through the subscription setup process. The GUIs and functions shall enable PG administrator to select a particular subscription to stop, confirm to publishing PG that the data has stopped coming, and set the status of the subscription to “stopped”. PG shall also be able to respond to publishing PG’s advisory to stop publishing data for this subscription by acknowledging the request to publishing PG.

PG-92. PG shall provide a function to automatically stop the data streaming of an established subscription for real-time streaming data signals by automatically sending a “stop” request with the subscription’s ID to the publishing PG using the method provided by the publishing PG through the subscription setup process. The function shall enable PG to stop a particular subscription with a status of “streaming”, confirm to publishing PG that the data of the subscription has stopped coming, and set the status of the subscription to “stopped”. PG shall also be able to automatically respond to publishing PG’s advisory to stop publishing data for this subscription by acknowledging the request to publishing PG.

PG-93. PG shall provide GUIs and functions for PG administrator to configure the automated stop of the data streaming of an established subscription. The GUIs and functions shall enable PG administrator to enable/disable the automated stop function, and to set various conditions for creating the request, such as creating a request upon receiving a “stop” request of the subscription from connected devices/applications on PG_REQUESTER’s own network side, etc., and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated stop of multiple subscriptions.

PG-94. PG shall provide GUIs and related functions for PG administrator to cancel an established subscription for real-time streaming data signals by sending a “cancel subscription” request with the subscription ID to the publishing PG. The GUIs and functions shall enable PG administrator to select a particular subscription to cancel, confirm to publishing PG that indeed that it want to cancel the subscription, and set the status of the subscription to “cancelled” after received publishing PG’s confirmation of cancellation.

PG-95. PG shall provide a function to automatically cancel an established subscription for real-time streaming data signals by automatically sending a “cancel subscription” request with the subscription’s ID to the publishing PG. The function shall enable PG to cancel a particular subscription with a status of “active”, confirm to publishing PG that indeed that it wants to cancel the subscription, and set the status of the subscription to “cancelled” after received publishing PG’s confirmation of cancellation. PG shall also be able to respond to publishing PG’s advisory to cancel the subscription by canceling the subscription and acknowledging the request to publishing PG.

PG-96. PG shall provide GUIs and functions for PG administrator to configure the automated cancellation of an established subscription for real-time streaming data signals. The GUIs and functions shall enable PG administrator to enable/disable the automated cancellation function, and to set various conditions for creating the cancellation request, such as creating a request upon receiving the last “cancel subscription” request from connected devices/applications on PG_REQUESTER’s own network side that were data users of the subscription, and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated cancellation of multiple subscriptions.

4.2.2.4 Historical data publishing

PG-97. PG shall provide a function for responding to DB relayed historical data discovery requests from other PGs. The function shall respond to DB relayed historical data discovery requests from UNKNOWN PGs by authenticating DB, validating the request with DB, obtaining and storing requesting PG identification information from DB for determining its access rights of the requesting PG, and sending all historical data signal IDs that the requesting PG is allowed to subscribe to DB for relaying to the requesting PG. The function shall respond to DB relayed historical data discovery requests from KNOWN PGs by authenticating DB and PG, validating the request with the requesting PG, sending all historical data signal IDs that the requesting PG is allowed to subscribe to the requesting PG, and informing DB that the request has been processed. (Note: Publishing PGs only provides historical data for all published real-time streaming data signals. Although signal IDs will be the same, the access rights to these signals may be different for real-time streaming data and historical data. For example, some real-time data may deemed to be sensitive for subscribing PG entity to access as it may have some market advantages to access the data, but will not be so once a certain time period has been passed. On the other hand, publishing PG owner may consider certain historical data being sensitive thus may want to limit their access to other subscribing PGs.)

PG-98. PG shall provide GUI and related functions for PG administrator to set historical data access policy for previously unknown PGs according to their registration information obtained from DB. The GUIs and functions for setting historical data access policy shall allow PG administrator to set the access policy on an individual PG basis with a signal level granularity. The GUIs and functions for setting historical data access policy shall also allow PG administrator to update the access policy on an individual PG basis with a signal granularity.

PG-99. PG shall provide GUI and related functions for PG administrator to review/validate the historical data discovery request, and manually select and send historical data signals that other PGs are allowed to access.

PG-100. PG shall provide a function for responding to DB relayed historical data subscription requests from other PGs. The function shall only respond to requests from known PGs. The function shall respond to DB relayed historical data subscription requests from known PGs by authenticating DB, validating the request with the requesting PG directly, and setting up the subscription with the subscription requesting PG. The function shall respond to DB with “unknown requesting PG” message for requests from unknown PGs.

PG-101. PG shall provide supporting functions for setting up historical data publishing.

PG-102. PG subscription supporting functions for setting up historical data publishing shall respond to subscribing PG’s subscription request by working with DB subscription management functions on QoS provisioning, subscription ID generation and management, and cryptographic key generation and management.

PG-103. The PG subscription supporting functions for setting up historical data publishing shall provide source data QoS statistics and PG loading information in response to DB subscription QoS provision function’s request to enable it to determine whether a new subscription can be supported and its QoS requirements can be met based on the DB components loading, NASPInet WAN network component loading, and PG loading of involved PGs.

PG-104. The PG subscription supporting functions for setting up historical data publishing shall store subscription ID generated by DB subscription ID generation and management functions for historical data subscription management and obtained from subscribing PG’s subscription request. PG shall use subscription ID in all future communications with subscribing PG and DB related to this subscription. The PG subscription supporting functions for setting up historical data publishing shall also store subscription cryptographic key generated by DB cryptographic key generation and management functions for historical data subscription management and obtained from DB at the completion of subscription setup when the historical data is to be published. PG shall use the key to encrypt the data file of the published historical data.

PG-105. PG shall provide a function for responding to “historical data subscription cancellation” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscriptions. The function shall respond to data subscription cancellation requests from known PGs by authenticating requesting PG, validating the request with the requesting PG, and confirming the cancellation of the subscription with the requesting PG. The function shall send a “PG unknown/Invalid Subscription” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscriptions.

PG-106. PG shall provide GUI and related functions for PG administrator to cancel an active historical data subscription. The GUIs and functions shall allow PG administrator to cancel a subscription by selecting the historical data subscription to be cancelled, sending a message to subscribing PG notifying the intent to cancel the subscription, and set the status of the subscription to “cancelled”.

PG-107. PG shall provide a function for responding to “start historical data transfer” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscriptions. The function shall respond to “start historical data transfer” requests from known PGs by authenticating requesting PG, validating the request, and starting the data transfer to the requesting PG. The function shall start the data transfer based on the traffic management policy and the actual traffic through the PG and DB. The function shall set the status of the subscription to “data transfer started” after received the confirmation that the subscribing PG is starting to receive the data correctly. The function shall provide means to alert PG administrators of publishing and subscribing PGs and DB administrator for any unsuccessful starting of the data transfer. The function shall send a “PG unknown/Invalid Subscription” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscription IDs.

PG-108. PG shall provide a function for responding to “pause historical data transfer” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscriptions. The function shall respond to “pause historical data transfer” requests from known PGs by authenticating the requesting PG, validating the request, and pausing the data transfer to the requesting PG. The function shall set the status of the subscription to “data transfer paused” after received the confirmation that the subscribing PG is no longer receiving the data transfer. The function shall provide means to alert PG administrators of publishing and subscribing PGs and DB administrator for any unsuccessful pausing of the data transfer. The function shall send a “PG unknown” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscriptions.

PG-109. PG shall provide a function for responding to “resume historical data transfer” requests from the subscribing PGs via DB. The function shall only respond to requests from known PGs with valid subscriptions. The function shall respond to “resume historical data transfer” requests from known PGs by authenticating requesting PG, validating the request, and resuming the data transfer to the requesting PG. The function shall resume the data transfer based on the traffic management policy and the actual traffic through the PG and DB. The function shall set the status of the subscription to “data transfer resumed” after received the confirmation that the subscribing PG is receiving the data again. The function shall provide means to alert PG administrators of publishing and subscribing PGs and DB administrator for any unsuccessful resuming of the data transfer. The function shall send a “PG unknown/Invalid Subscription” message to DB along with the requests for all the requests from unknown PGs and/or with invalid subscriptions.

4.2.2.5 Historical data subscription

PG-110. PG shall provide a function for inquiring accessible historical data from other PGs through DB NDS. The function shall be able to obtain accessible historical data information from publishing PGs by sending an “accessible historical data” request to DB either as a general query or as a targeted query with the targeted PG IDs, and receiving and storing signal IDs of the accessible historical data from publishing PGs along with publishing PGs’ IDs. For unknown PGs, the function shall obtain PG registration information of those PGs from DB NDS and store them for future PG authentication purpose.

PG-111. PG shall provide GUIs and related functions for PG administrator to initiate “accessible historical data” requests to DB. The GUIs and functions for initiating the requests shall enable PG administrator to include lists of PGs to be included/excluded in a request.

PG-112. PG shall provide a function for PG to automatically initiate the “accessible historical data” request to DB, and receiving and storing signal IDs for accessible historical data from publishing PGs via DB. For unknown PGs, the function shall obtain PG identification information from DB NDS and store them automatically for future PG authentication purpose.

PG-113. PG shall provide GUIs and functions for PG administrator to configure the automated initiation of “accessible historical data” requests to DB. The GUIs and functions shall enable PG administrator to enable/disable the automated initiations, set time interval that PG shall generate a request if enabled for timed request, and set various conditions of the requests, such as included/excluded PGs lists, abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up multiple automated initiation requests.

PG-114. PG shall provide GUIs and related functions for PG administrator to obtain detailed signal information using obtained signal IDs either from DB NDS or from publishing PG directly.

PG-115. PG shall provide a function for PG to automatically obtain detailed signal information using obtained new signal IDs from DB NDS and store these information for future use.

PG-116. PG shall provide functions for setting up subscriptions of selected historical data signals with the publishing PGs.

PG-117. PG shall provide GUIs and related functions for PG administrator to create subscription requests for historical data signals and send the requests to publishing PGs. The GUIs and functions shall enable PG administrator to select signals and length of the data for a subscription, and set the data service class and specific QoS requirements for the subscription. PG shall also provide a function for obtaining a subscription ID for the subscription from DB's subscription ID generation and management function, communicating with publishing PG to setup the subscription, and confirming to DB subscription management function of the successful setup. It shall also receive a cryptographic subscription key from DB which is different from all publishing and subscription keys of the active subscriptions.

PG-118. PG shall provide a function to automatically create subscription requests for historical data signals and send the requests to publishing PGs. The function shall enable PG to automatically select signals for a subscription, and set the data service class and specific QoS requirements for the subscription. PG shall also provide a function for obtaining a subscription ID for the subscription from DB's subscription ID generation and management function, communicating with publishing PG to setup the subscription, and confirming to DB subscription management function of the successful setup. It shall also receive a cryptographic subscription key from DB which is different from all publishing and subscription keys of the active subscriptions.

PG-119. PG shall provide GUIs and functions for PG administrator to configure the automated subscription request generation function. The GUIs and functions shall enable PG administrator to enable/disable the subscription request generation, and to set various conditions for creating the requests, such as creating a request upon receiving subscription request from connected devices/applications on PG_REQUESTER's own network side, etc., and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated generation of multiple subscription requests different from each other.

PG-120. PG shall provide GUIs and related functions for PG administrator to start the data delivery of an established subscription for historical data signals by sending a "start" request with the subscription's ID to the publishing PG using the method provided by the publishing PG through the subscription setup process. The GUIs and functions shall enable PG administrator to select a particular subscription to start, confirm to publishing PG that it is receiving the data, and set the status of the subscription to "delivering".

PG-121. PG shall provide a function to automatically start the data streaming of an established subscription for historical data signals by automatically sending a “start” request with the subscription’s ID to the publishing PG using the method provided by the publishing PG through the subscription setup process. The function shall enable PG to start a particular subscription, confirm to publishing PG that it is receiving the data of the subscription, and set the status of the subscription to “delivering”.

PG-122. PG shall provide GUIs and functions for PG administrator to configure the automated start of the data delivery of an established subscription. The GUIs and functions shall enable PG administrator to enable/disable the automated start function, and to set various conditions for creating the request, such as creating a request upon receiving a “start” request of the subscription from connected devices/applications on PG_REQUESTER’s own network side, etc., and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated start of multiple subscriptions.

PG-123. PG shall provide GUIs and related functions for PG administrator to pause the data delivery of an established subscription for historical data signals by sending a “pause” request with the subscription ID to publishing PGs using the method provided by the publishing PG through the subscription setup process. The GUIs and functions shall enable PG administrator to select a particular subscription to pause, confirm to publishing PG that the data has stopped coming, and set the status of the subscription to “paused”.

PG-124. PG shall not provide a function to automatically pause the data delivery of an established subscription for historical data signals.

PG-125. PG shall provide GUIs and related functions for PG administrator to resume the delivery of a paused subscription for historical data signals by sending a “resume” request with the subscription ID to publishing PGs using the method provided by the publishing PG through the subscription setup process. The GUIs and functions shall enable PG administrator to select a particular paused subscription to resume, confirm to publishing PG that the data has started coming, and set the status of the subscription to “delivering”.

PG-126. PG shall provide GUIs and related functions for PG administrator to cancel an established subscription for historical data signals by sending a “cancel subscription” request with the subscription ID to the publishing PG. The GUIs and functions shall enable PG administrator to select a particular subscription to cancel, confirm to publishing PG that indeed that it want to cancel the subscription, and set the status of the subscription to “cancelled” after received publishing PG’s confirmation of cancellation.

PG-127. PG shall provide a function to automatically cancel an established subscription for historical data signals by automatically sending a “cancel subscription” request with the subscription’s ID to the publishing PG. The function shall enable PG to cancel a particular subscription with a status of “active”, confirm to publishing PG that indeed that it wants to cancel the subscription, and set the status of the subscription to “cancelled” after received publishing PG’s confirmation of cancellation.

PG-128. PG shall provide GUIs and functions for PG administrator to configure the automated cancellation of an established subscription for historical data signals. The GUIs and functions shall enable PG administrator to enable/disable the automated cancellation function, and to set various conditions for creating the cancellation request, such as creating a request upon receiving the last “cancel subscription” request from connected devices/applications on PG_REQUESTER’s own network side that were data users of the subscription, and abnormal situation handling, etc. The GUIs and functions shall enable PG administrator to set up automated cancellation of multiple subscriptions.

4.2.3 Phasor Gateway traffic management

PG supplied by the PG_SUPPLIER shall meet the following PG traffic management functional requirements.

PG-129. PG shall provide an accurate timing source with an accuracy of ±1 µs for traffic QoS monitoring and traffic management functions. The timing source shall be highly stable (drift less than 1 µs per hour) and reliable.

4.2.3.1 NASPInet internal traffic QoS monitoring

PG-130. PG shall provide internal traffic QoS monitoring functions for all internal NASPInet traffic. The internal traffic include all data traffic between publishing PGs’ distribution component and subscribing PGs’ ingest components, and administrative traffic between PGs and DB components/services,

PG-131. Publishing PG shall provide an internal data traffic time recording function for departing data packets. The function shall be able to record the accurate time when a data packet leaves from the distribution component of a publishing PG on DB network side. The time shall be recorded along with sufficient information to uniquely identify the data packet, such as the subscription number and the timing tag of the data packet for a real-time streaming data packet.

PG-132. Subscribing PG shall provide an internal data traffic time recording function for arriving data packets. The function shall be able to record the accurate time when a data packet arrives at the ingest component of a subscribing PG on DB network side. The time shall be recorded along with sufficient information to uniquely identify the data packet, such as the subscription number and the timing tag of the data packet for a real-time streaming data packet.

PG-133. Subscribing PG shall provide an internal data traffic latency measurement function. The function shall be able to determine the accurate latency of received data packet by obtaining the time of the data packet when it left the distributor component of the publishing PG, and subtracting it from the time it arrives the subscribing PG.

PG-134. Subscribing PG shall provide a function for logging internal data traffic QoS related information for received data packets. The function shall log all anomalies of the received data packets, such as the bad data packets, the missing data packets, occurrences that data packets arrived in wrong order, and so on.

PG-135. Subscribing PG shall provide a reporting function for reporting the statistics of the QoS of the received data packets.

PG-136. Subscribing PG shall provide an alarming function for generating alarms under predefined QoS anomaly conditions.

PG-137. Subscribing PG shall provide GUIs and related functions for PG administrator to configure QoS monitoring and the alarm functions.

PG-138. Subscribing PG shall provide a function for responding to DB instrumentation service's request for internal data traffic QoS information.

PG-139. Subscribing PG shall provide a function for automatically sending internal data traffic QoS information to DB instrument service.

PG-140. Subscribing PG shall provide GUIs and related functions for PG administrator to configure the automated internal data traffic QoS information sending functions.

4.2.3.2 NASPInet external traffic QoS monitoring

PG-141. Publishing PG shall provide external traffic QoS monitoring functions for all traffic external to NASPInet. The external traffic include all data traffic between publishing PGs' ingest component and the data source devices.

PG-142. Publishing PG shall provide an external data traffic time recording function for arriving data packets. The function shall be able to record the accurate time when a data packet arrives at the ingest component of a publishing PG on PG_REQUESTER's own network side. The time shall be recorded along with sufficient information to uniquely identify the data packet, such as the device number and the timing tag of the data packet for a real-time streaming data packet.

PG-143. Publishing PG shall provide an external data traffic latency measurement function. The function shall be able to determine the accurate latency of received data packet by subtracting the time (from its time tag of the data packet) from the time it arrives at the publishing PG.

PG-144. Publishing PG shall provide a function for logging external data traffic QoS related information for received data packets. The function shall log all anomalies of the received data packets, such as the bad data packets, the missing data packets, the time that data packets arrived in wrong order, and so on.

PG-145. Publishing PG shall provide a reporting function for reporting the statistics of the QoS of the received data packets from external data traffic.

PG-146. Publishing PG shall provide an alarm function for generating alarms under predefined QoS anomaly conditions of the external data traffic.

PG-147. Publishing PG shall provide GUIs and related functions for PG administrator to configure the alarm functions of the external data traffic.

PG-148. Publishing PG shall provide a function for responding to DB instrumentation service's request for external data traffic QoS information.

PG-149. Publishing PG shall provide a function for automatically sending external data traffic QoS information to DB instrument service.

PG-150. Publishing PG shall provide GUIs and related functions for PG administrator to configure the automated external data traffic QoS information sending functions.

4.2.3.3 Phasor Gateway performance monitoring

PG-151. PG shall provide PG performance monitoring functions for all data traffic going through the PG. The PG performance monitoring functions shall monitor the PG performance for all data traffic from receiving at PG to departing from PG.

PG-152. PG shall provide a PG data traffic processing time measurement function. The function shall be able to determine the accurate time that PG used to process a data packet by subtracting the time when it is received by PG Ingest from the time when it is delivered by PG Distributor.

PG-153. PG shall provide a PG data traffic processing time recording function for processed data packets. The time shall be recorded along with sufficient information to uniquely identify the data packet, such as the device number and the timing tag of the data packet for a real-time streaming data packet.

PG-154. PG shall provide a function for logging PG performance anomalies related information for processed data packets. The function shall log all anomalies of the processed data packets, such as the dropped packets due to insufficient processing time, and so on.

PG-155. PG shall provide a reporting function for reporting the statistics of the PG performance anomalies of the processed data packets.

PG-156. PG shall provide an alarm function for generating alarms under certain PG performance anomaly conditions.

PG-157. PG shall provide GUIs and related functions for PG administrator to configure the PG performance anomaly alarm functions.

PG-158. PG shall provide a function for responding to DB instrumentation service's request for PG performance anomaly information.

PG-159. PG shall provide a function for automatically sending PG performance anomaly information to DB instrument service.

PG-160. PG shall provide GUIs and related functions for PG administrator to configure the automated PG performance anomaly information sending functions.

4.2.3.4 Traffic management

PG-161. PG shall provide traffic management functions for PG Ingest and Distributor to manage the data traffic according to the PG traffic management policies. PG traffic management functions shall include both normal operation traffic management functions and emergency mode traffic management functions according to corresponding traffic management polices.

PG-162. PG shall provide GUIs and related functions for PG administrator to configure the PG traffic management policies. The GUIs and related functions shall enable PG administrator to create, revise, and remove traffic management policies. The GUIs and related functions shall allow PG administrator to, as a minimum, assign/change traffic priorities to data service classes on an individual class basis. The GUIs and related functions shall also enable PG administrator to specify the automated policy changes in response to changes in resources status, PG loading and NASPInet DB loading. For example, lower the priority further or pause/drop the traffic completely for historical data classes when the network throughput is severely curtailed due to the loss of a major network link or equipment.

PG-163. PG shall provide a function for receiving NASPInet global traffic management policies from DB.

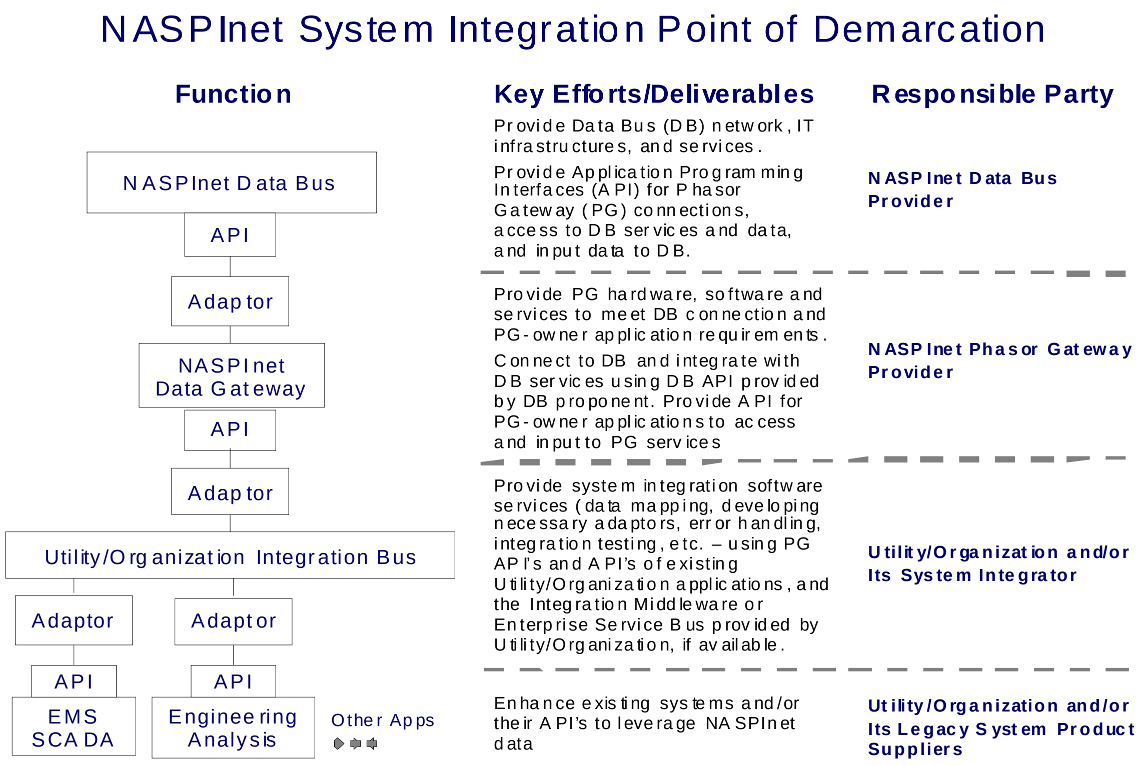
PG-164. PG shall provide a function to log the traffic management policies and the policy changes for use in NASPInet traffic and performance analysis. The function shall log the policy and policy change with accurate time tagging.

