H2: Protective Relay Applications Using the Smart Grid Communication Infrastructure

Working Group Members:

Mark Simon, Chair
Galina Antonova, Vice-chair
Alex Apostolov, Oscar Bolado, Patrick Carroll, Tom Dahlin, Kevin Donahoe, Mike Dood, Emmanuel Duvelson, George Gresko, Chris Huntley, Takahiro Kase, Tony Leszczynski, Bruce Mackie, Andre Marais, Bob McFetridge, Rene Midence, George Moskos, Dan Nordell, Bruce Pickett, Tarlochan Sidhu, Charles Sufana, Steve Turner, Mohammad Zubair

I Introduction:

Protection engineers now have available to them a range of new communications technologies which are being deployed as a part of the "Smart Grid." These technologies enable significant enhancement to existing protection applications, and also development of new applications never before practical. This report will help protection engineers to understand how Smart Grid communications technologies may be used to make this possible.

In the context of this report, the often-used term "Smart Grid" specifically applies to communications technologies that are useful for protection applications. (Many other applications are part of the Smart Grid, as the definition below illustrates.) These technologies include a range of capabilities, from local applications such as simple serial links and high-performance Ethernet networks, to wide-area fiber-optic networks covering areas the size of a city to a region, and even nation-wide data networks like the Internet. History shows that new technologies will continue to be developed over time, so this report is not specific to any particular technology but instead presents the requirements of different applications in general terms.

This report describes examples of the protective relay applications that can make use of the communication infrastructure provided by the Smart Grid. Each protective relay application example includes a summary description and the communication requirements necessary to provide suitable communication architectures, services, capabilities, and any other pertinent characteristics. The template for the summary descriptions is provided in the Appendix. It also provides a matrix summary of specific power system protection applications that use the Smart Grid communication infrastructure and their dependency on key communication requirements.

This information can be used to determine what requirements should be applied when specifying, designing or implementing a Smart Grid communication infrastructure. In sections of the network where multiple communication functions will take place, meeting the most stringent requirement will satisfy less stringent requirements. This technique is referred to as the "highest common denominator". Using the matrix summary, an

engineer can determine what requirements are important and determine the viable communication technologies for the Smart Grid infrastructure.

It is expected that a Smart Grid infrastructure will be made up of many different communication technologies. These will vary depending on the specific Smart Grid functions that are going to be implemented, feasibility of a solution, and overall strategy being taken. This report does not evaluate the communication technologies.

What is the Smart Grid:

The Smart Grid is not a tangible "thing" rather it is a collection of technologies and capabilities that have the following characteristics. In many cases, these are not new. However, their integration and customer focus may be. The following description is from the United States Energy Information Security Act (EISA) of 2007:

> (1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
> (2) Dynamic optimization of grid operations and resources, with full cyber-security.
> (3) Deployment and integration of distributed resources and generation, including renewable resources.
> (4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.
> (5) Deployment of `smart' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.
> (6) Integration of `smart' appliances and consumer devices.
> (7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal-storage air conditioning.
> (8) Provision to consumers of timely information and control options.
> (9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.
> (10) Identification and lowering of unreasonable or unnecessary barriers to adoption of Smart Grid technologies, practices, and services.

Abbreviations:

CCA	Critical Cyber Asset
CT	Current Transformer
CVR	Conservation Voltage Reduction
DNP	Distributed Network Protocol
DMS	Distribution Management System
DFR	Digital Fault Recorder
FCI	Faulted Current Indicator
FSC	Frame Sequence Check
GOOSE	Generic Object Oriented Substation Events
GPS	Global Positioning System
GSE	Generic Substation Event
HMI	Human Machine Interface
IED	Intelligent Electronic Device
IP	Internet Protocol
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
PQ	Power Quality
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SIPS	System Integrity Protection Schemes
UCA	Utility Communication Architecture
UTC	Universal Time Coordinated
VLAN	Virtual Local Area Network
VT	Voltage Transformer

II Examples of the Protective Relay Applications

This section contains the examples of the protective relay applications that make use of the communication infrastructure provided by the Smart Grid.

A) Dynamic Settings based on Smart Grid Measured Factors:

Load, Voltage Based
Feeder Configuration based
Seasonal Changes / Temperature
Distributed Generation / Variable In-feed

B) Reclosing Supervision based on Smart Grid data:

Based on pre-fault load (cold load pickup)
Based on Fault Magnitude
Based on computed fault location
Based on FCI data (1^{st} section inhibit)
Based on Feeder Configuration

C) Conservation Voltage Reduction Supervision based on Smart Grid data:

Metering data from Relays

D) Fault Locating:

Pre-fault location using FCIs
Branch Fault location using FCIs
Cable/Overhead, Location refinement using FCIs

E) Power Quality Data:

"Fault Anticipation". Location using Power Quality from Meters
Loose terminations

F) Time:

Local and wide-area

G) Application using Synchrophasors:

Wide-area situational awareness
Wide-area protection

H) Application using GOOSE:

Local and wide-area over a fiber optic network

I) Load Curtailment (Shedding):

At the feeder level from the substation based on real-time loading
On specific feeder subsections based on real time loading and distributed generation

J) System Integrity Protection Schemes

Wide-area or regional coordinated protection using communication infrastructure

A: Dynamic Settings based on Smart Grid Measured Factors

Purpose: Produce changes to protective relay settings based on real-time conditions of power system.

Function: Typically, settings are based on static configurations of the power system. Settings are determined so the protection will remain sensitive and selective under any operational scenario to which the relay will be exposed. However, fixed settings can be a compromise. Modern relays have settings groups which can be selected based on a defined set of conditions where changes to the relay settings will increase sensitivity while maintaining relay selectivity. Data from Smart Grid components can be used to determine the setting group scenarios and drive when to dynamically change these settings as operational conditions occur.

Example Operational Conditions and related measurements

- Load, Voltage-based
- Feeder Configuration-based
- Seasonal Changes / Temperature
- Distributed Generation / Variable In-feed

Operational Characteristics: How often data is required

Data can be delivered via a "report by exception" mechanism with a dead-band for analog data and based on status changes as switch positions, or similar devices, change.

Sources for the data

- Substation metering available from stand-alone metering equipment or from relays deliver real time bus voltage and feeder loading data.
- Status / Position of breakers, mid-circuit sectionalizing switches (automatic and manually operated), tie switches. These are located at the substation and along the feeder.
- Weather conditions such as temperature and wind. Regional or local lightning detection. Weather forecast messaging.
- Net metering or generation metering at source locations on the feeders. Both commercial and residential sources above generation level need to be available.

Data latency requirements for real-time data or historical data (Real-time = <5sec, Normal time <30 sec, Non-time critical <1 minute)

- Real-time field data is necessary for reclosing inhibit schemes.
- Real-time field data is necessary for settings changes resulting from a system configuration change that has resulted from a protection operation or changes in distributed generation.

- Normal time field data is necessary for settings changes resulting from a system configuration change that resulted from a manual change.
- Non-time critical field data is necessary for data that will be used for study to determine if settings are adequate for potential configuration changes.

Requirements for Data Quality

The field configuration data must be transported without any change. If the data is not available the last known data will be held over with a flag to indicate that it is stale. End devices that use the data will determine the behavior based on the quality.

Reliability

Field configuration data that is questionable due to error detection, checksum or security violations will be marked as invalid. The end device that will use the quality data will determine the outcome. Using the last known good data to determine the setting group or reverting to a specific setting group are the options.

Dependability

All field configuration data used for power system protection must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of messages are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Standards that exist

The use of standard protocols will allow interoperability between the various components that make up the data sources and the receptor of the data. Standard data protocols that meet the NIST framework are IEC 61850 and DNP. Standard transport and connection methods include IP and serial.

Gaps

None identified

Cyber security

Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field configuration data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not “require” adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

B: Reclosing Supervision based on Smart Grid data

Purpose:
Produce changes to the automatic reclosing settings based on real-time conditions of the power system.

Function:
Typically the automatic reclosing settings are static and historically have not been able to be adjusted based on the existing operating scenario. By receiving data from Smart Grid components, it is now possible to adjust the automatic reclosing settings in real-time.

Operational Characteristics: How often data is required
Data can be delivered on an event driven; report by exception basis.

What are the data sources?

- Gas and oil real-time chemical analyzers if the circuit breaker or transformer is so equipped
- Status/position of breakers, mid-circuit sectionalizing switches (automatic and manually operated), and tie switches. These will be located at the substation and along the feeder
- Status of fault current indicators (FCI)
- Status of any "distributed resource" generation
- Type of fault detected by the relay protection
- Equipment operational status (i.e. maintenance records indicating temporary equipment de-ratings)
- Revenue, net, or generation meters
- Weather monitors
- Weather forecast messaging
- Regional or local lightning detection

What are the devices that need to communicate?