5 System Integration Requirements

This section describes the system integration requirements of the PG system and/or the PG_SUPPLIER such that the PG will function in concert with the DB and other PG_REQUESTER systems to enable the overall NASPInet and PG functions described in Sections 3 and 4 above.

5.1 Point of Demarcation

Figure 5-1 outlines the roles and responsibilities of the PG_SUPPLIER versus the DB_SUPPLIER and other related parties. Basically, the DB_SUPPLIER shall provide a set of Application Programming Interfaces (API) to facilitate PG connection and integration of PG/DB services. The PG_SUPPLIER shall (1) integrate the PG with the DB using the DB_SUPPLIER provided APIs and (2) provide the APIs for other PG_REQUESTER IT systems and applications to access the PG services and for data integration between the PG and those PG_REQUESTER systems. PG_REQUESTER or its selected System Integrator, if applicable, shall use the PG_SUPPLIER-supplied APIs to integrate the PG_REQUESTER systems with the PG. The required DB APIs and PG APIs are listed in Sections 5.3.1 and 5.3.2 respectively.



NASPInet System Integration Point of Demarcation

Key Efforts/Deliverables	Responsible Party
Provide Data Bus (DB) network, IT infrastructures, and services. Provide Application Programming Interfaces (API) for Phasor Gateway (PG) connections, access to DB services and data, and input data to DB.	NASPInet Data Bus Provider
Provide PG hardware, software and services to meet DB connection and PG-owner application requirements. Connect to DB and integrate with DB services using DB API provided by DB proponent. Provide API for PG-owner applications to access and input to PG services	NASPInet Phasor Gateway Provider
Provide system integration software services (data mapping, developing necessary adaptors, error handling, integration testing, etc. – using PG API's and API's of existing Utility/Organization applications, and the Integration Middleware or Enterprise Service Bus provided by Utility/Organization, if available.	Utility/Organization and/or Its System Integrator
Enhance existing systems and/or their API's to leverage NASPInet data	Utility/Organization and/or Its Legacy System Product Suppliers

Figure 5-1 System Integration Role & Responsibility of PG and DB providers and others

5.2 System Integration Services

As stated in Section 5-1 above, as part of the PG implementation services, the PG_SUPPLIER shall connect the PG to the DB and integrate with the DB services using the Application Programming Interfaces (API) to be provided by the DB_SUPPLIER. In addition, the PG_SUPPLIER shall provide all APIs specified in Section 5.3.3 below, along with all necessary design documentation, configuration and application guides, etc., and is expected to support PG_REQUESTER in integrating its existing systems and applications with the PG.

The overall integration services of the PG_SUPPLIER shall include the following efforts as a minimum:

1. Provide specific constraints on technical architecture and standards as distilled from functional requirements (Sections 3 and 4). Document the overall set of technical requirements and standards compliance/impacts on PG_REQUESTER systems and applications.

2. Facilitate the development and documentation of <u>detailed</u> functional and technical requirements for each system interface. Functional requirements shall include detailed use cases and information requirements to support those use cases. Technical requirements shall include response time, scalability, security, and availability requirements.

3. Document integration requirements including detailed system integration design and detailed PG configurations needed to support the DB integration.

4. Provide detailed integration design documenting the technical and physical architecture of the integrated PG environment. Compile documentation for each system interface, including input/output data mapping, data transformation, adaptors, enterprise service/message mapping, frequency and latency, expected transaction rates and performance requirements, data validation and exception handling, etc. The designs will consider integration requirements for both analytic and transaction processing.

5. Develop and document the configuration design, and design of any customization or enhancements needed, of the PG to support integration with the DB and PG_REQUESTER systems/applications. The design will cover on-line and batch processing as well as specific requirements for operational reporting and analytics.

6. Configure the PG to support the DB integration. Develop any PG customizations and enhancements needed to support the DB and PG_REQUESTER application integration, per the design document, and deliver the end product to PG_REQUESTER.

7. Implement PG interfaces and adaptors per the detailed design specifications.

8. See Section 11, Implementation and Sustainment Services, regarding the installation, testing, training, documentation, and other service requirements.

5.3 Application Programming Interfaces

The PG_SUPPLIER shall deliver APIs for their products as outlined in below, including software, documentation, and sample test data sets.

5.3.1 Common API Requirements

5.3.1.1 Security

All API functions shall enable security assurance for appropriate access to and usage of NASPInet resources and information, including authentication and authorization, encryption and decryption of API and response data, audit trail, etc. All security violations, such as a failed authentication or authorization, shall be logged, and the DB System Administrator as well as the corresponding PG Administrator would be notified of the event.

5.3.1.2 Error Handling and Error Tolerance

All APIs shall include appropriate error and exception handling and have the ability to insulate the system from data errors sent through the API and from problems occurred in other systems. In other words, the system shall continue to function normally in all areas not directly associated with the data from the API and not directly relying on the functions of the faulted external system. All interface errors shall be time stamped, error coded, and logged.

5.3.1.3 API Results Confirmation

All APIs shall reply to the requesting system with a success/failure code. The success code may be CREATED, CANCELED, CHANGED, etc. The error code should provide a reason for the failure (e.g. "invalid data field XXX". "Device ID not recognized", etc.)

5.3.2 Data Bus API

This Section is for PG_SUPPLIER information only. The DB_SUPPLIER is expected to provide the following APIs for PGs to access DB data and services. The DB_SUPPLIER is expected to provide details of the API constructs as part of the DB project.

5.3.2.1 System Management/Common Services API

This set of APIs is intended for managing the administration of connecting PGs, devices, and signals. They shall follow IEC 61970 Interface Standards, Part 402, Common Services.

5.3.2.1.1 Create PG Registration API

The DB API shall allow a PG to provide data that can be used to identify itself to the DB to facilitate the PG registration with the DB Name Services. The PG registration data may include the following for example:

- Physical location of the PG (Country, State, etc.)
- Owner information (company name, type of organization, region, address, etc.)
- System administrator information (name, email, phone, SMS address, etc.)
- PG functions – subscribe only, publish and subscribe, highest class of data services to be supported (latency, availability, sampling rate), etc.
- Default data access rights by organization type, region, and class of data
- Data access right exceptions (list of PG IDs and their owner organization names with specific access right by data class for each PG/owner)
- Authentication information

Upon authenticating the owner information, validating the owner authority to connect PG to NASPInet, and checking for logical registration data errors, the DB API shall return a message to the PG with "CREATED" and a unique PG ID assigned by the NASPInet Name & Directory Services. If errors occur in the registration process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.2 Change PG Registration API

The DB API shall allow a PG to change data of the existing PG registration (see example data in the Create PG Registration API) with the DB Name & Directory Services. The API shall automatically stop any data ingests through the registered PG before making the change and provide a message to the PG requesting restart of the data ingests.

In addition to the new registration data, the PG must also provide via the API the unique PG ID assigned during the registration process along with the authentication information provided with the registration. If the changes are successful, the API will return a message "CHANGED" to the PG. If errors occur in the process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.3 Cancel PG Registration API

The DB API shall allow a PG to remove itself from the registration with the DB Name Services. Upon proper authentication and authorization checks, the API shall automatically stop any data ingests through the registered PG before deleting the registration. The DB shall automatically cancel the registrations of all PMU/PDC devices and signals connected via the PG. This API shall also allow deletion from an authorized 3rd party source, such as the PG owner through an external user interface application.

Note that all registration records should be archived in the DB server. This API would deactivate the PG and remove its entry in the NASPInet Name & Directory Service, so no NASPInet services can be accessed after processing of the API.

The PG or requesting application must provide via the API the unique PG ID assigned during the registration process along with the authentication information provided with the registration. If the cancelation is successful, the API will return a message “CANCELED” to the PG or requesting application along with a list of Device IDs and Signal IDs that have been automatically canceled. If errors occur in the process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.4 Create Device Registration API

The DB API shall allow a PG to register, with the DB Name & Directory Services, a PMU/PDC device connected to the PG. The same API shall be able to support registering a PDC. The registration data may include the following for example:

- PG ID
- Device owner information
- Physical location of the device (Country, State, etc.)
- Location identification (substation name, etc.)
- Type of device (PMU, PDC, etc.)
- Device identification (owner organization name, device name, sequence number, etc.)
- Device configuration (physical & logical)
- Highest signal quality supported (data class – latency, reliability, etc.)
- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Authentication information

Upon authenticating the PG and owner information and checking for logical registration data errors (e.g. the highest signal quality supported must be below the highest level supported by the PG), the DB API shall return a message to the PG with “CREATED” and a unique Device ID assigned by the NASPInet Directory & Name Services. If errors occur in the registration process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.5 Change Device Registration API

The DB API shall allow a PG to change data of an existing PMU/PDC device registration with the DB Name & Directory Services. Upon proper authentication and authorization checks, the API shall automatically stop any data ingests from the PMU/PDC before making the change and provide a message to the PG requesting restart of the data ingests.

In addition to the new registration data (see Create Device Registration API for sample data), the PG must also provide via the API the unique PG ID and Device ID assigned during the registration process along with the authentication information provided with the registration. If the changes are successful, the API will return a message "CHANGED" to the PG. If errors occur in the process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.6 Cancel Device Registration API

The DB API shall allow a PG to remove an existing PMU/PDC device registration with the DB Name & Directory Services. Upon proper authentication and authorization checks, the API shall automatically stop any data ingests of all data signals connected to the registered PMU/PDC device and cancel the registration of these data signals before canceling the device registration.

Note that all registration records should be archived in the DB server. This API would deactivate the Device and remove its entry in the NASPInet Name & Directory Service.

The PG must provide via the API the unique PG ID and Device ID assigned during the registration process along with the authentication information provided with the registration. If the cancelation is successful, the API will return a message "CANCELED" to the PG along with a list of all registered signals that have been automatically canceled. If errors occur in the process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.7 Create Data Signal Registration API

The DB API shall allow a PG to add a data signal from a registered PMU/PDC that will be available through NASPInet. The registration data may include the following for example:

- PG ID
- Device (PMU/PDC) ID
- Complete signal description (type of signal, reporting rate, data format, etc.)
- Signal origin (e.g., original PMU signal that a PDC signal is derived from)
- Signal source (measurement CT/PT, source devices, etc.)
- Signal processing methods (if not original signal)

- Signal quality (data class – latency, reliability, etc.)
- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Authentication information

Upon authenticating the PG and Device ID and checking for logical registration data errors (e.g. the signal quality must be below the highest level supported by the registered PG and Device), the DB API shall return a message to the PG with "CREATED" and a unique Signal ID assigned by the NASPInet Name & Directory Services. If errors occur in the registration process, the API shall return an error code and log the error in the Data Bus.

5.3.2.1.8 Cancel Data Signal Registration API

The DB API shall allow a PG to cancel a data signal from a registered PMU/PDC device that will be available through NASPInet. Upon proper authentication and authorization checks, the API shall automatically stop any data ingests from the data source before canceling the registration.

Note that all registration records should be archived in the DB server for auditing purposes. This API would deactivate the Signal and remove its entry in the NASPInet Name & Directory Service.

The PG must provide via the API the unique PG ID, Device ID, and Signal ID assigned during the registration process along with the authentication information provided with the registration. If the cancelation is successful, the API will return a message "CANCELED" to the PG. If errors occur in the process, the API shall return an error code and log the error in the Data Bus.

5.3.2.2 Streaming Data API

This set of APIs is intended for enabling the operational functions associated with streaming data. They shall follow IEC 61970 Interface Standards, Part 404, High-Speed Data Access.

5.3.2.2.1 Show Streaming Data API

The DB API shall enable the DB to request one or more streaming data signals from a registered PMU/PDC device through its owner PG to start ingesting through the DB to NASPInet. The DB shall provide the following information through the API:

- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs
- Requester PG ID
- Authentication information

- Encryption/decryption information
- Date/time of request

Upon authentication of the request, the source data PG will start ingesting the requested signal data to the DB – if the request is the first request for the data signal. The data source PG shall return a “STARTED” message to the DB. The streaming data will continue until a cancelation is received for all active requests.

The DB shall automatically encrypt the streaming signal at the data entry node and decrypt it at data receiving nodes.

5.3.2.2.2 Cancel Streaming Data API

The DB API shall enable the DB to stop ingesting data from one or more registered PMU/PDC data signals through the DB to NASPInet. The DB shall provide the following information through the API:

- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs
- Requester PG ID
- Authentication information
- Date/time of request

The DB shall authenticate the Requester PG before sending the request to the Source Data PG. Upon authentication of the request, the Source Data PG will stop ingesting the requested signal data to the DB – if the request is the last request of the data signal. The PG shall return a message “CANCELED” to the DB.

5.3.2.2.3 Subscribe Streaming Data API

The DB API shall allow a PG to subscribe to data from one or more registered PMU/PDC data signals on the NASPInet through the DB. The API shall include provisions for selecting the data source signals and specifying the desired sampling rate for potential future NASPInet enhancements. The PG shall provide the following information via the API:

- Requester PG ID
- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs

- Authentication information
- Data quality desired (data rate, etc.)
- Date/time of request

The DB shall authenticate the requester PG and check its data access authorization against the data source PG records before sending the request to the data source PG. Upon authentication of the request and data from the data source, the DB shall publish the streaming data to the requester PG.

The receiving node of the Requester PG shall decrypt the data from the Source PG and encrypt the data with a key that is specific to the streaming data subscription request. The DB API shall return a message “STARTED” with the decryption key to the Requester PG. If the streaming data is not successful, the DB API shall return an error code to the Requester PG.

5.3.2.2.4 Unsubscribe Streaming Data API

The DB API shall allow a PG to cancel an existing subscription of data from one or more registered PMU/PDC data signals. This API shall also allow the unsubscription request from an authorized 3rd party source, such as the PG owner or site administrator through an external user interface application. The PG shall provide the following information via the API:

- Requester PG ID
- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs
- Authentication information
- Date/time of request

The DB shall authenticate the Requester PG and verify the unsubscribe request before sending the request to the data source PG. Upon confirmation of cancelation from the data source PG, the DB shall return a “CANCELED” message to the requester PG.

5.3.2.2.5 Browse Available Streaming Data API

The DB API shall allow a PG to get a list of available streaming data sources that it has access to through the DB Name & Directory Service. The PG shall send the following information via the API:

- Requester PG ID
- Authentication information

- Requester information (organization name, etc.)
- Organization and region of data of interest
- Signal types of data of interest

The DB shall authenticate the Requester PG and return with an error code, “NULL” if no data is available that the Requester PG has authority to access, or a list of data sources available, including source data PG ID and owner information, Device ID and location information, Signal ID, data types, and data quality (reliability, data rate, etc.)

5.3.2.3 Historical Data API

This set of APIs is intended for enabling access to historical data stored in data sources available to NASPInet. They shall follow IEC 61970 Interface Standards, Part 407, Time Series Data Access.

5.3.2.3.1 Browse Historical Data API

The DB API shall allow a PG to get a list of available historical data sources through the DB Name & Directory Service. The PG shall send the following information via the API:

- Requester PG ID
- Authentication information
- Requester information (organization name, etc.)
- Organization and region of data of interest
- Signal types of data of interest
- Begin and end date/time of data of interest

The DB shall authenticate the requester PG and return with an error code, “NULL” if no data is available that the Requester PG has authority to access, or a list of data sources available, including source data PG ID and owner information, Device ID and location information, Signal ID, data types, time period when historical data is available, and format of available data.

5.3.2.3.2 Get Historical Signal Data API

The DB API shall allow a PG to request historical data available from an external PG for a specified data source/signal, PMU/PDC (including all data signals connected to the PMU/PDC), or the external PG (including all PMU/PDCs and all their data sources) for a specified period of time. The requester PG or application shall provide the following information via the API:

- Requester PG ID

- Authentication information
- Data source PG ID
- PMU/PDC Device ID
- Signal IDs
- Begin and end date/time

The DB shall authenticate the requester PG before sending the request to the source data PG. The source data PG shall return with a historical request ID and data-available period, which DB shall forward to the requester PG. (Note: The historical data will be in whatever format is available. The DB is not required to do any data conversions.)

5.3.2.3.3 Start Historical Data Transmission API

The API shall enable a PG to start transmission of the requested historical data. The PG will provide the historical data request ID along with information needed for its authentication.

Upon authentication of the request, DB will send the request to the source data PG to start the historical data transmission. The transmission will continue until the requested data is completely transferred or until a pause or cancel command is received.

5.3.2.3.4 Pause Historical Data Transmission API

The API shall enable a PG to pause an ongoing historical data transmission. The PG will provide the historical data request ID along with information needed for its authentication.

Upon authentication of the request, DB shall send the request to the source data PG to pause the historical data transmission.

5.3.2.3.5 Resume Historical Data Transmission API

The API shall enable a PG to resume a paused historical data transmission. The PG will provide the historical data request ID along with information needed for its authentication.

Upon authentication of the request, DB shall send the request to the source data PG to resume the historical data transmission.

5.3.2.3.6 Cancel Historical Data Transmission API

The API shall enable a PG to cancel a historical data request. The PG will provide the historical data request ID along with information needed for its authentication.

Upon authentication of the request, DB shall send the request to the source data PG to cancel the historical data request. If there is ongoing data transmission for the requested historical data, the source PG shall stop start the historical data transmission.

5.3.2.4 System Performance Management API

This set of APIs is intended for enabling access to data related to the Quality of Services history and system events of NASPInet.

5.3.2.4.1 Get NASPInet QoS Data API

The DB API shall allow a PG to query the DB for the quality of service measures within the DB and NASPI network for a specified data signal, PMU/PDC device (including all data signals connected to the PMU/PDC), or the PG (including all PMU/PDCs and all their data sources) over a specified period of time.) The DB will authenticate the requested PG and return the requested information to the PG. This API shall follow IEC 61970 Interface Standards, Part 403, Generic Data Access.

5.3.2.4.2 Get PG QoS Data API

The DB API shall allow the DB system administrator or application to query a PG for the quality of service measures on the PG side of the overall system for a specified data signal, PMU/PDC device (including all data signals connected to the PMU/PDC), or the PG (including all PMU/PDCs and all their data sources) over a specified period of time.) The PG is expected to authenticate the request and return the requested information to the DB. This API shall follow IEC 61970 Interface Standards, Part 403, Generic Data Access.

5.3.2.4.3 Get Transaction and Error Log API

The DB API shall allow a PG to query the DB for obtain a digital copy of the log of transactions and errors associated with the PG over a specified period of time. This API shall also allow queries from an authorized 3rd party source, such as the PG owner or site administrator through an external user interface application. The DB will authenticate the requested PG and email the requested information to the PG System Administrator that has been registered with the PG. This API shall comply with IEC 61970 Interface Standards, Part 403, Generic Data Access.

5.3.2.4.4 Subscribe Event Notification API

The DB API shall allow a PG to receive notifications of events associated with the PG, on event driven basis. The notification shall include originator of the event, timestamp, and type of event. The type of event may include, for example, (a) new device visible but not registered and provisioned for NASPInet, (b) an intrusion attempt through the PG, (c) a fatal error detected in an attempted API/transaction, etc. The DB will authenticate the requested PG and send the requested information to the PG System

Administrator (via email and/or SMS) that has been registered with the PG. This API shall comply with IEC 61970 Interface Standards, Part 405, Generic Eventing and Subscription.

5.3.3 Phasor Gateway API

The PG_SUPPLIER shall provide APIs for interfacing the PG with other PG_REQUESTER systems and applications. The APIs shall include the following as a minimum. The API function requirements are listed below. The PG_SUPPLIER shall describe details of the API constructs. Please see Sections 3 and 4 for data requirements.

5.3.3.1 System Management/Common Services API

This set of APIs is intended for managing the administration of connecting PMU/PDC devices and signals to NASPInet via the PG. They shall follow IEC 61970 Interface Standards, Part 402, Common Services. It is assumed that canceling a device or signal registration would not be done via an external application of information source, hence no API is needed for that purpose.

5.3.3.1.1 Create-Change Device Registration API

The PG API shall allow inputs of information needed for NASPInet/DB registration of a PMU/PDC from an authorized 3rd party source, such as an external user interface application or from the PMU/PDC when the PG and PMU/PDC have the self discovery/self registering capabilities.

The registration data may include the following for example:

- PG ID
- Device owner information
- Physical location of the device (Country, State, etc.)
- Location identification (substation name, etc.)
- Type of device (PMU, PDC, etc.)
- Device identification (owner organization name, device name, sequence number, etc.)
- Device configuration (physical & logical)
- Highest signal quality supported (data class – latency, reliability, etc.)
- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Authentication information

After validation of the registration data and authentication information, the PG shall determine whether the registration is new or existing and shall accordingly either issue a “create device registration” or "change device registration" via the corresponding DB API as described in the DB API subsection above. The PG shall expect a confirmation message with "CREATED" and a unique Device ID as assigned by the NASPInet Directory and Name Services, or "CHANGED" for a changing registration request. If the registration creation or change is not successful, the PG shall expect an error code from the DB. It shall process the error code and send a notification message to the PG system administrator.

5.3.3.1.2 Create-Change Data Signal Registration API

The PG API shall allow inputs of information needed for NASPInet/DB registration of a PM data signal from an authorized 3rd party source such as an external user interface application or from an Intelligent Electronic Device (IED) directly when the PMU/PDC/IED have the self discovery/self registering capabilities.

The registration data may include the following for example:

- PG ID
- Device (PMU/PDC) ID
- Complete signal description (type of signal, reporting rate, data format, etc.)
- Signal origin (e.g., original PMU signal that a PDC signal is derived from)
- Signal source (measurement CT/PT, source devices, etc.)
- Signal processing methods (if not original signal)
- Signal quality (data class – latency, reliability, etc.)
- Signal access method through P-PG (1-to-1, 1-to-N, etc.)
- Authentication information

After validation of the registration data and authentication information, the PG shall determine whether the registration is new or existing and shall accordingly either issue a "create data signal registration" or "change data signal registration" via the corresponding DB API as described in the DB API subsection above. The PG shall expect a confirmation message with "CREATED" and a unique Signal ID as assigned by the NASPInet Directory and Name Services, or "CHANGED" for a changing registration request. If the registration creation or change is not successful, the PG shall expect an error code from the DB. It shall process the error code and send a notification message to the PG system administrator.

5.3.3.2 Streaming Data API

This set of APIs is intended for enabling the operational functions associated with streaming data. They shall follow IEC 61970 Interface Standards, Part 404, High-Speed Data Access.

5.3.3.2.1 Subscribe Streaming Data API

The PG API shall allow an external system or application to subscribe to one or more registered streaming PM data signals from a PMU/PDC device on the NASPInet. The PG shall input the following information through the API and forward the request to DB via the corresponding DB API upon authentication of the requester and verification of the request:

- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs
- Requester PG ID
- Authentication information
- Date/time of request

The PG shall expect from the DB a confirmation message with “STARTED” and a decryption key which the PG shall use to decrypt the data for the requesting application. If the streaming data request is not successful, the PG shall expect an error code, which it shall log in its event log and relay the error to the requesting application.

5.3.3.2.2 Unsubscribe Streaming Data API

The PG API shall allow an external application to cancel an existing subscription of one or more PM data signals. The PG shall allow input of the following information via the API and forward the request to DB via the corresponding DB API upon authentication of the requester and verification of the request:

- Requester PG ID
- Source Data PG ID
- Device (PMU/PDC) ID
- Signal IDs
- Authentication information
- Date/time of request

The PG shall expect from the DB a confirmation message with “CANCELED”. If the unsubscribe request is not successful, the PG shall expect an error code, which it shall log in its event log and relay the error to the requesting application.

5.3.3.2.3 Browse Available Streaming Data API

The PG API shall allow an external application to request a list of available streaming data sources that it has access to through the DB Name & Directory Service. The PG shall allow the input of following information via the API and forward the request to DB via the corresponding DB API upon authentication of the requester and verification of the request:

- Requester PG ID
- Authentication information
- Requester information (organization name, etc.)
- Organization and region of data of interest
- Signal types of data of interest

The PG shall expect from the DB API an error code, "NULL" if no data is available that the requester has authority to access, or a list of data sources available, including source data PG ID and owner information, Device ID and location information, Signal ID, data types, and data quality (reliability, data rate, etc.) The PG API shall provide the request result to the requesting application.

5.3.3.3 Historical Data API

This set of APIs is intended for enabling access to historical data stored in data sources available to NASPInet. They shall follow IEC 61970 Interface Standards, Part 407, Time Series Data Access.

5.3.3.3.1 Browse Historical Data API

The PG API shall allow an external application to request a list of available historical PM data sources that it has access to through the DB Name & Directory Service. The PG shall allow the input of following information via the API and forward the request to DB via the corresponding DB API upon authentication of the requester and verification of the request:

- Requester PG ID
- Authentication information
- Requester information (organization name, etc.)
- Organization and region of data of interest
- Signal types of data of interest
- Begin and end date/time of data of interest

The PG shall expect from the DB API an error code, "NULL" if no data is available that the requester has authority to access, or a list of data sources available, including source data PG ID and owner information, Device ID and location information, Signal ID, data types, time period when historical data is available, and format of available data. The PG API shall provide the request result to the requesting application.

5.3.3.3.2 Get Historical Signal Data API

The PG API shall allow an external application to request historical PM data available through NASPInet for a specified period of time. The PG shall allow the input of following information via the API and forward the request to DB via the corresponding DB API upon authentication of the requester and verification of the request:

- Requester PG ID
- Authentication information
- Data source PG ID
- PMU/PDC Device ID
- Signal IDs
- Begin and end date/time

The PG shall expect from the DB API an error code, “NULL” if no data is available, or a file containing the requested data. The PG API shall provide the request result to the requesting application. The file will be in whatever format is available at the data source. NASPInet is not expected to do any file and data conversions.

6 Networking and Communications Requirements

This section describes overall networking and communication requirements for NASPInet including the Phasor Gateway (PG) and Data Bus (DB) of NASPInet, and specific requirements for PG that connects to the NASPInet WAN and various devices (PMUs/PDCs) and applications on PG_REQUESTER network side. This section includes an overview of the overall networking and communication needs and requirements of the NASPInet. While the PG_SUPPLIERs are encouraged to use their standard, field proven system architecture and standard external system interfaces to the fullest extent possible, the proposed system interfaces **must** adhere to PG_REQUESTER's Information Technology (IT) standards and guidelines identified in this section.

6.1 Overall NASPInet Networking and Communications Requirements

As shown in Section 1 and Section 3 of this specification, the NASPInet consists of two major parts: the Phasor Gateways (PG) and the Data Bus (DB) that connects all PGs. The DB is the logical entity facilitating data transportation among connected PGs. A PG will be the portal for a connected entity that enables it to publish its own synchrophasor data to the DB and/or subscribe to data from other PGs through the DB.

All services and functionalities of NASPInet are provided through various PG specific components/services, DB specific components/services and common services of NASPInet as described in Section 2. All PGs and DB components are connected through a wide-area network (NASPInet WAN) to interact with each other for providing required functionalities and services. PGs also interface with their phasor data publishers/subscribers' own networks to forward the data received from publishers' networks to DB and the data received from DB to subscribers' networks.

PG-165. **Support all classes of data.** The NASPInet WAN and the PGs shall be able to simultaneously transport different classes of data and ensure the Quality of Service (QoS) requirements for each class. As a minimum, the NASPInet WAN and PGs shall support data classes with QoS requirements specified in 8.2.

PG-166. **Phased implementation.** The NASPInet WAN is expected to be built through multiple phases to be in step with the growth of the number of connected PGs, external devices such as PMUs/PDCs and the network traffic. The NASPInet WAN design shall enable a gradual build-out of the network in steps of the increase of the connected PGs, traffic growth and overall network reliability requirement change. The PG locations and their data requirements at different phases of NASPInet deployment are provided as Attachment I of DB's RFP for NASPInet WAN network design and provisioning.

PG-167. **Life expectancy**. The minimum life expectancy of the NASPInet WAN is 30 years.

The following describe networking and communications requirements for NASPInet WAN that connects DB and PGs, and for PGs, as well as PG's networking interface requirements.

6.2 Scope of the NASPInet Interfaces

PG-168. The NASPInet PG network interface with PG_REQUESTER WAN (NI2 as shown in Figure 6-1) shall support integration of several key components on PG_REQUESTER's network side, including, but not limited to the following:

- Integration with various types of PMU devices, such as standalone and multifunction PMU devices
- Integration with various types of Phasor Data Concentrators
- Integration with data archiving and storage devices/systems
- Integration with various types of utility applications, such as visualization, archiving, and control applications
- Integration with a variety of commercial enterprise systems (such as EMS/SCADA systems)

These application programming interfaces (API) to these components shall be provided through PGs' network interfaces to PG_REQUESTER's network. The design details of required API functionality and customization shall be finalized during the initial stages of the PG contract negotiation phase with PG_REQUESTER.

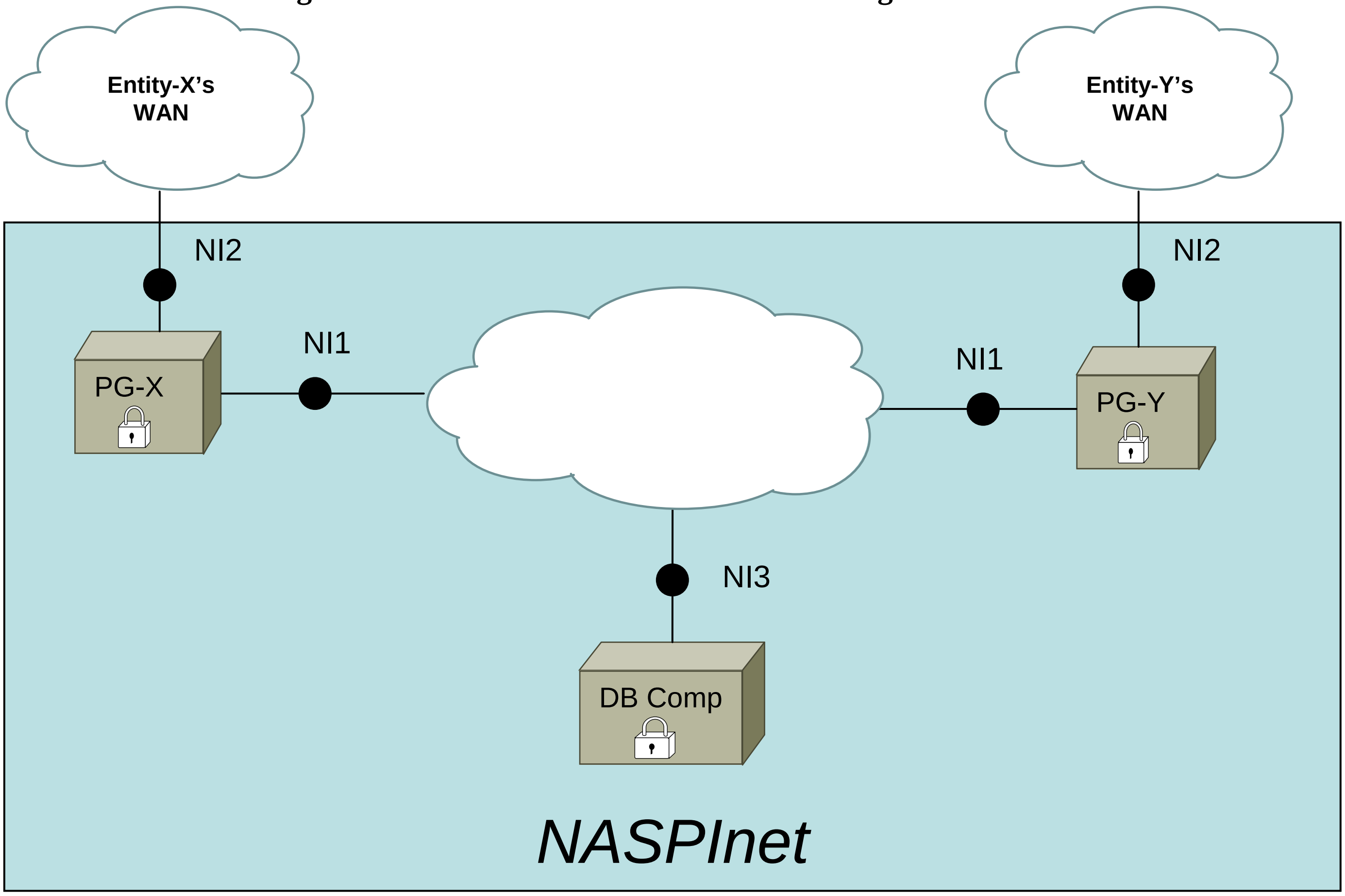
6.3 NASPInet WAN Requirements

The NASPInet WAN network shall be a private networking environment consisting of Local Area Networks (LANs) and Wide Area Networks backbone to interconnect the PGs and DB components, and employing, wherever practical, industry standards for hardware, software, and user interfaces. The goal of this type of "open" network architecture is to allow the addition of future functionality and the replacement of hardware without disruption to the NASPInet normal operation. The private network in this RFP is defined as that all network assets are owned and under the control of the owner. This shall include all physical components of the network including the routers or interconnectivity between PG and DB components.

The different NASPInet network interfaces are illustrated in Figure 6-1, NASPInet Network Interfaces Diagram. The diagram depicts at a high level the main interfaces that the PG_SUPPLIERs shall address with their response.

Specifications for the NASPInet WAN are part of the Data Bus specification. The PG must interface with NASPInet WAN as previously specified.

Figure 6-1: NASPInet Network Interfaces Diagram



6.4 PG Network Interfaces

As shown in Figure 6-1, PGs interface with both NASPInet WAN network and PG owner's own WAN network.

The traffic of PG network interface with NASPInet WAN network include:

- Published/subscribed data flows
- NASPInet data subscription administration traffic (PG/PMU/PDC registration, data subscription/unsubscription, and so on)
- NASPInet administration traffic (PG registration, and so on)
- NASPInet network management traffic (network performance monitoring, network configuration, network diagnose, etc.)

The traffic of PG interface with PG owner's network mainly include

- PG ingest data traffic (Data received from PMUs/PDCs in PG owner’s network to be published to NASPInet)
- PG distribution traffic (Data received from NASPInet to be delivered to applications, PDCs, data archives, etc. within PG owner’s network)
- PG device management traffic
- NASPInet data publication/subscription support administration traffic
- PG owner’s network management traffic

6.4.1 Independent Network Interfaces

The network interfaces of a PG to NASPInet WAN (NI1) and to its owner’s network (NI2) must be independent with each other to ensure a complete separation of its NASPInet traffic and its owner’s network traffic.

PG-169. **Physical separation.** The PG shall have physically separated network interface connections for connecting PG to NASPInet WAN network and to PG owner’s network. PG_SUPPLIERs shall provide a detailed description of such physical separation in its proposed PG design.

PG-170. **Independent Network Interface Administration.** The PG shall provide independent network interface administration for NASPInet WAN network interface and for PG owner’s network interface. Access to one interface’s administrator account shall not enable a user to perform the system configuration and administration for the other interface. PG_SUPPLIERs shall provide a detailed description of such independent administration implementation in its proposed PG network interface design.

6.4.2 PG – NASPInet WAN Network Interface NI1

The NI1 network interface between PG and NASPInet WAN shall meet the following requirements.

6.4.2.1 Interface Options

PG-171. **Default interface options.** The PG to NASPInet WAN network interface shall offer as minimum two default options: optical Ethernet interface option and galvanic Ethernet interface option.

PG-172. **Optical Ethernet interface option requirement.** The PG optical network interface option shall meet the following technical requirements. The interfaces shall provide interconnectivity from 300 meters to 80 kilometers.

Function	Value	
Applicable standard	IEEE 802.3u 100BASE-FX	IEEE 802.3z 1000BASE-SX
Communication speed	100 Mbps full-duplex	1000 Mbps full-duplex
Connectors	ST RX/TX Style connectors	ST RX/TX Style connectors
Cable	62.5/125 µm multi-mode fiber optic cable (glass)	50/100 µm multi-mode fiber optic cable (glass)
Optical wavelength	1270-1380 µm	850 nm
LED Indicators	Link Active, Receive Data, 100 MB/s, Transmit Data	Link Active, Receive Data, 100 MB/s, Transmit Data

PG-173. **Galvanic Ethernet interface option requirement.** The PG Galvanic network interface option shall meet the following technical requirements.

Item	Value	
Applicable standards	IEEE802.3u 100BASE-TX	IEEE802.3ab 1000BASE-T
Communication speed	100 Mbps for full-duplex	1000 Mbps for full-duplex
Connector	RJ-45	
Cable	2-Pair UTP Cat 5 up to 100m	2-Pair UTP Cat. 5, 5e, 6, and 7, up to 100m

PG-174. **Other interface options.** PG shall also be capable of supporting other network interface options for NI1 network interface through replacing network interface card, using protocol converters/gateways, and so on.

6.4.2.2 Network Protocols

PG-175. **IPv6/IPv4 network protocol support.** The PG NI1 interface shall support both IPv6 and IPv4 network protocols.

6.4.2.3 Redundancy and Hot-swap Capability

PG-176. **Data class based redundancy requirements.** PG NI1 network interface shall meet redundancy requirement in accordance to its supported data classes.

Class supported	Publishing	Subscribing
A	Redundant	Redundant
B	Redundant	Redundant
C	Redundant	Redundant
D	Non-redundant	Non-redundant
E	Non-redundant	Non-redundant
PG NI1 redundancy requirement	= Requirement for highest class supported	

PG-177. **No-interruption repair.** When redundant NI1 interface is required, the PG NI1 network interface hardware and software shall support no-interruption repair capability for replacing defective network interface hardware/software.

6.4.2.4 NI1 Network Interface Management

PG-178. **Network Interface Management**. The PG design shall include NI1 network interface management functionalities for configuration, monitoring, and diagnose the interface.

PG-179. **Network Interface diagnosis capabilities**. The PG design shall support local (on-site PG administrator) and remote (NASPInet WAN network administrator) diagnostics capable of detecting and autonomously alerting abnormal operating parameters in NASPInet network communications.

PG-180. **Network Interface Hardware Equipment diagnosis capabilities**. The PG design shall support local (on-site PG administrator) and remote (DB administrator) diagnostics capable of detecting and autonomously alerting abnormal interface's hardware equipment operating conditions including, but not limited to, memory failure, power supply degradation, microprocessors(s) failures (e.g. computer operating system watchdog events), firmware/software problems, excessive device temperature, etc.

6.4.2.5 Monitoring, Alarming and Reporting

PG-181. **Monitoring.** PG shall implement proper NI1 network interface monitoring functionalities for network traffic monitoring and network connection health assessment. The monitoring function shall monitor the real-time traffic volume, latency, dropped packets, corrupted packets, network interruptions, and other important network performance matrices. The monitoring function shall also collect and provide monitoring data for use by alarming and reporting functions.

The PG_SUPPLIER shall provide a detailed description of the implemented network interface monitoring functionalities, including methods to determine network traffic volume going through each port, transmission latency from publishing PG to subscribing PG, and so on.

PG-182. **Alarming.** PG shall implement NI1 network interface alarming functions which will alert PG and DB administrators when abnormal network conditions are detected, such as excessive transmission delay, network interruption, and so on.

The PG_SUPPLIERs shall describe in detail the NI1 network interface alarming functionality that will be provided, such as types of alarms included, methods of detection, detection time, methods to set and adjust alarm detection functions, alarmed event logging, and all other related functions.

PG-183. **Reporting.** PG shall provide NI1 network interface performance reporting functionality for generating periodical and on-demand reports.

PG-184. The statistics of NI1 network interface performance shall be reported on a periodically basis, such as hourly, daily, weekly, monthly, etc., and the reporting period shall be configurable by PG administrators. The periodical reports may be divided into two categories: Live Report for near real-time short interval (typically 5 to 15 minutes) network interface status report; and Static Report for longer term (daily, weekly, monthly, or quarterly) statistical information report.

PG-185. Live Reports shall include: Utilization (Measured at the Interfaces, and CoS Queues for each class of data); Traffic (Throughput, average packet size, packet discards for each class of data); CoS/QoS performance (Latency, Jitter and Packet Loss for each class of data); and interface hardware equipment health (Port up/down status, traffic level, utilization and error rate for Interface port).

PG-186. Static Reports based on actual data ("historical") that has been accumulated over a period of time, such as a month. Static Reports compare actual data with service targets that include: Faults (Fault restoration times vs. service targets for each class of data); and Availability (overall availability vs. service targets for each class of data).

PG-187. PG shall also provide on-demand report generation capability, which will allow PG administrator to request the generation of a report for a specified period of an interface.

The PG_SUPPLIER shall provide a detailed description of the supported NI1 network interface reporting functionality, including the standard types of reports that can be generated, sample standard reports, method to create a new type of report, and methods for standard report customization.

6.4.3 PG – Owner's Network Interface NI2

The NI2 network interface between PG and PG owner's network shall meet the following requirements.

6.4.3.1 Interface Options

PG-188. **Default interface options.** The network interface NI2 between PG and PG owner's network shall offer as minimum two default options: optical Ethernet interface option and galvanic Ethernet interface option.

PG-189. **Optical Ethernet interface option requirement.** The PG optical network interface option shall meet the following technical requirements.

Function	**Value**	
Applicable standard	IEEE 802.3u 100BASE-FX	IEEE 802.3z 1000BASE-SX
Communication speed	100 Mbps full-duplex	1000 Mbps full-duplex
Connectors	ST RX/TX Style connectors	ST RX/TX Style connectors

Function	Value	
Cable	62.5/125 µm multi-mode fiber optic cable up to 2 km (glass)	50/100 µm multi-mode fiber optic cable up to 550 m (glass)
Optical wavelength	1270-1380 µm	850 nm
LED Indicators	Link Active, Receive Data, 100 MB/s, Transmit Data	Link Active, Receive Data, 100 MB/s, Transmit Data

PG-190. **Galvanic Ethernet interface option requirement.** The PG Galvanic network interface option shall meet the following technical requirements.

Item	Value	
Applicable standards	IEEE802.3u 100BASE-TX	IEEE802.3ab 1000BASE-T
Communication speed	100 Mbps for full-duplex	1000 Mbps for full-duplex
Connector	RJ-45	
Cable	2-Pair UTP Cat 5 up to 100m	2-Pair UTP Cat. 5, 5e, 6, and 7, up to 100m

PG-191. **Other interface options.** PG shall also be capable of supporting other network interface options for NI2 network interface through replacing network interface card, using protocol converters/gateways, and so on.

6.4.3.2 Network Protocols

PG-192. **IPv6/IPv4 network protocol support.** The PG NI2 interface shall support both IPv6 and IPv4 network protocols.

6.4.3.3 Redundancy and Hot-swap Capability

PG-193. **Data class based redundancy requirements.** PG NI2 network interface shall meet redundancy requirement in accordance to its supported data classes.