- Circuit breakers and transformer monitoring equipment
- Sectionalizing switches
- Tie switches
- Chemical analyzers
- Fault current indicators (FCI)
- Distributed Resources
- Revenue, net, or generation meters
- Weather monitors
- Lightning detection systems
- Protective relays including automatic reclosing relays

Is the data real-time, retrieved from archive or both?
Real-time

What information does the data need to contain?

- Date and time stamp
- Position status of switch, bus tie, circuit breakers, etc
- Indication that a fault has occurred
- Voltage level
- Fault current level
- Protective relay status
- Fault location if available

Requirements for Data Quality

The data must be transported without any change. If the data is not available the last known data will be held over with a flag to indicate that it is stale. End devices that use the data will determine the behavior based on the quality. For automatic reclosing, it may be preferable to inhibit automatic reclosing until a determination is made as to what the issues are with the data.

Reliability

Data that is questionable due to error detection, checksum or security violations will be marked as invalid. The end device that will use the quality data could determine the outcome. Using the last known good data to determine the setting group, reverting to a specific setting group, or inhibiting automatic reclosing are options.

Dependability

All data used for power system protection and automatic reclosing must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of messages are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Standards that exist

The use of standard protocols will allow interoperability between the various components that make up the data sources and the receptor of the data. Standard data protocols that meet the NIST framework are IEC 61850 and DNP. Standard transport and connection methods include IP and serial.

Gaps

None identified.

Cyber security

Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not “require” adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

C: Conservation Voltage Reduction Supervision based on Smart Grid data

Purpose:
Produce changes to the Conservation Voltage Reduction (CVR) settings based on real-time conditions of the power system.

Function:
Adjust the Conservation Voltage Reduction settings based on the existing operating scenario. By receiving data from Smart Grid components, the required voltage levels may be obtained in an optimal manner. CVR schemes tend to contain two fundamental components; one for voltage optimization and one for reactive power compensation. Reactive power compensation is mainly achieved through the use of shunt capacitors. Voltage optimization is typically achieved through the use of voltage regulators.

Operational Characteristics: How often data is required
Status data can be delivered on an event driven; report by exception basis. Analog voltage and current data can be delivered on a sampled basis as often as every minute.

What are the data sources?

- Status/position of breakers, mid-circuit sectionalizing switches (automatic and manually operated), and tie switches. These will be located at the substation and along the feeder
- Status of any Distributed Resource generation
- Relay protection status
- Equipment operational status (i.e. maintenance records indicating temporary equipment de-ratings)
- Revenue, net, or generation meters
- Voltage sensors
- Current sensors
- Series capacitor banks
- Parallel capacitor banks
- Voltage regulators
- Transformer tap changers
- Series inductors
- Shunt inductors

What are the devices that need to communicate?

- Circuit breakers
- Sectionalizing switches
- Tie switches
- Distributed Resources
- Revenue, net, or generation meters
- Voltage sensors
- Current sensors
- Series capacitor banks

- Shunt capacitor banks
- Voltage regulators
- Transformer tap changers
- Series inductors
- Shunt inductors

Is the data real-time, retrieved from archive or both?
Real-time

What information does the data need to contain?

- Date and time stamp
- Position status of switch, bus tie, circuit breakers, etc
- Voltage level
- Current level
- Protective relay status
- Series capacitor banks status
- Parallel capacitor banks status
- Voltage regulators status
- Transformer tap changers status
- Series inductors status
- Shunt inductors status

Requirements for Data Quality
The data must be transported without any change. If the data is not available the last known data will be held over with a flag to indicate that it is stale. End devices that use the data will determine the behavior based on the quality. For CVR it might be preferred to revert to a normal operating voltage scenario or to freeze at the present voltage level should the data become unstable or stale.

Reliability
Data that is questionable due to error detection, checksum or security violations will be marked as invalid. The end device that will use the quality data could determine the outcome. Using the last known good data to determine the setting group, reverting to a specific setting group, reverting to the normal operating voltage, or freezing the voltage at the present level are options.

Dependability
All data used for power system protection and CVR must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of messages are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Standards that exist
The use of standard protocols will allow interoperability between the various components that make up the data sources and the receptor of the data. Standard data protocols that meet the NIST framework are IEC 61850 and DNP. Standard transport and connection methods include IP and serial.

Gaps
None identified.