Class supported	Publishing	Subscribing
A	Redundant	Redundant
B	Redundant	Redundant
C	Redundant	Redundant
D	Non-redundant	Non-redundant
E	Non-redundant	Non-redundant
PG NI2 redundancy requirement	= Requirement for highest class supported	

PG-194. **No-interruption repair.** When redundant NI1 interface is required, the PG NI1 network interface hardware and software shall support no-interruption repair capability for replacing defective network interface hardware/software.

6.4.3.4 NI2 Network Interface Management

PG-195. **Network Interface Management**. The PG design shall include NI2 network interface management functionalities for configuration, monitoring, and diagnose the interface.

PG-196. **Network Interface diagnosis capabilities**. The PG design shall support local (on-site PG administrator) and remote (Owner's network administrator) diagnostics capable of detecting and autonomously alerting abnormal operating parameters in owner's network communications.

PG-197. **Network Interface Hardware Equipment diagnosis capabilities**. The PG design shall support local (on-site PG administrator) and remote (Owner's network administrator) diagnostics capable of detecting and autonomously alerting abnormal interface's hardware equipment operating conditions including, but not limited to, memory failure, power supply degradation, microprocessors(s) failures (e.g. computer operating system watchdog events), firmware/software problems, excessive device temperature, etc.

6.4.3.5 Monitoring, Alarming and Reporting

PG-198. **Monitoring.** PG shall implement proper NI2 network interface monitoring functionalities for network traffic monitoring and network connection health assessment. The monitoring function shall monitor the real-time traffic volume, latency, dropped packets, corrupted packets, network interruptions, and other important network performance matrices. The monitoring function shall also collect and provide monitoring data for use by alarming and reporting functions.

The PG_SUPPLIER shall provide a detailed description of the implemented network interface monitoring functionalities, including methods to determine network traffic volume going through each port, transmission latency from publishing PG to subscribing PG, and so on.

PG-199. **Alarming.** PG shall implement NI2 network interface alarming functions which will alert PG and DB administrators when abnormal network conditions are detected, such as excessive transmission delay, network interruption, and so on.

The PG_SUPPLIERs shall describe in detail the NI2 network interface alarming functionality that will be provided, such as types of alarms included, methods of detection, detection time, methods to set and adjust alarm detection functions, alarmed event logging, and all other related functions.

PG-200. **Reporting.** PG shall provide NI2 network interface performance reporting functionality for generating periodical and on-demand reports.

PG-201. The statistics of NI2 network interface performance shall be reported on a periodically basis, such as hourly, daily, weekly, monthly, etc., and the reporting period shall be configurable by PG administrators. The periodical reports may be divided into two categories: Live Report for near real-time short interval (typically 5 to 15 minutes) network interface status report; and Static Report for longer term (daily, weekly, monthly, or quarterly) statistical information report.

PG-202. Live Reports shall include: Utilization (Measured at the Interfaces, and CoS Queues for each class of data); Traffic (Throughput, average packet size, packet discards for each class of data); CoS/QoS performance (Latency, Jitter and Packet Loss for each class of data); and interface hardware equipment health (Port up/down status, traffic level, utilization and error rate for Interface port).

PG-203. Static Reports based on actual data ("historical") that has been accumulated over a period of time, such as a month. Static Reports compare actual data with service targets that include: Faults (Fault restoration times vs. service targets for each class of data); and Availability (overall availability vs. service targets for each class of data).

PG-204. PG shall also provide on-demand report generation capability, which will allow PG administrator to request the generation of a report for a specified period of an interface.

The PG_SUPPLIER shall provide a detailed description of the supported NI2 network interface reporting functionality, including the standard types of reports that can be generated, sample standard reports, method to create a new type of report, and methods for standard report customization.

7 Security Requirements

This section describes the NASPInet cyber security framework and mechanisms, as well as specific cyber security requirements of PG, for ensuring a high level of security of the NASPInet. The specific security requirements for DB are provided in the Security Requirements section of DB specification.

7.1 NASPInet Overall Security Requirements/Considerations

The two key components of the NASPInet - the Phasor Gateway and Data Bus – shall be combined to satisfy the overall NASPInet security requirements contained in this subsection. The NASPInet security requirements are stated in three levels: System level (This subsection), Data Bus (DB) level (Subsections 7.2 and 7.3 of the Data Bus Specification), and Phasor Gateway (PG) level (Subsections 7.2 and 7.3 of this Specification). The security requirements of PMU, PDC, and the associated NASPInet access networks are beyond the scope of this NASPInet specification. However, it is expected that most of the security requirements of PG shall be adapted to PMU and PDC security requirements, and several of Data Bus requirements are applicable to the security requirements of NASPInet's access networks.

The overall (system level) NASPInet cyber security requirements are as follows.

7.1.1 End-to-End Security

All traffic of NASPInet shall be transmitted through the NASPInet with an end-to-end security guarantee, which means that the required security properties (e.g., confidentiality, integrity, authentication) of a given traffic flow must be satisfied by all the system components involved in the flow, namely, the end systems (e.g., PGs, servers) and the Data Bus. It shall prevent man-in-the-middle from intercept the traffic and tamper with it, and also shall prevent traffic replay attacks, colluding attacks, and masquerading attacks.

7.1.2 Flow Security

The data flow and control flow supported by the NASPInet shall satisfy security properties of confidentiality, integrity, authentication, non-repudiation, and availability. The implementation shall comply with the Federal Information Processing Standards (FIPS) relative to cryptographic infrastructure where applicable. FIPS PUB 140-2 titled "Security requirements for cryptographic modules" defines Security Levels 1-4 with increasing level of security from level 1 through 4. Many of NASPInet's data services shall as a minimum, support "FIPS 140-2 Level 1" security. However, FIPS 140-2 Level 2 or higher levels of security shall also be supported as appropriate for certain applications to enhance the "physical security" (e.g., tamper resistance) of devices and cryptographic modules, e.g., to protect private keys. In addition, the overall system design shall meet the specified security level stated above for each data flow, service, and protection functions of the NASPInet. (Refer to http://www.itl.nist.gov/fipspubs/by-num.htm for other relevant FIPS standards).

7.1.3 Heterogeneous Security Needs

The NASPInet shall support a diverse mix of security properties and priorities for different traffic classes, i.e., while some traffic shall require data integrity and authentication only, other traffic shall require data confidentiality in addition to integrity and authentication. For example, the PMU stream data flow shall prioritize data integrity property over confidentiality property, whereas infrastructure services such as the naming service and registration service shall require both confidentiality and integrity.

7.1.4 Security Infrastructure

NASPInet shall incorporate a FIPS compliant infrastructure, with relevant components including but not limited to certificate authorities, registration servers, naming servers, etc. to enable the required security functions for the various data flows supported. The infrastructure design shall specify how any private and/or PKI-based components will function relative to public and private key management.

There shall be no single point of failure in the security architecture and overall NASPInet resource management architecture. The architecture shall incorporate sufficient degree of redundancy of security services at the PG and Data Bus.

7.1.5 Infrastructure Security

The NASPInet infrastructure shall provide appropriate mechanisms to protect from, detect and respond to infrastructure based attacks such as protocol-based, service-based, intrusion-based, man-in-the-middle (data modification, interruption, replay), denial of service, and other malicious attacks. It shall also be resilient, in terms of extensible pattern-matching, heuristic, parameter-based and other detection and alerting capabilities, to emerging and zero-day attacks via a suitable real-time security monitoring and mitigation framework.

7.1.6 Vulnerability Assessment

The PGs and servers shall support vulnerability assessment and mitigation which collectively includes instrumentation of security event logs, real-time log analysis, vulnerability testing, and remedial measures such as security upgrades and patch management.

7.1.7 Trust Management

Establishing credentials among NASPInet components shall be an important design consideration. A central authority (e.g. NERC) shall be established to handle the credential management for NASPInet connected entities, which includes entity registration, verification, credential distribution and revocation. As a minimum, this authority shall be able to:

- Define the various services and the type of credentials that are needed to access the given service.
- Define the various credentials and defining the superset/subset relation among credentials and union/intersection operation among credentials.
- Establish methods to grant and revoke credentials to a user/machine.
- Establish methods to upgrade/degrade the credentials required to access a given service.

7.1.8 Considerations of PMU Data Characteristics

7.1.8.1 Data Size and Static Data

The size of PMU signal data is typically small (4 to 8 bytes). Also, the PMU data is somewhat static in nature meaning that it does not change every measurement cycle. These characteristics require that approved encryption algorithms shall be utilized correctly in general, and especially relative to these unique considerations.

7.1.8.2 Security Granularity

The NASPInet system shall support security at different levels of granularity depending on class-specific requirements and implementation. The design shall weigh the pros and cons associated with security implementation at different levels to support fine-grained data publishing and accessibility. For example:

The system shall support streaming data flow's security as follows: (i) at the "signal" granularity level and (ii) at the data "frame" level. Data arrives at a "publisher gateway" in, for example, IEEE C37.118-2005 frames typically containing multiple PMU signals, i.e. one C37.118 frame may contain a voltage phasor and a current phasor. The subscriber shall be able to receive data down to the individual signal level. In this example, the publisher shall be able to grant permission to view the voltage phasor but not the current phasor even though they are in the same C37.118 frame.

The publisher gateway shall be able to break all C37.118 frames down to the constituent signals. It shall also be possible to reconstruct a valid C37.118 frame on the subscriber side if this solution is implemented. Alternatively, the system may restrict access to, encrypt and/or otherwise secure each signal within a C37.118 data frame, and then send the entire frame out on NASPInet. The subscriber shall only have access to the signals for which they are authorized.

Conversely, for a different class of data, the information may be stored in a file containing post-event data, and effective security might encompass an encrypting file system, and/or Secure FTP, or other approaches.

7.1.9 Security and Controllability in a Dynamic Multicast Group

7.1.9.1 Dynamic groups

It is expected that more and more entities will be connected to NASPInet and new/outdated applications will be deployed/removed on a continuous basis by entities connected to the NASPInet. As a result, the subscribers of a multicast group, should multicast be used, for a published data stream will be very dynamic instead of being static. Maintain security and controllability of a dynamic multicast group will be critical for NASPInet but it is also a major challenge for it:

- The PG of an entity shall be able to maintain its full control over to/from which PGs it would like to share/receive the data in multicast groups, not only at the initial setup through a publisher/subscriber mechanism, but also for the life time

- The PG shall provide secure multicast communications with applicable and appropriate security measures including but not limited to source authentication as in unicast communications

Without proper security measures, the benefits of applying multicast technology to minimize the bandwidth utilization in NASPInet will be seriously negated. When dealing with security in multicast, the design shall account for the specific restrictions that are inherent in the way multicast works.

7.1.9.2 Key Management

The system shall enforce dynamic key control. If a multicast group, or any other group defined as constraining access to any class of NASPInet information, is dynamic (i.e., members join and leave the group dynamically), the key management protocol shall ensure that the keys are updated suitably to ensure join and leave secrecies. *Join secrecy* ensures that members that have joined the group newly should not able to decrypt existing data unless specifically allowed, and *leave secrecy* ensures that members who have left the group cannot decrypt the future data sent to the group. The design shall ensure that the overhead associated with secure multicast communication, such as overheads due to key management, encryption, and decryption does not contribute to violating the QoS guarantees of NASPInet applications.

Additionally, Key Management shall at a higher level provide the functionality to implement best practices including but not limited to on-demand, regular and random key rotation; key revocation with appropriate levels of granularity, and other best practices.

7.1.9.3 Security vs. QoS Tradeoffs

The NASPInet shall ensure QoS and maintain cyber security. However, meeting one requirement shall not degrade the other requirement. For example, increasing security by using longer encryption key will require more processing time at PGs during encrypting and decrypting processes, which may result in NASPInet not being able to meet QoS (e.g., end-to-end delay, delay jitter) requirement.

The design shall ensure that both the required QoS and security properties for the various flows are supported in the NASPInet. In case of overloads that arise due to unanticipated contingencies, suitable resource management mechanisms shall be in place to degrade QoS for low-priority flows, or even drop them if necessary, to support high-priority flows.

The design shall also address QoS and security guarantees for multicast flows for efficient implementation of publisher/subscriber model of data communication. The key distribution and rekeying overhead shall be kept small to meet this requirement.

7.1.9.4 A Key Management Example in a Multicast Environment

The example assumes the use of multicast capability of IPv6 protocol for real-time streaming data subscription fulfillment in a one-publisher-to-many-subscriber scenario. Separate cryptographic keys are used for a published data stream and for all subscriptions of the data stream that may subscribe to different portions of the data stream. The example is to illustrate a key management scheme that satisfies the above considerations. DB_Supplier shall, as a minimum, support this key management scheme and any other schemes that better balance the QoS and data security requirements of the NASPInet data publish/subscribe mechanism.

A generalized complex one-publisher-to-many-subscriber scenario for real-time streaming data distribution will be that a published data stream is subscribed by multiple subscribers, each subscribing to a different portion of the signals contained in the data stream with some overlaps between different subscriptions. Such scenario could occur as a result of different access rights were granted by the publishing PG to different subscribing PGs for signals contained in the data stream, and/or subscribing PGs selected different portions of the signals of the data stream to subscribe.

In this example, when a data stream is first published, P-PG shall obtain a publishing cryptographic key from NASPInet. The publishing cryptographic key shall be used by P-PG for encrypt the published data stream, and for DB to decrypt the data stream wherever needed.

For each subscription to the published data stream, the subscribing S-PG shall obtain a subscription cryptographic key from NASPInet. The subscription cryptographic key shall be used by S-PG for decrypt the subscribed data stream, and for DB to encrypt the subscribed data whenever necessary.

NASPInet DB key generation and management function shall ensure that all publishing cryptographic keys and subscription cryptographic keys are not duplicated for all active subscriptions.

The encrypted data stream from P-PG will be transported across the NASPInet WAN in IPv6 multicast protocol. The stream middleware of the NASPInet that resides closest to the S-PG of a subscription shall, upon recerving each frame of the data stream, perform the tasks of decrypting the data with the publishing cryptographic key of the data stream, extracting the subscribed data, and encrypting the subscribed data with subscription cryptographic key before delivering the data to the S-PG.

This scheme takes the advantage of the efficient real-time data stream delivery of the multicast data distribution capability of the IP network, while only require one additional decryption/encryption process for fulfilling each subscription. With separate publishing/subscription keys, the *join* and *leave* secrecy of the published data stream can be maintained.

7.1.10 NERC CIP Compliance

To comply with NERC critical infrastructure protection (CIP) standards, the cyber security functional requirements of NASPInet shall comply with the relevant subcategories of CIP-003, CIP-005, and CIP-007. http://www.nerc.com/page.php?cid=2%7C20

The NERC required level of "security management control" (CIP-003) shall be supported including information protection (CIP-003-4), access control (CIP-003-5), and change control and configuration management (CIP-003-5).

The notion of "electronic security perimeter (CIP-005-1)" covering critical cyber assets (CIP-002-1) of NASPInet shall be identified. The security perimeter architecture (CIP-005-1) shall effectively enforce electronic access control (CIP-005-2), monitoring electronic access (CIP-005-3), and enable cyber vulnerability assessment (CIP-005-4), and generate necessary logs and documentations (CIP-005-5).

The NERC required "system security management" (CIP-007) shall be supported including security patch management (CIP-007-3), malware software protection (CIP-007-4), account management (CIP-007-5), and security status monitoring (CIP-007-6).

7.2 Phasor Gateway General Security Requirements

The PG shall be authorized by a central Authorization Server (AS) of the NASPInet before connecting to the NASPInet.

PG shall have mechanisms to authorize/de-authorize devices (PDCs/PMUs) that connect to it.

PG shall incorporate, either internally and/or via external services, intrusion detection and intrusion tolerance capabilities to detect and appropriately mitigate intrusions into the NASPInet.

PG shall have the requisite credentials, obtained from the AS, to publish its data on the Data Bus or to provide any service.

PG shall have requisite credentials to subscribe to a given data stream or service.

7.2.1 Access Control

The PG shall, as a minimum, support "role based access control" to support efficient administration of user login to it. The roles shall be flexibly defined by the System Administrator to assign assets and services that can be accessed and controlled on a flexible manner. The access to PG shall provide authentication of valid users with encrypted passwords on the network and passwords shall be stored in encrypted format.

7.2.2 Malware Scan

The system shall allow commercial products that system administrator uses to scan for viruses, spy-ware and other mal-ware without interrupting the functionality, significantly impacting system performance or impacting failover capability of the system. The system shall be scanned for viruses, worms, Trojan horses, and other software contaminants during different stages of the development life cycle and periodically during the production stage, using up-to-date signatures as provided by the anti mal-ware software.

7.2.3 File Integrity

The PG shall be provided with file integrity verification capability to periodically scan for or be alerted for unauthorized modifications to selected system files. The scans shall not have a significant negative impact on the system performance and not impact functionality.

7.2.4 Audit Logs

Logs recording user, administrator and operator activities, exceptions and faults, and security events shall be produced and kept real-time for a period as determined by the administrator. It shall be possible to archive logs and easily access them for 1-3 years of time frame dependent on the type of log. Logs shall be captured at minimum on operating system, network components, database and application level. The logs shall be protected from both unintentional and malicious modifications, and shall be kept at remote locations and should be easily accessible when they are needed.

7.2.5 Security Updates

Any major security updates and patch management processes shall be tested for correctness in a controlled production software environment before being deployed into the real system. Testing shall confirm that the patch corrects the published errors and does not introduce any new errors. The system design shall provide the required resources and procedures to support safe system updates. The system shall also rollback features that shall enable the PG_REQUESTER, under agreement with and direction from a trusted authority, to remove updates that are causing problems and return to at least the previous system state.

7.3 Phasor Gateway Specific Security Requirements

PG shall meet the following security requirements in identification and authentication, logical access control, information assurance and monitoring & auditing in supporting the NASPInet overall security requirements.

7.3.1 Identification and Authentication Requirements

PG-205. A PG shall be able to positively identify and authenticate all equipment that it communicates with and each user that has access to. A PG shall also be able to positively identify and authenticate each subscription among all subscriptions. All identification shall be implemented using unique 128-bit IDs. A PG shall meet the following identification and authentication requirements.

PG-206. **DB component identification and authentication:** Prior to connecting to NASPInet DB, PG administrator shall obtain secure IDs for DB components and authentication methods through a secure procedure. The DB IDs shall be securely stored in PG and are used for positively identify and authenticate messages received from DB components once PG is connected to the DB. The DB IDs shall be encrypted, and securely stored. It shall not be possible for PG users and PG administrator to alter these IDs. Positive identification of obsolete or compromised DB IDs, the process of purging them and assigning new DB IDs must also be supported.

PG-207. **PG identification and authentication:** Prior to connecting a PG to NASPInet DB, the PG's administrator shall also obtain a secure ID for the PG and the PG authentication method for other PGs through a secure procedure. The PG ID shall be securely stored for use in all communications with other equipment that the PG communicates with, such as DB and other PGs of NASPInet. Each PG shall be authorized by a central Authorization Server (AS) that issues such ID and shall be provided as part of the NASPInet DB. The PG ID shall be encrypted, and securely stored. It shall not be possible for PG users and PG administrator to alter PG ID. PG shall also be capable of storing other PGs IDs and authenticate those PGs using the authentication methods that it obtained. Positive identification of obsolete or compromised PG IDs, the process of purging them and assigning new PG IDs must also be supported.

PG-208. **Device (e.g., PMU/PDC) and application identification and authentication:** PG shall have a mechanism to positively identify and authenticate any device/application that sends/receives data to/from PG through PG_REQUESTER's network. The device ID, as well as IDs of signals to/from the device, or application ID shall be obtained through the secure registration process with NASPInet directory and name server. The device ID, signal ID, and application ID shall be encrypted and securely stored in PG for use in future communications. A device or an application shall use its ID to communicate with PG in direct device-PG or application-PG communications. Positive identification of obsolete or compromised device IDs and signal IDs, the process of purging them and assigning new IDs must also be supported.

PG-209. **Subscription identification and authentication:** PG shall obtain a unique subscription ID for each approved subscription. The subscription ID shall be encrypted and securely stored in PG along with the subscription details. The subscription ID shall be used for authenticate all subscription related communications. Positive identification of obsolete or compromised subscription IDs, the process of purging them and assigning new IDs must also be supported.

PG-210. **PG user identification and authentication:** PG shall provide PG administrators with full capabilities in creating/modifying/deleting user accounts, assigning user IDs, and designating access rights of each user. PG administrator shall assign each PG user with a user ID. PG user shall be authenticated by its user ID and the password linked to the user account.

7.3.2 Logical Access Control Requirements

PG-211. **Access Control:** PG shall meet access control requirement of NERC CIP standard. PG shall implement separate access control for its interfaces to DB of NASPInet and to PG_REQUESTER's network side. It shall not be possible to gain PG access on one side by gaining PG access on the other side of the PG.

PG-212. **Access Control Policy:** PG shall provide a means for PG administrator to set various access control policies, including user access control policy, device/application access control policy, and access control policy for other PGs and DB components.

PG-213. **User Access Control Policy:** PG shall allow PG administrator to set user access control policy based on multiple factors, including but not limited to user identity, roles, location, time, transaction, service constraints, and common access modes. PG shall allow PG administrator to set such user access control policy on an individual user basis.

PG-214. **Device/Application Access Control Policy:** PG shall allow PG administrator to set device/application access control policy based on multiple factors, including but not limited to device/application identity, functions, location, time, transaction, service constraints, and common access modes. PG shall allow PG administrator to set such device/application access control policy on an individual device/application basis.

PG-215. **Access Control Policy for other PGs:** PG shall allow PG administrator to set access control policy for other PGs based on multiple factors, including but not limited to PG identity, PG ownership, location, time, transaction, service constraints, and common access modes. PG shall allow PG administrator to set such access control policy for other PGs on an individual PG basis. PG shall also allow PG administrator to set signal access control rights for other PGs at the signal granularity level for each PG.

PG-216. **Access Control Policy for DB components/servers:** PG shall allow PG administrator to set access control policy for DB components/servers based on multiple factors, including but not limited to DB component/server identity, DB component/server functions, location, time, transaction, service constraints, and common access modes. PG shall allow PG administrator to set such access control policy for DB components/servers on an individual DB component/server basis.

PG-217. **PG_REQUESTER side user access control:** PG shall use one or more access control methods or a combination of them, such as password/token, PKI based authentication, ACL, constrained user interface, and security labels, to control PG_REQUESTER side's user access to PG. PG shall support as a minimum two-factor (one static and one dynamic) login. PG shall adopt the best practices in user ID and password management, such as one-way password encryption, password strength enforcement, regular password update, and so on. PG shall provide means for PG administrator to set the password management parameters.

PG-218. **PG_REQUESTER side equipment/application access control:** PG shall limit equipment access to PG to only data/control flow exchanges and the supporting messaging in accordance with their respective API. No login to PG by equipment/application shall be allowed. All communications with equipment and applications shall be accompanied with proper identification and authentication process.

PG-219. **DB side user access control:** PG shall not provide any PG administrator and PG user login mechanism that will allow them gain access of their accounts from connecting to NASPInet WAN. It shall also not be possible for DB administrator, other PGs administrators/users to gain access of the PG through NASPInet WAN.

PG-220. **DB side access control:** PG shall limit its communication with DB and other PGs to only data/control flow exchanges and the supporting messaging (subscription setup, start/stop streams, etc.) through NASPinet WAN. No login to the PG by DB components and other PGs shall be allowed. All communications with equipment and applications shall be accompanied with proper identification and authenticated by proper authentication processes. In addition to authentication within the PG using methods obtained prior to connecting to DB, a PG shall also be able to authenticate DB components and other PGs through the DB security server and other PGs. PG shall also provide means for authenticate a DB component or the other PG through multiple authentication methods/processes.

PG-221. **Access control administration:** PG administrator shall be the only one who has the rights and privileges to administer the PG access control. It shall not be possible for other PG users to administer the PG access control.

7.3.3 Information Assurance Requirements

PG-222. PG shall ensure that all communications of the PG with others meet the information assurance requirements in confidentiality and integrity. PG shall provide means to ensure that any information that it sends across NASPInet is secure from unauthorized use, which can only be understood and used by the intended recipient(s). PG shall also provide means to enable information recipient(s) including itself to verify the integrity of the delivered/received information.

PG-223. Contents of PG traffic shall satisfy appropriate information assurance properties – confidentiality, integrity, authentication, and non-repudiation properties – using a combination of technologies such as encryption (to achieve confidentiality), message authentication codes (to achieve integrity), and digital signatures (to achieve authentication and non-repudiation). The PG shall implement information assurance mechanisms at multiple security strengths to accommodate diverse traffic requirements. PG shall implement secret key based encryption/decryption methods for streaming data and control flows. PG shall support overall PKI infrastructure of the NASPInet (to be specified in NASPInet DB specification) for all other traffic, such as system administration traffic (e.g., PG registration, device registration, etc.), subscription setup process traffic, historical data exchange traffic, etc. The PG shall support relevant FIPS standards for cryptography. Representative algorithms include encryption algorithms (FIPS 197), message authentication codes (FIPS 198), PKI (FIPS 196), Digital signatures (FIPS 186). Refer to the following NIST publications for FIPS standards' details.
http://csrc.nist.gov/publications/PubsTC.html#Cryptography
http://csrc.nist.gov/groups/ST/toolkit/index.html

PG-224. PG shall work in concert with DB to provide means to generate and manage secret cryptographic keys for streaming data and control flow encryption/decryption. PG and DB shall provide a key management mechanism for secret key generation and distribution. The mechanism shall be able to generate a secret key for each subscription setup, ensure that the key is different from all other keys across the NASPInet, and provide the key to the subscribing PG for decrypting the subscribed streaming data and control flow. PG and DB shall provide means for administrators to adjust secret key generation and distribution, such as the strength of the key, the life span of the key, dynamic key management, and so on. The secret key management mechanism shall also provide means for addressing the *join* secrecy and *leave* secrecy in the one-publisher-to-many-subscriber streaming data subscription scenario, meaning subscribers shall only have access to subscribed data when it has an active subscription, but not before the subscription was setup and after the subscription is cancelled.

PG-225. For streaming data and control flows, PG and DB shall implement information integrity assurance mechanisms for verifying information integrity by the recipients, such as message authentication codes (e.g., MAC, HMAC).

PG-226. For historical data exchange, PG shall ensure that the confidentiality of each subscription is strictly enforced by employing appropriate cryptographic method on the data. PG shall also implement information integrity insurance mechanisms for verifying information integrity of the delivered historical data by the recipients, such as CRC, digital signature, digital watermark, and so on.

7.3.4 Monitoring and Auditing Requirements

PG-227. PG shall provide active monitoring and auditing mechanisms for detecting, mitigating, controlling and diagnosing any security anomaly, including system failures, intrusions, attacks, etc.

PG-228. PG shall log all user activities and communication events with others. All logged information shall be securely stored and can not be changed or deleted by users or PG administrators once stored. The PG administrator shall be able to duplicate the logged information to other media/location for analysis and audit. PG shall provide a means for PG administrator to set the maximum time period that the logged information shall be kept by PG before purged by PG. The minimum value for this maximum time period of keeping the logged information shall not be less than 30 days, which shall be fixed and can not be adjusted by PG administrators.

PG-229. PG logging shall provide complete traceability of user activities and communication events at the system level relating to PG interaction with DB and other PGs. The logging shall include the identities of the users/equipment involved, sequence of the activities/events, and other relevant information.

PG-230. PG shall also provide complete traceability of user activities and communication events at the subscription level relating to each individual subscription. The logging shall include the identities of the users/equipment involved, sequence of the activities/events, and other relevant information associated with every subscription.

PG-231. PG logging shall also provide complete traceability of user activities related to PG users and PG administrator accessing the PG. The logging shall include the identities of the users involved, sequence of the activities, and other relevant information.

PG-232. PG shall implement automatic auditing functions that continuously analyze all logged user activities and communication events. The automatic auditing functions shall report and alert PG administrator immediately for any anomaly that it detects through visual and other notification means, such as email. PG administrator and users shall not be allowed to disable or alter PG automatic auditing functions and PG security anomaly reporting and alerting functionalities. PG security anomaly reporting and alerting functionalities shall include means to indicate that they are in good operating conditions.

PG-233. PG automatic auditing functions shall provide an automatic report generating functionality for generating NERC CIP compliance report. PG administrator shall be able to set the format of the report and the time interval for generating such report.

PG-234. PG shall provide means for PG administrator to view and analyze logged information. PG shall also provide means for exporting logged information and generating audit report by PG administrator.

8 Sizing, Performance, and Availability

This section describes PG performance requirements, including system availability, spare capacity and expansion requirements, quality of service, sizing, latency, normal and worst-case loading, maximum number connections of PMUs, PDCs, signals, and interfacing applications/users.

8.1 System Sizing

The PG hardware (including CPU memory, risk, number of processors, etc.) and software (dimensioning, licensing, etc.) shall be sized to ensure delivery of the required system performance specified in this document for the number of connecting PMU/PDC devices and signals with traffic level corresponding to data service class of each signal, and expected interfacing applications/user counts.

The PG hardware and software shall support the numbers of PMU/PDC devices, signals, and interfacing applications/users specified in Attachment I, plus a 100% margin, without adding new system components (e.g. servers) and without requiring changes to technology platforms.

The information for determining PG sizing requirements related to real-time streaming data exchange is listed in Table 8-1. The information for determining PG sizing requirements related to historical PMU data is listed in Table 8-2. A, B, C, D and E indications in Table 8-1 and Table 8-2 denote data service classes of A, B, C, D and E respectively.

Table 8-1 PG real-time data exchange needs for determine sizing requirements

Sizing items	Initial Quantity						Ultimate Quantity					
	Publish			Subscribe			Publish			Subscribe		
	A	B	C	A	B	C	A	B	C	A	B	C
No. of real-time data streams												
Min. frame size (kB/frame)												
Max. frame size (kB/frame)												
Avg. frame size (kB/frame)												
Min. analog data points/frame												
Max. analog data points/frame												
Total analog data points												
Min. digital data points/frame												
Max. digital data points/frame												
Total digital data points												
Min. reporting rate (frames/s)												
Max. reporting rate (frames/s)												

Note: Frame size (kB) only counts the actual data contained in each frame of a data stream in its native format. Overhead of synchrophasor streaming data protocols (e.g., IEEE C37.118-2005 data frame protocol), network communication protocols (e.g. TCP, UDP, IP, etc.), and actual size change due to data encryption/decryption and/or data compressions are not included in this frame size value. PG_SUPPLIER shall take overhead into account when estimating the actual throughput and processing power requirements for various components of the PG based on PG_SUPPLIER's proposed system design.

Table 8-2 PG historical data exchange needs for determine sizing requirements

Sizing items	Initial Quantity				Ultimate Quantity			
	Publish		Subscribe		Publish		Subscribe	
	D	E	D	E	D	E	D	E
No. of HDS								
Total analog data points								
Total digital data points								
Min. No. of daily file transfer								
Max. No. of daily file transfer								
Min. file size (MB)								
Max. file size (MB)								
Avg. file size (MB)								

Note: File size (MB) is the total size of a file, which may include data file headers and other configuration information in addition to the data, but does not include any overhead of network communication protocols (e.g. TCP, UDP, IP, etc.), and file size change due to data encryption/decryption and/or data compressions. PG_SUPPLIER shall take overhead into account when estimating the actual throughput and processing power requirements for various components of the PG based on PG_SUPPLIER's proposed system design.

8.2 System Performance Requirements

The PG in its initial configuration shall meet the performance requirements defined herein. The loading for the PG in its initial configuration shall be simulated during the Factory Acceptance Tests. PG testing is described in Section 11 of this RFP.

8.2.1 System Activity Level Definition

For the purpose of identifying the PG performance under different system activity levels, the terms "steady state" and "high activity state" are defined below for each system. The PG_SUPPLIER shall simulate these activity levels during factory acceptance testing.

8.2.1.1 Steady State

The PG is said to be in a steady state when all of the following are true (and are continuously recurring) over a 15-minute period:

1) The PG is performing all normal operational functions including scanning and processing data from all phasor measurement data sources in the system configuration.

2) The PG system administrator is performing system administration functions such as registering and removing phasor measurement data sources, modifying the list of published signals, modifying subscriptions to real-time streaming data sources or historical data sources, and other NASPInet administration functions.

3) Fifty percent of all registered analog and digital streaming data signals are being sampled and delivered to subscribers at a rate of 30 samples per second and the remaining 50% of registered analog and digital streaming data signals are being sampled and delivered to subscribers at 10 samples per second.

4) Seventy percent of all registered analog and digital streaming data signals that the PG is subscribed to are being received from publishers at a rate of 30 samples per second and the remaining thirty percent of registered analog and digital streaming data signals that the PG is subscribed to are being sampled and delivered to subscribers at 10 samples per second.

5) The PG is retrieving one hour's worth of historical data over NASPInet for 50% of phasor data points and 50% of digital data points.

6) The PG is supplying one hour's worth of historical data over NASPInet for 50% of phasor data points and 50% digital data points.

The steady state conditions listed above may be modified as necessary to reflect the additional loading imposed by optional functions selected by PG_REQUESTER.

8.2.1.2 High Activity State

The PG is said to be in a high activity state when all of the following conditions are happening and are continuously recurring over a 15-minute period:

1) The PG is performing all normal operational functions including injesting and processing data from all phasor measurement data sources in the system configuration.

2) The PG administrator is performing system administration functions such as registering and removing phasor measurement data sources, modifying the list of published signals, modifying subscriptions to real-time streaming data sources or historical data sources, and other NASPInet administration functions.

3) All registered analog and digital streaming data signals are being sampled and delivered to subscribers at a rate of 30 samples per second.

4) All registered analog and digital streaming data signals that the PG is subscribed to are being received from publishers at a rate of 30 samples per second.

5) The PG is retrieving one hour's worth of historical data via NASPInet for all stored phasor data points and digital data points

The high activity state conditions listed above may be modified as necessary to reflect the additional loading imposed by optional functions selected by PG_REQUESTER.

8.2.2 Time Reference Unit Accuracy and Stability

Time Reference Units shall be used to synchronize all clocks within PG's processors and workstations to a common time standard. All PG clocks shall be synchronized to an accuracy of plus or minus 1 microsecond (μs) or better to the Universal Coordinated Time (UTC). UTC may be obtained from the Global Positioning System (GPS) time.

Upon loss of the time signal, the time reference unit shall revert to an internal time base. The internal time base shall have a stability of 1 μs per hour or better. The time shall return to within ±1.5 μs of UTC within five minutes of reacquisition of time sync signal.

8.2.3 System Latency

The system latency is defined as the time elapsed from the time when data is received by a publishing PG's ingest to the time when data left a subscribing PG's distributor. The system latency (delay) for transferring data from publishers to subscribers through NASPInet shall not exceed the following amounts under normal and high activity conditions:

1) The latency associated with real-time streaming data sources shall vary depending on class of data, as shown in Table 8-3 for Class A, B, and C data.

2) The latency associated with the start of historical data transfers (Class D and Class E data) shall not exceed thirty seconds for a thirty-minute event involving 200 phasor and 200 digital data points.

Table 8-3: NASPInet Availability and Latency Requirements for Each Data Class

Description	Class	Data rate (fps)	Availability	Max Interrupt Time	Latency	Max event length
Feedback control	A	30, 60, 120	99.9999%	< 5 ms	< 50 ms	N/A
Feed forward control	B	20, 30, 60	99.999%	< 25 ms	< 100 ms	N/A
Display	C	10, 15, 20 or 30	99.99%	< 250 ms	< 1 s	N/A
Disturbance analysis	D	30, 60, 120	99.9%	N/A	< 2 s for request/ response; best efforts for data transfer	30 min./event
Research	E	30, 60, 120	99.9%	N/A	< 2 s for request/ response; best efforts for data transfer	30 min./event

N/A: Not applicable.

8.2.4 System Utilization

This section lists the utilization figures for each activity level along with response times expected during the activity that the PG_SUPPLIER shall demonstrate during the Factory Acceptance Test.

8.2.4.1 Steady State Utilization

When the PG is in the steady state (as defined in Section 8.2.1.1), the PG utilization shall be as follows:

1) The utilization of each server in the PG measured over the fifteen (15) minute interval shall be 30 percent (30%) or less.

2) Over any fifteen (15) minute period, each hard disk device in the PG system shall not be busy with data transfer for more than 30 percent (30%) of the time. The average data access time shall be used in any bulk memory timing analysis.

8.2.4.2 High Activity State Utilization

When the System is in the high activity state (as defined in Section 5.6.1.2), the PG utilization shall be as follows:

1) The utilization of each processor in the PG over any fifteen (15) minute period shall be 50 percent (50%) or less measured over the fifteen (15) minute interval.

2) Over any fifteen (15) minute period, each hard disk in the PG shall not be busy with data transfer for more than 50 percent (50%) of the time.

8.2.5 Alarm Response Time

With the PG in the steady state or the high activity state, all alarms shall be reported by audible and visual alarms at a PG Administrator’s workstation within three (3) seconds. For the purpose of verification during FAT, an alarm message shall be displayed and alarmed facilities highlighted on displays within this time period.

8.2.6 Display Response Time

The display response time is defined as the elapsed time from the instant the display request is made by the user to the instant the requested display is completely shown on the console screen. Display response time shall not exceed one (1) second under steady state and high activity state conditions.

8.2.7 System Fail Soft Capability

The PG shall be designed to prioritize PG application functions to ensure that critical functions are carried out without excessive degradation in performance during PG overload periods (PG load exceeds the limit for the high activity state). Under no circumstances shall the PG fail to run due to “bursts” of input data changes and alarms. During a “fail soft” condition, the PG shall be designed to maintain the same level of function, QoS, reliability, and security.

8.3 System Availability

The individual PG component, and the PG as a whole, shall satisfy the availability requirements described in this section. The PG_SUPPLIER shall determine the level of redundancy required for each system component needed to satisfy these requirements. Redundant facilities shall maintain the same level of functionality, QoS, reliability, and security. The capability of the PG to satisfy the availability requirements shall be demonstrated during the PG Availability Tests during SAT.

The PG shall meet the availability requirements for each data service class (data class general requirements are contained in Section 3 of this RFP document). The availability is defined as the ratio of total time minus the total downtime, to the total time on an annualized basis.

The PG shall also meet the maximum interruption time requirement to ensure uninterrupted delivery of the real-time streaming data.

The NASPInet availability, maximum interruption time and latency requirements for each class of data are specified in Table 8.3. The overall PG availability and processing time limit requirements are specified in Table 8-4. In addition to the system availability requirements for each class of data, each PG_SUPPLIER-furnished device shall individually exhibit a minimum availability of at least 99.9%.

The proposed PG configuration shall have no single point of failure and shall protect against multiple device failures where devices have high failure rates or long repair times. The PG_SUPPLIER shall identify critical equipment, hardware components, software, and processes in the proposed PG configuration. If the failure of any single device (or sub-system) will cause the "critical" PG functions, such as security, real-time streaming data subscription fulfillment, etc., to become unavailable, either a redundant unit shall be provided for that device or a dual-PG (primary and backup) design shall be adopted. Automatic failover to backup facilities shall be completed with no loss of data and no interruption to "critical" PG functions.

Table 8-4 PG Availability and Processing Time Limit Requirements

Class	Data rate (fps)	Availability	PG processing time limit (ms)
A	30	99.9999%	6.25
	60		6.25
	120		4.17
B	20	99.999%	12.5
	30		12.5
	60		8.3
C	10	99.99%	50.0
	15		33.3
	20		25.0
	30		16.7

Note: PG processing time limit (ms) is the minimum of a) ½ of the reporting period, or b) 1/8 of NASPInet latency time allowed for a data service class.

8.3.1 System Availability Definition

For the PG to be considered "available" all "critical" functions of the PG shall be executing properly without any degradation in response times AND the minimum complement of hardware must be operational.

"Critical" functions shall include all periodic and on-demand PG functions.

8.4 Equipment Operating Life

The PG system shall be designed to have a useful life of at least ten (10) years with minimal servicing, part replacement, and software subsystems.

Appendix A: PG requirements applicability check list

The numbered Phasor Gateway requirements contained in this specification are divided into four categories applicable to each data service class as shown in this Appendix:

- ***Mandatory requirement (M):*** These are essential and must-meet requirements of the Phasor Gateway. Failure to meet these requirements will eliminate the solution from consideration.
- ***Highly-desirable requirement (H):*** Important but not absolutely essential. Would be very advantageous to have.
- ***Desirable requirement (D):*** Not essential, but would be nice to have.
- ***Not-a-requirement (N):*** Not a requirement (optional), but PG_SUPPLIER should take note and acknowledge the information provided in its response.

Please note a requirement could be a mandatory one for one class of data service, but could be highly desirable (or desirable, not-a-requirement) requirement for the other class of data service. In the following check list, M, H, D, and N are used to denote the type of the requirement that is applicable to the corresponding class of data service. If a requirement does not apply to the class of data service, the table cell is left blank.

In addition, there are requirements that may be highly desirable during the initial pilot implementation of the NASPInet, but will become mandatory for the full deployment of the NASPInet. The requirement applicability check list below has used two separate grouping to indicate this possible difference.

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-1	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-2	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-3	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-4	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-5																				
PG-6	M	M	M	M	M	M	M				M	M	M	M	M	M	M			
PG-7	M	M	M	M	M	M	M				M	M	M	M	M	M	M			
PG-8	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-9	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-10	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-11	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-12	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-13	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-14	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-15	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-16	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-17	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-18	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-19	H	H	H	H	H	H	H	H	H	H	M	M	M	M	M	M	M	M	M	M
PG-20	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-21	H	H	H	H	H	H	H	H	H	H	M	M	M	M	M	M	M	M	M	M
PG-22	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-23	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-24	H	H	H	H	H	H	H	H	H	H	M	M	M	M	M	M	M	M	M	M
PG-25	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-26	H	H	H	H	H	H	H	H	H	H	M	M	M	M	M	M	M	M	M	M
PG-27	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-28	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-29	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-30	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-31	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-32	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-33	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-34	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-35	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-36	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-37	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-38	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-39	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-40	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-41	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-42	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-43	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-44	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-45	D	D	D	D	D	D	D	D	D	D	H	H	H	H	H	H	H	H	H	H
PG-46	M	M	M	M	M						M	M	M	M	M					
PG-47	M	M	M								M	M	M							
PG-48	M	M	M	M	M						M	M	M	M	M					
PG-49						M	M	M	M	M						M	M	M	M	M
PG-50						M	M	M								M	M	M		
PG-51						M	M	M	M	M						M	M	M	M	M
PG-52	D	D	D	D	D	D	D	D	D	D	H	H	H	H	H	H	H	H	H	H
PG-53	D	D	D	D	D	D	D	D	D	D	H	H	H	H	H	H	H	H	H	H
PG-54	D	D	D	D	D	D	D	D	D	D	H	H	H	H	H	H	H	H	H	H
PG-55	M	M	M	M	M						M	M	M	M	M					
PG-56						M	M	M	M	M						M	M	M	M	M
PG-57	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-58	M	M	M	M	M						M	M	M	M	M					
PG-59	M	M	M								M	M	M							
PG-60	M	M	M								M	M	M							
PG-61	M	M	M								M	M	M							
PG-62	M	M	M								M	M	M							
PG-63	M	M	M								M	M	M							
PG-64	M	M	M								M	M	M							

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-65	M	M	M								M	M	M							
PG-66	M	M	M								M	M	M							
PG-67	M	M	M								M	M	M							
PG-68	M	M	M								M	M	M							
PG-69	M	M	M								M	M	M							
PG-70	M	M	M								M	M	M							
PG-71	M	M	M								M	M	M							
PG-72	M	M	M								M	M	M							
PG-73	M	M	M								M	M	M							
PG-74	M	M	M								M	M	M							
PG-75						M	M	M								M	M	M		
PG-76						M	M	M								M	M	M		
PG-77						H	H	H								M	M	M		
PG-78						H	H	H								M	M	M		
PG-79						M	M	M								M	M	M		
PG-80						H	H	H								M	M	M		
PG-81						M	M	M								M	M	M		
PG-82						M	M	M								M	M	M		
PG-83						H	H	H								M	M	M		
PG-84						H	H	H								M	M	M		
PG-85						M	M	M								M	M	M		
PG-86						H	H	H								M	M	M		
PG-87						H	H	H								M	M	M		
PG-88						M	M	M								M	M	M		
PG-89						H	H	H								M	M	M		
PG-90						H	H	H								M	M	M		
PG-91						M	M	M								M	M	M		
PG-92						H	H	H								M	M	M		
PG-93						H	H	H								M	M	M		
PG-94						M	M	M								M	M	M		
PG-95						H	H	H								M	M	M		
PG-96						H	H	H								M	M	M		
PG-97				M	M									M	M					
PG-98				M	M									M	M					
PG-99				M	M									M	M					
PG-100				M	M									M	M					
PG-101				M	M									M	M					
PG-102				M	M									M	M					
PG-103				M	M									M	M					
PG-104				M	M									M	M					
PG-105				M	M									M	M					
PG-106				M	M									M	M					
PG-107				M	M									M	M					
PG-108				M	M									M	M					
PG-109				M	M									M	M					
PG-110									M	M									M	M
PG-111									M	M									M	M
PG-112									H	H									M	M

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-113									H	H									M	M
PG-114									M	M									M	M
PG-115									H	H									M	M
PG-116									M	M									M	M
PG-117									M	M									M	M
PG-118									H	H									M	M
PG-119									H	H									M	M
PG-120									M	M									M	M
PG-121									H	H									M	M
PG-122									H	H									M	M
PG-123									M	M									M	M
PG-124									M	M									M	M
PG-125									H	H									M	M
PG-126									M	M									M	M
PG-127									H	H									M	M
PG-128									H	H									M	M
PG-129	M	M	M	H	H	M	M	M	H	H	M	M	M	H	H	M	M	M	H	H
PG-130	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-131	M	M	M	D	D						M	M	M	D	D					
PG-132						M	M	M	D	D						M	M	M	D	D
PG-133						M	M	M	D	D						M	M	M	D	D
PG-134						M	M	M	M	M						M	M	M	M	M
PG-135						M	M	M	M	M						M	M	M	M	M
PG-136						M	M	M	M	M						M	M	M	M	M
PG-137						M	M	M	M	M						M	M	M	M	M
PG-138						M	M	M	M	M						M	M	M	M	M
PG-139						M	M	H	H	H						M	M	M	M	M
PG-140						M	M	H	H	H						M	M	M	M	M
PG-141	M	M	H	H	H						M	M	H	H	H					
PG-142	M	M	M	H	H						M	M	M	H	H					
PG-143	M	M	H	H	H						M	M	H	H	H					
PG-144	M	M	M	H	H						M	M	M	H	H					
PG-145	M	M	M	H	H						M	M	M	H	H					
PG-146	M	H	H	H	H						M	H	H	H	H					
PG-147	M	H	H	H	H						M	H	H	H	H					
PG-148	M	M	M	M	M						M	M	M	M	M					
PG-149	M	H	H	H	H						M	H	H	H	H					
PG-150	M	H	H	H	H						M	H	H	H	H					
PG-151	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N
PG-152	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N
PG-153	M	H	H	N	N	M	H	H	N	N	M	M	M	N	N	M	M	M	N	N
PG-154	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N
PG-155	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N
PG-156	M	M	H	N	N	M	M	H	N	N	M	M	M	N	N	M	M	M	N	N
PG-157	M	M	H	N	N	M	M	H	N	N	M	M	M	N	N	M	M	M	N	N
PG-158	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N	M	M	M	N	N
PG-159	M	M	H	N	N	M	M	H	N	N	M	M	M	N	N	M	M	M	N	N
PG-160	M	M	H	N	N	M	M	H	N	N	M	M	M	N	N	M	M	M	N	N

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-161	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-162	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-163	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-164	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-165	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-166	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-167	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-168	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-169	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-170	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-171	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-172	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-173	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-174	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-175	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-176	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-177	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-178	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-179	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-180	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-181	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-182	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-183	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-184	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-185	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-186	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-187	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-188	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-189	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-190	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-191	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
PG-192	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-193	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-194	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H	H
PG-195	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-196	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-197	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-198	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-199	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-200	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-201	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-202	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-203	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-204	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-205	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-206	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-207	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-208	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M

Requirement Number	Pilot NASPInet implementation										NASPInet full deployment									
	Publish					Subscribe					Publish					Subscribe				
	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E	A	B	C	D	E
PG-209	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-210	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-211	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-212	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-213	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-214	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-215	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-216	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-217	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-218	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-219	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-220	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-221	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-222	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-223	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-224	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-225	M	M	M			M	M	M			M	M	M			M	M	M		
PG-226				M	M				M	M				M	M				M	M
PG-227	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-228	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-229	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-230	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-231	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-232	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-233	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
PG-234	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M

Appendix B: Abbreviations and Acronyms List

The definitions and meaning of the abbreviations and acronyms used in this specification are list below.

ACL – Access Control Level or Access Control List
ADK – Adapter Development Kit
ANSI – American National Standards Institute
API – Application Programming Interface
AS – Authorization Server
CIA – Confidentiality, Integrity, & Authentication (also Central Intelligence Agency)
CIP – Critical Infrastructure Protection
CoS – Class of Service
COTS – Commercial Off-The-Shelf (product)
CPU – Central Processing Unit
CRC – Cyclic Redundancy Check
CT – Current Transformer
DB – Data Bus
ECO – Equipment Change Order
EMS – Energy Management System
FAT – Factory Acceptance Test
FCO – Field Change Order
FERC – Federal Energy Regulatory Commission
FIPS – Federal Information Processing Standards
FTP – File Transfer Protocol
GPS – Global Position System
GUI – Graphical User Interface
HDS – Historical Data Source (device that supplies recorded phasor data)
HMAC – Heavy Message Authentication Codes
HMI – Human-Machine Interface
IA – Information Assurance
ID – Identification number (for NASPInet, all IDs are 128-bit)

Application ID – identifier for an individual application on a device that sends data to or receives data from NASPInet
Device ID – identifier for any device that sends data to or receives data from NASPInet
PG ID – identifier for any PG connected to the NASPInet DB
Signal ID – identifier for every signal that is published and can be accessed on NASPInet
Subscription ID – identifier for a subscription to a signal available on NASPInet
User ID – identifier for any user of the net with access to any PG or the DB

IEEE – Institute of Electrical and Electronic Engineers
IEC – International Electrotechnical Commission
IED – Intelligent Electronic Device
IP – Internet Protocol (also Intellectual Property)
ISO – International Organization for Standardization
IT – Information Technology
J2EE – Java 2 platform Enterprise Edition
l-to-l – line to line (connection)
l-to-N – line to neutral (connection)
kB – Kilo-bytes (1 kB = 1024 bytes)

LAC – Logical Access Control
LAN – Local Area Network
MAC – Message Authentication Codes
MB – Mega-bytes (1 MB = 1024000 bytes)
MTBF – Mean Time Before Failure
MTTR – Mean Time To Repair
NASPI – North American Synchrophasor Initiative
NDS – Name & Directory Service
NERC – North American Electric Reliability Corporation
NEC – National Electric Code
NEMA – National Electrical Manufacturers Association
NFPA – National Fire Protection Association
NI1 – Network Interface 1; interface on PG connecting to the NASPInet DB
NI2 – Network Interface 2; interface on PG connecting to devices external to NASPInet
NI3 – Network Interface 3; interface on internal NASPInet DB components
OEM – Original Equipment Manufacturer
PC – Personal Computer
PDC – Phasor Data Concentrator
PKI – Public Key Infrastructure
P-PG – Publishing Phasor Gateway
PG – Phasor Gateway

- PG-A – Phasor Gateway Access; PG logical component
- PG-D – Phasor Gateway Distributor; PG logical component
- PG-DM – Phasor Gateway Device Management; PG logical component
- PG-H – Phasor Gateway Historian; PG logical component
- PG-I – Phasor Gateway Ingest; PG logical component

PMU – Phasor Measurement Unit
PT – Potential Transformer
QoS – Quality of Service
RAID – Redundant Array of Independent Discs
RDBMS – Relational Database Management System
RFP – Request For Proposal
RPC – Remote Procedure Call
RT – Real Time
RT-SDS – Real-Time Streaming Data Source (device that streams phasor data in real-time)
S-PG – Subscribing Phasor Gateway
SAN – Storage Area Network
SAT – Site Availability Test or Site Acceptance Test
SCADA – Supervisory Control And Data Acquisition (system)
SDK - Software Development Kit
SDS – Streaming Data Source (device that streams phasor data)
SOA – Service Oriented Architecture
SOX – Schema for Object-oriented XML
SS – Security Service or Security Server
UTC – Coordinated Universal Time
WAN – Wide Area Network
XML – eXtensible Markup Language

Attachment I

This attachment is intended for the PG_REQUESTER to put in information regarding its company that the PG_SUPPLIER would need to know to develop specific solution configurations for the PG_REQUESTER and thus a more precise bid, including the following materials for example:

- Number of PMU/PDC, signals, and interfacing applications/users
- IT policies and guidelines – e.g. IT governance, security policy, preferred IT platforms, etc.
- Operating procedures – e.g. safety procedures, equipment connection guidelines, etc.
- Existing and planned infrastructures – e.g. major facility locations, telecom network, etc.
- Existing IT systems – Enterprise IT common services (e.g. Enterprise Service Bus or middleware), Database Management System, Enterprise Performance Management tools, etc.

Attachment II

This attachment is intended for the PG_REQUESTER to put in specifications for hardware, software, and project implementation and system sustainment services based on the PG_REQUESTER's specific requirements and guidelines. Following are examples of these specifications that the PG_REQUESTER may tailor for its own needs or replace in whole with its standard Request for Proposal materials. Note that the following sections in this attachment follow the section numbering of the main text of the specifications so that PG_REQUESTER can conveniently move the tailored text to the main specifications body.

9 Hardware Requirements

This section of the RFP describes the hardware requirements for PG, which includes all PG hardware components that are included in the PG_SUPPLIER’s scope of supply.

It is PG_REQUESTER’s intention to procure a PG system that generally satisfies the requirements of this section but which is adapted to best use the PG_SUPPLIER’s standard products.

In some cases, preferences are identified for a particular manufacturer’s equipment or a particular equipment design. Strict compliance with these preferences is recommended but not required. Compliances with preferences stated in this RFP shall not release the PG_SUPPLIER from the contractual obligations to satisfy the functional, availability, performance, security, capacity and other requirements of this RFP.

9.1 General Hardware Requirements

All hardware shall be manufactured, fabricated, assembled, finished, and documented with workmanship of the highest production quality and shall conform to all applicable quality control standards of the original equipment manufacturer(s) and the PG_SUPPLIER. All hardware components shall be new and suitable for the purposes specified.

The PG_SUPPLIER shall supply the most up to date hardware that is available at the time of shipment. Delivered hardware shall include all engineering changes and field changes announced by the manufacturer since it was produced. As part of the Site Acceptance Test, the PG_SUPPLIER shall have all hardware inspected and certified as acceptable for service under a maintenance contract by the local service offices representing the equipment manufacturers.

All hardware features described in the Proposal and in the Proposal's supporting reference material shall be fully supported by the system.

9.2 Processors and Auxiliary Memory

All processors shall be current models selected for the efficient operation of a real-time system.

The PG_SUPPLIER shall supply all processors that are used in servers and peripheral equipment.

The PG System shall include a suitable user interface for accessing the servers. A convenient mechanism shall be provided to connect the server user interface devices to any of the servers. The server user interface devices shall be rack mounted in the same cabinet as the servers, and shall be equipped with a suitable draw out shelf (or equivalent device) so that the server user interface devices can be stored when not being used.

The processors shall include facilities for orderly shutdown and resumption of processor operation upon detection of power loss and subsequent resumption of power. The PG processors shall ensure that only authorized personnel can perform system shutdown/restart. All such operations shall be logged as system events.

9.3 Archive Storage

Archive storage devices shall be used for backup of the PG system data and software and archival storage for the historical data functions.

9.4 Local Area Networks

The PG system local area network (LAN) shall support the necessary throughput to meet overall system performance requirements. The PG system “backend” LAN shall be based on 1-Gbps Ethernet. Connections to clients (workstations) shall be based on 100 Mbps LAN. Suitable grade cabling for the application shall be provided.

9.5 Time Reference Unit

Time Reference Units shall be used to synchronize all clocks within PG processors and workstations to a common time standard. The accuracy and stability of the Time Reference Unit shall meet the requirement specified in Section 8.

The time reference unit shall include digital displays that, as a minimum, are capable of displaying the time in formats that conform to ISO 8601 standard specifications.:

9.6 Spare Parts and Test Equipment

The PG_SUPPLIER shall deliver with the system all spare parts and special test equipment for all PG system components that will be maintained by PG_REQUESTER. PG_REQUESTER-maintained components will include all system components that cannot be maintained using OEM-supplied maintenance contracts. In particular, spare parts for critical PG system components that are **not** readily available from multiple sources shall be supplied to satisfy the availability requirements specified above.

Spare parts and test equipment shall also be supplied for other system components if necessary to satisfy the availability requirements specified above.

For multiple devices of the same type, the quantities of spare parts and test equipment shall be sufficient to maintain the equipment even if more than two similar failures occur simultaneously.

The PG_SUPPLIER proposal shall contain a list of spare parts that are included in the PG_SUPPLIER's base offering. The proposal shall also include a list of recommended spare parts that are not included in the base proposal.

9.7 Interconnecting Cables

The PG_SUPPLIER shall supply all cabling between components of the PG system. Plug-type connectors with captive fasteners shall be used for all interconnections. The connectors shall be polarized to prevent improper connections. Each end of each interconnection cable shall be marked with the cable number and the identifying number and location of each of the cable's terminations; this information shall agree with the drawings. Each cable shall be continuous between components; no intermediate splices or connectors shall be used. Terminations shall be entirely within the enclosures.

All interconnecting cables shall be rated as NEC Class 2 Plenum cable. Cables shall be tested to NFPA 262-1985 Test for Fire and Smoke Characteristics of Wires and Cables to a maximum peak optical density of 0.5, a maximum average optical density of 0.15, and a maximum allowable flame travel distance of five feet.

9.8 Equipment Enclosures

All PG_SUPPLIER-supplied PG equipment shall be mounted in PG_SUPPLIER-supplied enclosures.

The equipment enclosures shall be type HP Universal Rack 10642 G2 Pallet Rack Enclosure Cabinets or equivalent.

The enclosures shall meet the following requirements:

1) The enclosures shall meet or exceed NEMA 1 requirements

2) The enclosures shall be finished inside and out. All cabinet metal shall be thoroughly deburred, cleaned and sanded, and welds chipped to obtain a clean, smooth finish. All surfaces shall be treated. All edges and corners shall be rounded to prevent injury.

3) Enclosures shall be floor mounted with front and rear access to hardware and wiring. Enclosure height shall not exceed 80 inches.

4) Enclosures shall be lockable.

5) Moving assemblies within the enclosures, such as swing frames or extension slides, shall be designed such that full movement of the assembly is possible without bending or distortion of the enclosure or the moving assembly. Enclosures shall not require fastening to the floor to prevent tipping of the enclosure when the moving assembly is extended.

6) Wiring within enclosures shall be neatly arranged and securely fastened to the enclosure by non-conductive fasteners. Wiring between all stationary and moveable components, such as wiring across hinges or to components mounted on extension slides, shall allow for full movement of the component without binding or chafing of the wire.

7) Wiring within and between enclosures shall be secured and insulating devices (such as grommets) installed such that wire-to-metal contact is not possible.

8) All materials used in the enclosures, including cable insulation or sheathing, wire troughs, terminal blocks, and enclosure trim shall be made of flame retardant material and shall not produce toxic gasses under fire conditions.

9) Cable entry for PG equipment shall be through the bottom and sides of the enclosures.

10) Cooling air shall be drawn from the conditioned air within the room.

11) Wherever operating voltages in the hardware exceed 50 volts, the hardware shall be covered or shielded from accidental contact and shall be labeled accordingly.

12) All PG_SUPPLIER-supplied enclosures shall be suitable for mounting on PG_REQUESTER-supplied seismically-qualified "mounts."

9.9 Power Supply and Distribution

9.9.1 Uninterruptible Power Supply

All PG equipment will be powered via PG_REQUESTER-supplied Uninterruptible Power Supplies that furnish single phase 110/220 Vac power output with a maximum voltage variation of ±5% from nominal. The PG_SUPPLIER shall identify the maximum power demand for all PG_SUPPLIER-supplied components.

9.10 General Hardware Requirements

All PG system equipment shall satisfy the general hardware requirements described in the following sections.

9.10.1 Operating Environment

All PG equipment will be installed in facilities in which the temperature and humidity are controlled. PG equipment shall be designed to operate over an ambient temperature range of 60 to 90 °F with a maximum rate of change of 15 °F per hour. Relative humidity will range from 40% to 90% non-condensing.

9.10.2 Equipment Noise

The noise generated by the equipment in any enclosure, including desktop equipment, located in the computer room shall not exceed 60 dbA 1 meter (3 feet) from the enclosure. The noise generated by the equipment in any enclosure, including console equipment, located outside the computer room shall not exceed 50 dbA 1 meter (3 feet) from the enclosure. Sound-deadening enclosures shall be provided where necessary to meet these requirements.

9.10.3 Assembly and Component Identification

Each assembly in the system, to the level of printed circuit cards, shall be clearly marked with the manufacturer's part number, serial number, and the revision level. Changes to assemblies shall be indicated by an unambiguous change to the marked revision level. All printed circuit card cages and all slots within the cages shall be clearly labeled. Printed circuit cards shall be keyed for proper insertion orientation.

9.10.4 Enclosure Grounding

A safety ground in accordance with the National Electrical code shall be provided within each enclosure and shall connect to the ground (green) wire of the ac power input. Enclosure grounding shall be subject to PG_REQUESTER’s approval.

9.11 System Environments and Facilities

9.11.1 System Environments

The PG_SUPPLIER shall provide the hardware needed to support the following environments:

- Production, including redundant servers, power suppliers, LAN/WAN connections, cluster and/or automated backup/failover, SAN and/or RAID disks, etc.
- Development
- Testing and staging
- Training
- Disaster Recovery

The Production environment shall meet all system sizing and performance requirements as specified in Section 8. The PG_SUPPLIER is requested to provide recommendations for the other environments.

9.11.2 Facilities

The DB_Supplier shall provide estimates of the total facility and infrastructures needed to host the required equipment enclosures, installation space and admin workspaces, power supply, cooling, etc. for all system environments specified above, for the initial deployment phase and for each of the subsequent phases.

The DB_Supplier shall itemize all facility requirements that it assumes that DB_REQUESTER would provide, for example electrical wiring, AC, LAN/WAN connections, etc.

10 Software Requirements

PG_REQUESTER's goal is to acquire a software platform that will be economical to maintain and upgrade over the life of the system. PG_REQUESTER expects to incorporate additional functionality in the system throughout the lifetime of the PG to keep pace with changing requirements.

The software delivered to PG_REQUESTER shall be the latest version/release that is available at the time of shipment so that additional software upgrades are not required within six months following shipment.

10.1 Conformance to Industry Standards

PG_REQUESTER requires that the PG conform to mainstream computing standards and *de facto* standards wherever those standards are appropriate in the context of the PG design.

10.2 Use of PG_SUPPLIER Standard Support Software

Although a specific set of software support requirements are presented in this section, the primary intent of this section is to elicit a clear statement from the PG_SUPPLIER as to the nature of the proposed software support environment. In any case, PG_REQUESTER will require the PG_SUPPLIER to adhere to its proposal and will verify this during testing.

10.3 Distributed Computing Environment

The PG_SUPPLIER shall provide a distributed computing environment that assures adequate flexibility for the evolution of the PG. Use of any of the services described in this section shall be restricted to users with proper authorization. The term "product", as used in this section, refers to established, recognized commercial offerings with a significant installed base.

10.3.1 Computer Operating Systems

The PG_SUPPLIER shall not modify the computer operating systems. The PG_SUPPLIER may use value-added utilities and subroutines that utilize the operating system services, provided they are fully supported by the PG_SUPPLIER or by the OEM of the utility.

The PG shall be designed such that upgrades to the operating systems may be performed independently of application functions, without interruption of the PG operations. It shall be possible to update redundant components one at a time.

10.3.2 Computing Network Communications

Communications within and among the computing networks supplied by the PG_SUPPLIER shall conform to OSI (Open Systems Interconnection) standards, as well as the TCP/IP ("Internet") protocols.

The distributed computing environment shall be able to use both local area networks and wide area networks transparently, such that there shall be no restriction (other than capacity limitations) on the geographic dispersal of applications among the processors of the PG.

10.3.3 Open System Interfaces

The PG_SUPPLIER shall publish and make readily available for use by PG_REQUESTER detailed interface documents for all hardware and software subsystems that are part of the PG. These interface documents shall be sufficiently detailed to permit PG_REQUESTER to replace hardware or software subsystems with enhanced hardware or software and to integrate applications supplied by PG_REQUESTER with the PG.

10.3.4 Management and Monitoring of Computing Networks

Commercially available, standards based network management products shall be provided, and shall employ SNMP standards. All PG resources, including processors and network devices, shall include SNMP agents for use by the configuration management tools.

PG network and IT management toolset shall be compatible with the monitoring tools used by PG_REQUESTER, which are provided in Attachment I.

10.3.5 Network Time Synchronization

Network time shall be maintained for all elements of the PG. Synchronization among the PG processors shall be made through the use of distributed time services. Each processor and console in the network shall periodically synchronize to the timeserver.

Processor clocks shall be automatically synchronized to within 1 µsec of the time reference unit. In the event that the time reference unit is not available, synchronization shall be suspended. The authorized system maintenance person shall be able to manually suspend the time synchronization service and manually update the processor clock through the user interface. If a processor’s internal clock and the time standard differ by more than an adjustable amount, synchronization shall be suspended and an alarm shall be generated.

10.3.6 Distributed Backup and Archiving

The PG shall include hardware, services, and procedures to backup, archive, and restore all PG software and data independently of its location on the PG networks. Once initiated, the distributed backup and archiving services shall automatically back up all information needed to recover from failures or data corruption without manual intervention by users. Although the devices being backed up may be physically separate, the backup system shall be managed centrally.

10.3.7 Diagnostics

The PG shall include all diagnostic software provided by the manufacturers of all hardware, including processors and peripheral devices, supplied with the PG. The PG shall also include error detection and diagnostic tools.

10.4 Application and System Development

PG_REQUESTER intends to incorporate new PG_SUPPLIER product offerings as well as product offerings from other suppliers on the PG. To manage and integrate these products and applications PG_REQUESTER requires tools to track changes that have been applied to the PG_SUPPLIER products and tools.

10.4.1 Off-Line Development Environment

The PG shall include an off-line Development Environment that shall enable PG_REQUESTER to update and test all system software (including operating system software, application software and associated models, database, and displays) in a manner that does not interfere with or jeopardize the integrity of the real-time operation of the PG. PG_REQUESTER prefers that the Training/Development system be used for this purpose.

The Development environment shall include all utilities required to develop and test new and modified software using a copy of the PG software. Facilities that shall enable PG_REQUESTER to transfer new and updated software from the Development Environment and integrate the new and modified software into the production (real-time) system without disrupting the operation of the production system shall also be provided.

10.4.2 Delivery of Source Code

The PG_SUPPLIER shall supply a compiled version of all executables with debug option to enable PG_REQUESTER personnel to view the source code for initial troubleshooting purposes. This compiled software shall be provided for all PG application and for all PG software that has been developed specifically for PG_REQUESTER's purposes.

10.4.3 Software Configuration Management

The PG shall include a software configuration management system to define the elements and the associated attributes of the applications provided in the PG. Currently, PG_REQUESTER uses software configuration products listed in Attachment I. Source definitions for the application's elements (such as source code, display formats, etc.), the residency requirements (such as local, shared), and any access attributes shall be defined through the software configuration management system.

10.4.4 Communications Diagnostics

The diagnostics for all communications interfaces shall provide at least the following capabilities:

1) Select any communications channel for test.

2) Select a request message for transmission to another computer.

3) Select single or cyclic message transmissions to another computer for test purposes.

4) Monitor displays of information received from another computer.

The PG_SUPPLIER shall provide a comprehensive set of communication support tools to support all communication interfaces. The communication support tools shall be integrated with the PG database, report, and display tools.

The support tools package shall provide at least the following capabilities:

1) Provide interactive access to all communication database parameters.

2) Facilitate the addition and modification of communication elements.

3) Provide error detection and recovery procedures.

4) Monitor and display data communication device status.

5) Provide communication statistics including the number of errors, retries, bytes transferred, etc.

Once modifications to the database or configuration have been validated, the database editor shall interface with network management services to re-initialize the appropriate links. Link reconfiguration shall not adversely affect the current communications processor functions.

Communications parameters shall be stored in the PG. On user request, the database management system shall print an annotated report listing all such parameters.

10.5 System Environments and IT Infrastructures

10.5.1 System Environments

The PG_SUPPLIER shall provide the software needed to support the following environments:

- Production

- Development (See Section 10.4.1)
- Testing and staging
- Training
- Disaster Recovery

The Production environment shall meet all system sizing and performance requirements as specified in Section 8. The DB_Supplier is requested to provide recommendations for the other environments.

10.5.2 Facilities

The DB_Supplier shall itemize all IT infrastructure requirements that it assumes that DB_REQUESTER would provide, for example, database management system, enterprise performance management, etc. Please see Enterprise IT common services in Sections 2 and 3 above.

11 Implementation and Sustainment Services

11.1 Quality Assurance and Testing

To ensure that the PG_SUPPLIER produces a well-engineered and contractually compliant PG, a quality assurance program shall be followed and both structured and unstructured tests shall be performed. PG testing and test documentation shall be performed in accordance with IEEE 829-1998 “Standard for Software Test Documentation”

All hardware and software furnished by the PG_SUPPLIER, including the PG_SUPPLIER’s standard functions and features that were not developed specifically for PG_REQUESTER, and all work performed under this Contract shall be inspected and tested. Except when early shipment of PG equipment is required, no hardware or software shall be shipped until all required inspections and tests have been made, thereby demonstrating that the system conforms to this RFP, and until the hardware and software have been approved for shipment by PG_REQUESTER.

PG_REQUESTER personnel and/or PG_REQUESTER-appointed representatives will conduct all PG factory tests with support as required from the PG_SUPPLIER. Some portions of the Site Acceptance Tests (SAT) will be conducted by the PG_SUPPLIER with PG_REQUESTER assistance as described in Section 11.1.8 of the RFP. Other portions of the SAT will be conducted by PG_REQUESTER with PG_SUPPLIER assistance (as described in Section 11.1.8). All tests shall be performed using PG_REQUESTER’s actual PG equipment.

11.1.1 Quality Assurance Program

The PG_SUPPLIER shall provide and maintain a Quality Assurance program that encompasses the entire project life cycle to ensure that all activities that affect the quality of the PG are adequately identified, controlled and documented. The QA program shall provide for the minimization of defects, the early detection of actual or potential deficiencies, timely and effective corrective action, and a method to track all such deficiencies. All PG deliverables, whether produced by the PG_SUPPLIER or a PG_SUPPLIER Subcontractor, shall be developed and maintained under a Quality Assurance (QA) program that meets the intent of the ISO 9000 quality assurance standards.

As a minimum, the PG_SUPPLIER’s inspection and testing procedures shall conform to Quality Standard ISO 9003. Such conformance shall be certified by an independent organization that is qualified and accredited to perform such certification. A copy of the Quality System Certificate shall be included in the proposal.

11.1.2 Inspection

Following proper notification, PG_REQUESTER shall have free entry into any of the PG_SUPPLIER's or the PG_SUPPLIER's Subcontractor's facilities where the PG hardware and software is being fabricated or tested. The intent of these inspections is to prove that the system is being fabricated in accordance with this RFP.

11.1.3 Test Plans and Procedures.

PG_REQUESTER-approved test plans and test procedures are required for all factory and site acceptance tests. Test plans and procedures for factory acceptance tests and site acceptance tests shall be developed and documented by the PG_SUPPLIER to ensure that each test is comprehensive and that any part of the test can be readily repeated. Test plans and procedures shall be designed so that PG_REQUESTER personnel can conduct the actual testing, including setting up the test, running the test, and monitoring the test results.

Test plans shall identify and describe in detail what tests will be performed, the test configuration for each stage of testing, the schedule for performing these tests, the "ground rules" and guidelines for conducting the tests, witness sign-off procedures, and procedures for handling variances.

11.1.3.1 Test Plans

Test plans shall identify and describe in detail what tests will be performed, the test configuration for each stage of testing, the schedule for performing these tests, the "ground rules" and guidelines for conducting the tests, witness sign-off procedures, and procedures for handling variances.

Particular attention shall be given in the test plan to the methods of simulating facilities that will not be available in the factory (such as interface to external systems and communication facilities), the method of simulating ultimate system loading conditions, and the method of demonstrating and verifying the results of PG applications.

Specifically, the test plans shall include the following:

- Definition of individual tests to be performed and purpose of each test
- Interdependencies between tests (i.e., what functions must be successfully tested prior to starting each test.)
- Test schedule
- Responsibilities of PG_REQUESTER and PG_SUPPLIER personnel
- Methodology for classifying, tracking and correcting variances
- Copies of certified test data to be used in lieu of testing
- Block diagrams of the hardware configuration(s) to be used during the testing

- Description of test equipment to be used during testing
- Methods used to verify the correct operation of advanced PG functions, whose results may be voluminous
- Method used to simulate equipment that will not be available during factory testing (communication facilities, PG interfaces to external systems, etc.)
- Method used to simulate the ultimate system loading under steady state and high activity state conditions during the performance tests
- Time allotted for unstructured testing.

Test plans shall be submitted to PG_REQUESTER for approval at least twelve (12) weeks prior to the start of the preliminary factory acceptance testing (Pre-FAT).

11.1.3.2 Test Procedures

The PG_SUPPLIER shall provide <u>detailed</u> test procedures for each PG function at least eight (8) weeks prior to the start of the Pre-FAT. The test procedures shall be written so that the tests can be conducted by PG_REQUESTER personnel who have completed the recommended PG training but are not intimately familiar with the PG functions and user interface. That is, the test procedures shall include exact step-by-step instructions on conducting each step (<u>all</u> steps shall be included – not steps shall be implied or omitted) with specific observations that should be made by test personnel following each step to ensure that the step was properly completed. <u>Test procedures that are not sufficiently detailed will be rejected by PG_REQUESTER.</u>

PG_REQUESTER shall have approval rights over all test plans and procedures. PG_REQUESTER will review the procedures to ensure that they thoroughly test each specified function, including PG requirements contained in this RFP that will be handled by the PG_SUPPLIER's standard and customized system functions.

As a minimum, factory test procedures shall include the following:

- Purpose of each test
- Function to be tested
- Pre-requisites for conducting the test (i.e., what tests must be successfully completed prior to beginning the test)
- Set-up and conditions for testing, including methods of simulating ultimate sizing and high/normal activity level and external interface.
- Exact step-by-step procedures to be followed
- Expected results
- Acceptance criteria
- Special equipment needed.

11.1.4 Test Records

The PG_SUPPLIER shall maintain complete records of all factory and site acceptance tests. Test records shall include:

- Test results for each test step, including a passed/failed indication.
- Description of any special conditions or deviations from the approved test plan
- Identification of persons conducting the test
- Descriptions of variances, if any, and their resolution.
- Signatures of authorized PG_SUPPLIER and PG_REQUESTER personnel participating in the test

11.1.5 Variances

A variance report shall be prepared each time a deviation from the approved test procedures is detected during testing. Variance reports shall also be generated upon observance of anomalies that are not specifically identified as necessary observations in the test procedures.

Variance reports shall also be used to track anomalies identified following the completion of the FAT and the SAT.

The variance report shall include a complete description of the variance, including:

- Time and date when the variance was discovered
- Description of test conditions at the time of the variance
- Identification of the specific test and test step (where applicable) during which the variance was identified
- Identification of witnesses
- Classification of the variance. The variance shall be assigned to one of the following classes by mutual agreement of PG_REQUESTER's test personnel and the PG_SUPPLIER's test personnel.
- Actions taken to eliminate the variance, including the repeat of testing of related functions that may have been impacted by changes implemented to eliminate the variance.
- Results of retesting following correction of the problem..

11.1.6 Communication Protocol Conformance Testing

The PG_SUPPLIER shall furnish evidence that all communication protocols used by PG_REQUESTER's PG have been conformance tested by an approved agency independent of the PG_SUPPLIER to demonstrate that all relevant requirements of the standard that defines the protocol have been satisfied.

11.1.7 Factory Acceptance Test (FAT)

Shipment of the PG shall be contingent upon the achievement of satisfactory results for the factory acceptance test conducted at the PG_SUPPLIER's factory. Factory testing shall demonstrate that all system hardware and software, including the PG_SUPPLIER's standard hardware and software that is not developed specifically for PG_REQUESTER, complies with these terms of reference.

All specified functions and interfaces between functions shall undergo thorough testing. PG functions that require facilities that will not be completely available in the factory (such as PG equipment that is shipped early, communication facilities, and interfaces to external systems) shall be simulated during factory acceptance testing.

11.1.7.1 Preliminary Factory Acceptance Test (Pre-FAT)

The PG_SUPPLIER shall conduct a Preliminary Factory Acceptance Test (Pre-FAT) that includes a complete "dry run" of the FAT using the approved test procedures. PG_SUPPLIER personnel shall conduct the Pre-FAT and shall certify to PG_REQUESTER that the Pre-FAT has been successfully completed..

PG_REQUESTER personnel shall have the right to witness all or part of the Pre-FAT; however, the presence of PG_REQUESTER personnel at Pre-FAT shall not be required. PG_REQUESTER will identify portions of the Pre-FAT that PG_REQUESTER is interested in witnessing, and the PG_SUPPLIER shall identify the specific dates on which the Pre-FAT testing of interest will be performed so that PG_REQUESTER may schedule its attendance during such portions of the test.

The Pre-FAT shall be successfully completed, and certification of successful completion shall be supplied to PG_REQUESTER, at least two (2) weeks prior to the start of FAT,

11.1.7.2 Test Setup

The following sections describe the required test configuration and the requirements for a test database and software simulators to support factory testing.

11.1.7.3 Test Configuration

The configuration of equipment used during testing shall include a fully configured PG including servers, communication processors, etc. and simulated interfaces to external systems to which the PG will be interfaced.

To the extent possible, the actual equipment that will be supplied to PG_REQUESTER shall be used during testing. The PG_SUPPLIER shall not use substitute equipment or cables except as a consequence of the early delivery requirements of these terms of reference.

This test setup shall be used to demonstrate the proper operation of the PG for the required PG application functions under all anticipated loading conditions (including the normal activity state and the high activity state).

The PG_SUPPLIER shall supply all necessary test equipment to simulate inputs to the PG during factory testing. This test equipment shall provide convenient mechanisms to vary PG simulated substation inputs over the full signal range of each point.

This equipment shall also enable the test personnel to simulate simultaneous changes to groups of points. This capability shall be used to simulate normal activity and worst case loading during the performance test.

Facilities that cannot be included in the factory test configuration, such as field communication facilities and the interfaces to external systems shall be simulated during factory testing. The proposal shall identify the proposed technique for simulating each external system.

11.1.7.4 Test Database

The database built by PG_REQUESTER using the PG development system shall be used during testing so that test personnel can demonstrate that this database has been properly implemented. In addition to PG_REQUESTER's database, the test database shall include additional test points that can be used to demonstrate all the functions and requirements of this specification, including the ultimate system capacity.

11.1.7.5 Basic PG Factory Acceptance Test

The basic PG test shall fully demonstrate that all PG_SUPPLIER-supplied hardware and software satisfies all requirements contained in this RFP. The basic test shall include, but not be limited to:

1) Demonstration that all hardware operates by a thorough exercising of devices, both individually and collectively.

2) Thorough demonstration of proper operation of all specified PG functions, including test cases with normal and exception data.

3) Demonstration of interfaces to external systems using PG_SUPPLIER-supplied facilities and PG_REQUESTER-supplied data files for simulating these interfaces.

4) Simulation of alarm and status change conditions

5) Demonstration of all user interface functions, including responses to erroneous operator entries

6) Simulation of failure conditions and failure of each system device that has a backup unit

7) Demonstration of the database software

8) Demonstration that spare utilization requirements have been met for the ultimate sized system.

11.1.7.6 Performance Tests

System performance and response shall be demonstrated during normal activity (steady state) and peak loading conditions (high activity state) by creating appropriate loading on the system and monitoring the response time, equipment utilization, and other items to determine the system performance under these conditions. The normal activity (steady state) conditions and worst-case conditions described in Section 7 of this RFP shall be simulated during the performance tests.

11.1.7.7 Unstructured Testing

A minimum of twenty (20) percent of the scheduled factory test time shall be set aside for “unstructured” exercising of the system hardware and software by PG_REQUESTER personnel. All variances identified during such testing shall be classified and resolved in similar fashion to variances uncovered during structured testing. Time delays caused by the system failures and the resolution of variances occurring during the unstructured testing shall be added to the total time allowed for unstructured testing.

11.1.8 Site Acceptance Testing

Site Acceptance Testing (SAT) shall be performed to verify that the system has been properly installed, and to demonstrate the proper operation of functions that could only be simulated during factory testing. The SAT shall also include an availability (endurance) test to verify that the PG is exhibits the required availability for each class of data over the specified test period when communicating with the full complement of PG_REQUESTER systems and components.

Special test equipment needed to conduct the site tests (if any) shall be provided by the PG_SUPPLIER.

The scheduling of all site-testing activities shall be coordinated with PG_REQUESTER. To avoid major impacts on PG_REQUESTERs, some of the site testing activities may be conducted at night or on weekends.

The following types of tests shall be included in the Site Acceptance Tests:

- Site Installation/Startup Testing (Section 11.1.8.1)
- Site Functional Testing (Section 11.1.8.2)
- Site Interface Testing (Section 11.1.8.3)
- Site “End-to-End” Testing (Section 11.1.8.4)
- Site Availability (Endurance) Testing (Section 11.1.8.5)

Some portions of the Site Acceptance Tests (SAT) will be conducted by the PG_SUPPLIER with PG_REQUESTER assistance. Other portions of the SAT will be conducted by PG_REQUESTER with PG_SUPPLIER assistance.

11.1.8.1 Site Installation/Startup Test

Site Installation/Startup test shall verify the proper installation of individual system components. This test shall verify that the individual major components of the PG have been properly installed and are operating correctly as individual units.

The Site Installation/Startup test shall be conducted by the PG_SUPPLIER with oversight by PG_REQUESTER personnel. PG_REQUESTER shall have the right to witness this test to ensure that the test is conducted as specified and to ensure that all variances that occur during the test are properly recorded and corrected by the PG_SUPPLIER.

11.1.8.2 Site Functional Testing

After the successful completion of the Site Installation/Startup tests,,Site Functional Tests shall be performed on the PG. The site functional test shall be a subset of the basic functional performance test performed in the factory. Particular emphasis during this test shall be placed on verifying that all outstanding variances from FAT have been corrected.

The Site Functional test shall be conducted by the PG_SUPPLIER with oversight by PG_REQUESTER personnel. PG_REQUESTER shall have the right to witness this test to ensure that the test is conducted as specified and to ensure that all variances that occur during the test are properly recorded and corrected by the PG_SUPPLIER.

11.1.8.3 Site Interface Testing

After the successful completion of the Site Functional tests, Site Interface Tests shall be performed on the PG. The objective of this test is to verify that the individual interfaces to external systems are functioning properly. During this test, the PG_SUPPLIER shall demonstrate that each external interface is capable of performing the PG_REQUESTER functional requirements for each interface using the specified integration architecture The PG_SUPPLIER shall simulate data transfers the PG and each external system in both directions (where applicable) using the actual interface hardware (adapters) and network facilities.

The Site Interface test shall be conducted by the PG_SUPPLIER with oversight by PG_REQUESTER personnel and its service providers. PG_REQUESTER shall have the right to witness this test to ensure that the test is conducted as specified and to ensure that all variances that occur during the test are properly recorded and corrected by the PG_SUPPLIER.

11.1.8.4 Site End to End Test

After the site interface test has been successfully completed for the individual major components of the PG and all system components have been installed and individually tested, an integrated system test shall be performed to demonstrate the complete end-to-end operation of the PG. The objective of this test is to verify that data transfers from PG are properly received and executed by the external system, and that external system transfers are properly received by PG. PG_REQUESTER personnel shall conduct this test, with technical support as needed from the PG_SUPPLIER.

The integrated system test shall include a full demonstration of system failure and recovery modes that are included in the dual primary redundant system. This test shall verify that the system fails over properly with no loss of data following individual processor failures and following the transfer of the controlling facilities between sites. System performance during communication network failures shall be demonstrated.

11.1.8.5 Availability (Endurance) Test

Following successful completion of the site installation/acceptance tests, an availability test shall be conducted to verify the PG's ability to meet its availability requirements while communicating with the full complement of devices and external systems. All variances against the system shall be resolved prior to the start of the availability test.

The PG shall exhibit the specified availability for each class of data over a 720-hour period in accordance with the availability criteria identified in Section 8 of this RFP. Total system availability shall be computed after adjusting for "hold" time. Hold time includes contingencies that are beyond the control of either party, and therefore will not be considered “down” time for the purposes of measuring system availability. Examples of “hold” time include power interruption and service response time. Such periods may be declared “hold” time by mutual agreement of PG_REQUESTER and the PG_SUPPLIER.

PG_REQUESTER will be responsible for conducting the availability test, which shall consist of normal system operation without special test equipment or procedures.

11.2 Documentation and Training

The PG_SUPPLIER shall furnish PG documentation and training that shall provide PG_REQUESTER personnel with a thorough understanding of the PG’s capabilities, use, system administration and maintenance. PG_SUPPLIER-supplied documentation and training shall enable PG_REQUESTER to develop a self-sufficient maintenance team. It is PG_REQUESTER’s intent to have complete operational and maintenance knowledge of the PG so that after the system has been installed and accepted, PG_REQUESTER’s technical staff may use, modify, and maintain the system with minimal assistance from the PG_SUPPLIER.

11.2.1 Documentation

The PG_SUPPLIER shall provide all of the documentation items described in this section for all PG hardware and software whether the hardware and software was developed by the PG_SUPPLIER or purchased from an Original Equipment Manufacturer (OEM). Documentation shall be subject to review and, for some documents, approval by PG_REQUESTER, as described in Section 11.2.1.2.

The documentation supplied with the PG shall reflect exactly the final as-built system. Errors or modifications to the PG resulting from the factory or site testing shall be incorporated in this documentation. The PG_SUPPLIER shall submit new manuals or drawings as required to ensure that the documentation supplied with the PG does in fact reflect the final system as delivered.

If the PG_SUPPLIER provides PG_REQUESTER with its own software or third party software, the PG_SUPPLIER shall submit a list detailing the function of the software and the latest revision of the software supplied to PG_REQUESTER.

11.2.1.1 General Documentation Requirements

All PG documentation shall accurately describe the PG as delivered. All changes to the standard documentation that are needed to accurately describe PG_REQUESTER’s PG shall be fully integrated into the document text.

All PG documentation shall be delivered in electronic and hardcopy form. The required quantities of electronic and hardcopy versions of the documentation are specified in Section 11.2.4. All text materials shall be typewritten including all revisions, notes, and corrections. Handwritten texts and/or notes are not acceptable.

Where a manual is revised to reflect a change in design, or a change for any other reason, each such revision shall be shown by a revision number, date, and subject in a revision block.

11.2.1.2 Documentation Approval Process

PG_REQUESTER shall have the right to review the documentation for all standard and non-standard hardware and software to ensure that the documentation is complete and accurately describes PG_REQUESTER's PG. In addition, non-standard hardware and software (i.e., developed or modified specifically for PG_REQUESTER) shall be subject to approval by PG_REQUESTER. The intent is to ensure that all required documentation is provided and that the documentation accurately describes the PG.

The PG_SUPPLIER shall submit documentation for approval by PG_REQUESTER for all hardware and software modifications to the PG_SUPPLIER's standard hardware and software required to conform to the requirements of this RFP. The PG_SUPPLIER shall not proceed with implementation of any modifications to standard hardware or software until the documentation has been submitted by the PG_SUPPLIER and approved by PG_REQUESTER. Any purchasing, manufacturing, and programming associated with changes to standard hardware or software initiated prior to PG_REQUESTER's approval shall be performed at the PG_SUPPLIER's risk. PG_REQUESTER will approve the document or submit comments to the PG_SUPPLIER within 10 working days after receipt of average sized documents. The design review schedule shall allow more time for larger documents.

The design document review schedule shall be arranged to minimize the burden on PG_REQUESTER's document reviewers. That is, draft documents for review shall be submitted on a schedule that minimizes the number of design documents PG_REQUESTER needs to review at any given time. More time shall be allotted for the review of large documents than small documents.

Documentation for the PG_SUPPLIER's standard hardware and software shall be furnished for PG_REQUESTER's review to verify the overall quality of the documents, but approval by PG_REQUESTER of these documents will not be required.

11.2.1.3 Document Identification

All documentation submitted by the PG_SUPPLIER shall be accompanied by a letter of transmittal and shall be submitted in a sequence that matches the project milestones of the PG. Each document shall be identified by a document number, drawing number, revision or issue number, and the date of release.

11.2.1.4 Document Submittals and Quantities

PG documents shall be submitted in the following quantities at the indicated steps of document delivery:

1) *Approval Submission* — One hard copy and one electronic copy (that can be edited by PG_REQUESTER for inserting comments) of all documentation shall be submitted for PG_REQUESTER's review and (for non-standard documents) approval.

2) *Final Submission* — Four hard copies and one electronic copy that can be reproduced by PG_REQUESTER shall be submitted of each final document that has been reviewed and (for non-standard documents) approved by PG_REQUESTER.

3) *As-Built Documents* — The final as-built PG_SUPPLIER-produced and OEM documentation shall be supplied in both hardcopy (paper) and electronic form (Microsoft Word so that the document is editable by PG_REQUESTER – PDF versions are not acceptable). One (4) hard copies and two (2) electronic copies of all documentation shall be submitted of the as-built version of all documents.

4) *As Built Drawings* — The final as built drawings shall be supplied in hardcopy (Mylar) form and electronic (Microsoft Visio) form. <u>Four</u> paper copies and <u>two</u> electronic copies of each as-built drawing shall be supplied.

11.2.1.5 Document Management Process

The PG_SUPPLIER shall utilize a quality control procedure for managing all documentation changes. The PG_SUPPLIER shall use a PG_REQUESTER-approved change management process for the PG_SUPPLIER copy of PG_REQUESTER's PG documentation.

11.2.1.6 Required Documents

As a minimum, the documents identified in the following sections shall be submitted.

11.2.1.6.1 System Functional Description

The System Functional Description document shall include a complete description of the functions performed by the PG. This document shall serve as a complete introduction to the PG and to the more specific hardware and software documents.

The document shall include an overview of the hardware configuration and indicate the functions of all major hardware components and/or subsystems. The Functional description document shall also identify the functions to be provided by the software. High-level hardware configuration block diagrams and software subsystem block and/or flow diagrams shall be included.

11.2.1.6.2 Hardware Documentation

The PG_SUPPLIER shall provide documentation for all PG hardware furnished to PG_REQUESTER. The hardware manuals provided for each OEM component of the system shall be supplied with the system.

The Hardware documentation shall describe the operational procedures and preventative maintenance procedures required as appropriate to keep the system in good operating condition. Hardware documentation shall included, but not be limited to, the items listed below. An inventory of all hardware documentation shall also be provided. The following hardware documentation shall be provided:

1) Configuration block diagrams showing the network configuration, as well as the logical and physical interconnections between the major hardware components,

2) Inventory of all PG hardware, including the manufacturer's name, model number, serial number, nameplate data, power consumption, and overall dimensions.

3) Physical planning/site preparation manuals containing detailed mechanical drawings of all equipment enclosures. Environmental requirements, such as operating temperature range, EMI/RFI susceptibility and standards certification, humidity operating range, vibration and shock limitations, and other such information, shall be identified for each hardware component.

4) Table of electrical power supply requirements for each hardware component.

5) Detailed installation wiring diagrams and cabling diagrams.

6) Assembly drawings for each enclosure

7) Jumper and/or switch settings for all applicable hardware components

8) OEM reference manuals and instruction books for all hardware.

9) Maintenance documentation, including manuals and other descriptive material, which will enable PG_REQUESTER personnel to maintain all PG equipment and test equipment.

10) Instructions for performing preventive maintenance

11) Diagnostic program user's manuals providing complete step-by-step instructions on the operation and interpretation of all on-line and off-line hardware diagnostic programs. These manuals shall identify symptoms, guides for locating faults, possible causes of trouble, and suggested remedial action.

12) Complete parts lists and breakdowns with sufficient descriptions to identify each component in the system, and ordering information for all hardware units.

13) Drawings showing the layout, detail dimensions, and mounting details of components

14) Control wiring diagrams

11.2.1.6.3 Software Documentation

The PG_SUPPLIER shall provide documentation for all software (including relevant firmware) to be supplied to PG_REQUESTER. An inventory of all software documentation shall be included. Software documentation shall include:

1) Description of the PG_SUPPLIER's change management process for all software.

2) A software overview document describing the system software on a subsystem basis.

3) Inventory of all software programs and modules and a cross-referenced index to the software documentation.

4) Software functional requirements document

5) Detailed description of interfaces between the PG and external systems (EMS, SMI, GIS, OMS, etc.)

6) Database documentation

7) Programmer reference manuals and documents

8) Reference and user manuals for all third party software packages.

11.2.1.6.4 PG User's Manuals

The PG_SUPPLIER shall provide a PG_REQUESTER-approved PG User's Manual containing detailed operating instructions and procedures for use by:

- Maintenance personnel

- Management personnel

The PG User's manual shall be divide into separate parts that are applicable to each of the user groups listed above. Information in each part of the manual shall be presented in terms that are meaningful to the specific users. That is, operator documentation shall not be presented as a programmer's manual. The manual shall include a description of the PG's functionality and usage as it relates to the specific PG user's tasks.

The PG User's Manual shall include detailed text descriptions of the PG functions. The Manual shall also include actual PG screen shots, flow diagrams, and other graphics and diagrams to illustrate and support the text information and aid the reader's understanding of the PG.

All user guidance and error messages shall be described, along with the steps necessary to recover from an error.

The PG user's manual shall also describe procedures to be followed as a result of computer system restarts or failures, including procedures for restarting the system, reconfiguring the system, and requesting the execution of diagnostic software.

11.2.1.6.5 Training Materials

The PG_SUPPLIER shall supply all materials used during training sessions, including all instructor materials and student materials.

11.3 Training Requirements

This section describes the requirements for PG_SUPPLIER-furnished training of PG_REQUESTER personnel. The training courses shall be oriented towards providing PG_REQUESTER personnel with a thorough understanding of the PG capabilities, comprehensive instruction in the operation of all PG components, and all hardware and software maintenance instruction required to develop a self-sufficient maintenance team.

At least half of the training time shall consist of "hands on" exercises for the trainees.

11.3.1 Training Plan

The PG_SUPPLIER shall provide a training plan and schedule to support the PG implementation schedule. The Training plan shall describe the specific training activities for each user group (e.g. system administrator, system maintenance, etc.

The training plan shall identify the recommended training courses for each user group. The Plan shall describe in detail the objectives and content of each course, recommendations on who should attend the course, the location of each course, the schedule for each course relative to other PG development and implementation activities, training course interdependencies (i.e., what courses must be taken before other courses), and required pre-requisites for each type of participant.

The Training plan shall be subject to approval by PG_REQUESTER.

11.3.2 Instructors

All training shall be conducted by qualified instructors that speak fluent English. Each instructor shall have had previous, formal classroom instructor experience in PG training and shall have a complete and thorough technical knowledge of the hardware and software supplied under this contract. The hardware instructor shall have a complete and thorough knowledge of test and laboratory hardware, diagnostic software, handbooks, guides and the use of tools and other aids in maintenance trouble-shooting and proper corrective actions for the system.

The instructors shall be able to present the materials in a manner that is most effective for the specific participants. Courses for control room operators shall be presented in terms that are familiar to the operators. Highly theoretical discussion of PG operations and algorithms is not acceptable for the control room operators and other non-engineers.

11.3.3 Training Materials

The PG_SUPPLIER and/or OEM shall prepare training manuals and instructor materials, and submit them to PG_REQUESTER ***prior*** to the start of classroom instruction with sufficient time for review. Each trainee shall receive an individual copy of the training materials.

The PG_SUPPLIER may utilize videotaped lectures as supplementary training material. However, videotaped lectures shall not serve as a replacement for a classroom instructor or as the primary training vehicle.

11.3.4 Course Content

The following sections identify the basic content of courses that shall be provided by the PG_SUPPLIER and/or OEMs.

11.3.4.1 Overall System Maintenance Training

The overall system maintenance course shall provide participants with an overview of, and hands on experience with, the PG functional capabilities and hardware and software diagnostic tools. This course shall cover all troubleshooting and debugging techniques available in the PG.

11.3.4.2 Hardware Training

The PG hardware training course shall provide all hardware training necessary to satisfy PG_REQUESTER’s requirement to develop a self-sufficient hardware maintenance team. The hardware training courses shall cover the operation, maintenance, and repair of all PG_SUPPLIER-supplied hardware. These courses shall cover actual equipment operation, interfaces between equipment, preventive maintenance procedures, and troubleshooting procedures, including the use of all special test equipment.

11.3.4.3 Software Training

The PG_SUPPLIER shall provide all training courses to satisfy PG_REQUESTER’s requirements to develop a self-sufficient software development and maintenance team. The software courses shall provide PG_REQUESTER personnel with thorough training on all PG software and all software tools and techniques used by the DA PG_SUPPLIER.

Software training shall include System administration, which shall provide participants with hands-on training maintaining and regenerating the operating system. This course shall include discussion of strategies and techniques used to expand and modify system software definitions, including the addition of new field equipment, consoles, and other devices to the system.

11.3.4.4 PG System Administration Training

PG_SUPPLIER shall train designated system administrators of PG_REQUESTER on how to manage PG and PMU/PDCdevice and signal registration with DB, manage PG user accouts, create and maintain PMU/PDC devicecommections, handle system events and alarms, monitor and tune PG QoS, system backup and restore, etc. .

11.4 System Implementation and Sustainment

This section specifies project installation, implementation, maintenance and sustainment requirements, including project management procedures, project documents, and other activities leading up to shipment of the PG. This section of the RFP also describes PG_REQUESTER’s requirements for post-warranty maintenance and upgrade services.

11.4.1 PG Testing, Shipment, and Commissioning

The transition of activities from the implementation of the system in the PG_SUPPLIER's facilities through testing, shipment, installation, and commissioning is crucial to the success of the project. This section sets out the sequence of these activities and expands on the responsibilities of PG_REQUESTER and the PG_SUPPLIER for these activities.

11.4.1.1 Authorization for Shipment

Acknowledgement of the successful completion of all factory acceptance tests shall be deemed as authorization for the PG_SUPPLIER to ship the tested hardware and software to PG_REQUESTER's site.

However, the PG_SUPPLIER shall submit an official notice of intent to ship at least one month prior to completion of the factory test. The notice shall indicate the contents, names of all carriers, estimated shipping weight, size of shipment, insurance provisions, date scheduled to leave the factory, and estimated date and time of arrival at PG_REQUESTER's facilities.

11.4.2 PG Installation Support

PG_REQUESTER will oversee the PG_SUPPLIER's personnel during installation and startup of the PG equipment PG_REQUESTER will also supply resources to assist with on-site coordination and logistics. PG_REQUESTER will also provide all field equipment and communication backbone facilities. PG_SUPPLIER will perform the Site Installation/Startup tests, the Site Functional Test, and the Site interface test with the PG_SUPPLIER's resource team to demonstrate that the system is operating correctly under PG_REQUESTER oversight. PG_REQUESTER will conduct the site end-to-end testing and the availability test with assistance from the PG_SUPPLIER as needed. During these site activities, the PG_SUPPLIER shall be on-site to ensure that the system is being properly installed and to ensure that problems experienced during equipment installation, startup, and testing are promptly addressed and corrected. The PG_SUPPLIER shall also provide on-site technical support to PG_REQUESTER throughout this period. The PG_SUPPLIER shall identify the required levels of support and skill sets for information or integration to external systems that PG_REQUESTER needs to provide. PG_SUPPLIER shall include the engagement models for working with PG_REQUESTER service providers and application sustainment teams.

11.4.3 Maintenance and Upgrade Program

This section specifies the requirements for hardware and software maintenance for the PG. This section also includes options for hardware and software maintenance after the warranty period.

11.4.3.1 Definitions

The responsibility for maintenance of hardware and software will vary depending on the time during the Contract. So that the times for changes in responsibility can be determined, the following definitions shall be used:

- *Delivery* – Delivery of any item shall be interpreted as receipt of the item at PG_REQUESTER's facility.

- *Commissioning* – Commissioning of any item shall be interpreted as receipt of the item at PG_REQUESTER's facility, installation on-site, successful completion of the site tests, correction of all variances from the tests and completion of formal acceptance by PG_REQUESTER/BCH.

11.4.3.2 Early Shipment of Equipment

Upon approval by PG_REQUESTER, some components of the PG may be shipped to PG_REQUESTER’s site prior to the successful completion of the factory acceptance test. The objective of early shipment is to expedite equipment installation and site testing activities.

As a minimum, the PG development system shall be shipped at an early stage (within two (2) months after award of contract) to enable PG_REQUESTER to gain familiarity with basic PG functionality and begin working on the PG_REQUESTER specific database and displays.

Early shipment will only be approved for components that are not required during factory acceptance testing to demonstrate that the functional and performance requirements contained in this RFP have been completely satisfied.

11.4.3.3 Hardware Maintenance

This section describes the PG_SUPPLIER’s and PG_REQUESTER’s responsibilities for maintaining the PG_SUPPLIER-supplied PG hardware. The PG_SUPPLIER’s hardware maintenance responsibilities shall vary depending on the stage of the project and the location of the PG equipment.

11.4.3.3.1 Prior to Shipment

The PG_SUPPLIER shall be responsible for maintaining all PG_SUPPLIER-supplied PG hardware components prior to shipping this equipment to PG_REQUESTER. This maintenance may be performed under a maintenance contract with OEMs or other parties or by PG_SUPPLIER staff using spare parts from the PG_SUPPLIER's stores or other sources. However, the PG_SUPPLIER shall not use spare parts to be delivered to PG_REQUESTER for this maintenance. PG_SUPPLIER is responsible to ensure no production hardware equipment is older than 6 months at the time of shipment.

11.4.3.3.2 Maintenance During Installation, Startup, and Commissioning

After delivering the PG hardware, but prior to the commencement of the availability test, the PG_SUPPLIER shall have the responsibility for maintaining all PG_SUPPLIER-supplied hardware that is installed in the operating control centers. PG_SUPPLIER-supplied maintenance for this equipment may be performed under a maintenance contract with OEMs or other parties or by PG_SUPPLIER staff using spare parts from the PG_SUPPLIER's stores or other sources. However, the PG_SUPPLIER shall not use spare parts to be delivered to PG_REQUESTER for this maintenance.

During this period, the PG_SUPPLIER shall be responsible for maintaining all PG_SUPPLIER-supplied PG components. PG_REQUESTER shall be responsible for PG_REQUESTER-supplied components of the system.

Failed equipment shall be replaced or repaired and spares inventories replenished to their delivered level throughout this period. Any spare parts found to be defective during initial delivery inspection or during this period shall be replaced within one week after notification. There shall be no charges to PG_REQUESTER for these replacement parts, including delivery charges. All spare parts replaced under maintenance shall be new parts unless otherwise accepted by PG_REQUESTER.

11.4.3.3.3 Maintenance Under Warranty

Maintenance during the warranty shall be in conformance with the terms of the warranty sections of this Contract. During the warranty period, PG_REQUESTER hardware maintenance responsibilities will include the following:

- Performing preventive maintenance and installing engineering changes as needed on the equipment
- Performing initial troubleshooting when problems occur.
- Performing corrective maintenance with remote support and (if necessary) on-site support from the PG_SUPPLIER
- Providing local assistance to the PG_SUPPLIER during the PG_SUPPLIER's on-site problem resolutions.

PG_SUPPLIER hardware maintenance responsibilities during this period shall include the following:

- Providing materials and instruction for appropriate engineering changes.
- Provision of technical guidance towards the resolution of all hardware problems for the PG equipment.
- When needed, the PG_SUPPLIER shall respond to requests for technical support using a remote diagnostic, dial-up connection within four hours, 24 hours a day, seven days a week
- Providing on site corrective maintenance if PG_REQUESTER is unable to make the necessary repairs

Failed equipment shall be replaced or repaired and spares inventories replenished to their delivered level throughout this period. Any spare parts found to be defective during delivery inspection or during this period shall be replaced within one week after notification. There shall be no charges to PG_REQUESTER for these replacement parts, including delivery charges. All spare parts replaced under maintenance shall be new parts unless otherwise accepted by PG_REQUESTER.

The PG_SUPPLIER's technical support staff shall work with PG_REQUESTER's technical staff to establish a strategy to efficiently resolve each identified problem. If at any time, PG_REQUESTER believes that the PG_SUPPLIER's technical support is not effectively resolving a problem, PG_REQUESTER may request that PG_SUPPLIER's staff or staff from the equipment's manufacturer be dispatched to PG_REQUESTER's facility. The PG_SUPPLIER's technical team shall be at PG_REQUESTER's facility within 24 hours to provide hands-on support towards the problem resolution. PG_REQUESTER will not be responsible for any expenses connected to the technical support, including travel expenses.

11.4.3.3.4 Post-Warranty Maintenance (Option)

As an optional service, PG_SUPPLIER shall provide post-warranty maintenance services for select PG_SUPPLIER-supplied hardware:

The maintenance contracts shall cover preventative and remedial maintenance, spare parts, and installation of all engineering, equipment, and field change orders and upgrades. PG_REQUESTER agrees to notify the PG_SUPPLIER of their intent to install any changes or upgrades so that their compatibility with the other elements of the PG may be determined.

11.4.3.3.5 Spare Parts, Tools, and Test Equipment

The PG_SUPPLIER shall recommend on-site spare parts for field-replaceable and -repairable modules for PG_SUPPLIER-supplied PG equipment. The spare parts to be supplied shall be adjusted by the PG_SUPPLIER during the project so that the delivered set is consistent with the delivered PG configuration. The recommended spare parts shall include any special tools and test equipment that the PG_SUPPLIER and the original equipment manufacturer (OEM) use and which are applicable for PG_REQUESTER’s maintenance.

All spare parts used to make repairs prior to and during the warranty period shall be replaced or repaired by the PG_SUPPLIER and spares inventories replenished by the PG_SUPPLIER to their delivered level throughout this period

11.4.3.3.6 Hardware Minimum Support Period

The PG_SUPPLIER shall guarantee the availability of spare parts and hardware maintenance support services for all PG equipment for a minimum period of ten years after the expiration of the warranty. Subsequent to this minimum support period, the PG_SUPPLIER shall provide to PG_REQUESTER a minimum of one year's advance notice of their intent to terminate such services.

11.4.3.3.7 Expendable Supplies

The PG_SUPPLIER shall supply all expendable supplies required for use during the project while the equipment is at the PG_SUPPLIER's facility. The PG_SUPPLIER shall also provide a list of recommended expendable supplies one month prior to any delivery of hardware to PG_REQUESTER's site.

11.4.3.4 Software Maintenance

The term software shall include all software delivered under this Contract, as well as the associated installation kits, release media, documentation, and support media such as on-line help facilities and maintenance tools.

11.4.3.4.1 Software Categories

Software shall be divided into two categories:

- *Category 1* – All software, whether supplied by the PG_SUPPLIER or a Subcontractor, exclusive of that software defined as Category 2.

- *Category 2* – Commercial 3rd party software, such as operating systems.

11.4.3.4.2 Pre-Delivery Maintenance

The PG_SUPPLIER shall have the responsibility for maintenance for all software prior to delivery. This maintenance may be carried out under a maintenance contract with OEMs or other parties or by PG_SUPPLIER staff.

11.4.3.4.3 Maintenance during Commissioning

The PG_SUPPLIER shall have the responsibility for maintenance of all Category 1 software after delivery and prior to commencement of the availability test. This maintenance may be carried out under a maintenance contract with OEMs or other parties or by PG_SUPPLIER staff.

PG_SUPPLIER shall have the responsibility for maintenance of all Category 2 software after delivery and prior to commencement of the availability test.

During this period, PG_SUPPLIER will make changes to databases, displays, reports, and application programs as necessary to meet PG_REQUESTER's operational needs. PG_REQUESTER agrees to inform the PG_SUPPLIER of all such changes at least 24 hours prior to installation of the changes. If the PG_SUPPLIER believes that the changes may adversely affect the operation of software for which the PG_SUPPLIER is responsible, PG_REQUESTER shall be notified of the potential problem and the changes shall be reviewed. Both parties shall work towards a mutually agreeable implementation of the desired changes.

11.4.3.4.4 Maintenance under Warranty

Maintenance during the warranty shall be in conformance with the terms of the warranty sections of this Contract. The PG_SUPPLIER shall have the responsibility for maintenance for all Category 1 software during the warranty period. This maintenance may be carried out under a maintenance contract with OEMs or other parties or by PG_SUPPLIER staff.

PG_REQUESTER shall have the responsibility for maintenance for all Category 2 software during the warranty period.

The PG software will likely be composed of PG_SUPPLIER's standard system elements, customized or specially developed elements, and several third party products. In order to facilitate the efficient maintenance of the PG software, the PG_SUPPLIER shall follow the general principle that software that is specific to PG_REQUESTER shall be implemented in specific libraries that are properly identified. This principle shall ensure that changes and upgrades to the PG_SUPPLIER's standard system software, applications, or third-party products can be implemented without affecting or interfering with the specific PG_REQUESTER software.

During this period, PG_REQUESTER will make changes to databases, displays, reports, and application programs as necessary to meet PG_REQUESTER's operational needs. PG_REQUESTER shall be under no obligation to inform the PG_SUPPLIER of such changes.

11.4.3.4.5 Post-Warranty Maintenance (Option)

As an optional service, PG_SUPPLOER shall provide post-warranty maintenance services for select Category 1 software:

11.4.3.4.6 Software Minimum Support Period

The PG_SUPPLIER shall guarantee the availability of upgrades, technical support for all PG software, and announcements of software and hardware releases applicable to the system for a period of ten years after the expiration of the warranty. Subsequent to this minimum support period, the PG_SUPPLIER and/or the PG software subcontractors shall provide to PG_REQUESTER a minimum of one year's advance notice of their intent to terminate such support.