Standards that don't exist
None identified.

Standards that need to be "enhanced" or updated that have not been identified by NIST
Presently each state has it owns rules governing what voltage levels are to be provided to the customer. In order to have a nationwide impact, CVR rules may need to be established on a federal rather than state basis. The overall impact may differ if the rules say that a certain minimum voltage level must be maintained at all times versus rules that would allow a lower minimum voltage level during times of a declared system emergency.

Standards indicating how low of a voltage consumer type equipment is allowed before the device no longer functions correctly need to be enhanced.

Cyber security
Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not "require" adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

D: Fault Locating

Description, Function and Purpose:
Various devices that can be applied to the distribution system as part of a Smart Grid can be utilized to provide information that can be used to determine the location of a system fault. This information can lead to prompt field location, circuit repair and outage restoration.

Operational Characteristics: How often data is required (continuous, event driven, random, sampled)?
Data is outage event driven and should be gathered within seconds or minutes of a fault occurring on the system to allow for analysis and use.

What are the data sources?
Data sources can include numerous devices depending on the application including: substation relay or recloser control, line recloser or smart switch control, line faulted circuit indicators (FCIs), customer meters, SCADA, digital fault recorders, and substation controllers/ HMIs.

What are the devices that need to communicate?
The devices listed above need to communicate either in a peer-to-peer fashion, or back to a location where the fault location analysis can be performed such as a substation controller or intelligent distribution management system (DMS).

Is the data real-time, retrieved from archive or both?
For fault locating and restoration purposes the data would be needed in near real-time.

What information does the data need to contain?
The information needs to contain either system quantities such as current and voltage, or calculated fault location data based on impedance models within the device itself. The information needs to contain a time stamp for correlation with other data. In addition, the substation controller or intelligent distribution management system needs to have a system model including impedances available to perform fault location calculations.

Requirements for Data Quality
The data needs to be delivered within seconds or minutes to aid in outage evaluation activities. It needs to be delivered without errors as errors could lead to erroneous fault locations thus potentially extending outage durations. While it is desirable for dependable data, redundancy is not required if there is a failure to deliver the data as traditional methods will be used in the field to determine outage location and restore the circuit. The use of this data aids in providing reliable service and generally is not related to safety issues as this function is not related to the base functionality of protective devices.

Standards that exist

- IEEE Std C37.111-1999 IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems.

- IEEE Std 1159.3 Recommended Practice for the Transfer of Power Quality Data.
- IEEE Std C37.114-2004 IEEE Guide for Determining Fault Location on AC Transmission and Distribution Lines.

Gaps
None identified.

Cyber security
Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment or DMS location due to the definition of the physical security parameters. While locations that are not CCAs may not "require" adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

Work groups that need access
Distribution system control and/or dispatch personnel typically use available fault location information during outage events to aid in restoration. Depending on the Smart Grid system functionality in place, other work groups may require access to the data such as protection engineering or relay test personnel.

Risks if data or access is breached
In theory, erroneous fault location data could be provided, resulting in extended outage durations.

Impact of security on the requirements
Security requirements may dictate the need to authenticate user access.

E: Power Quality Data

Purpose: To arrive at protection related decisions based on power quality measurements.

Function: Power quality measurements can be used to identify fault related conditions such as high impedance faults and developing faults. Once a condition has been identified the next step is to identify fault location. If Smart Grid components can be effectively deployed, then the data from these components can be used to identify and locate the condition. There are then two methods of data usage for fault identification. One method is where a high impedance fault occurs and the decision is made and an operation occurs. Additional data would be needed to identify fault location. The other method involves trending the power quality data. This is one way of tracking developing faults due to insulation breakdown. This data can also be used for tracking sources of harmonic distortion related to additions to the power system.

Operational Characteristics: How often data is required
For fault location after an event the data would need to be gathered for analysis within minutes. For trending purposes, data can be gathered on a periodic basis. This assumes that the data can be stored locally until the polling for the data takes place.

Sources for the data
Power quality monitors measuring current and voltage.

Devices that need to Communicate
The monitors will need to communicate to a data gathering point for fault locating and trending operations.

Real time or archived
For fault locating purposes the data would be needed in near real time, fast enough to enable restoration efforts. Trending operations would come from archived data.

Data needed
Besides the power quality data itself, the data needs to be time stamped.

Requirements for Data Quality
The data needs to be delivered unchanged. However, neither usage of the data requires high speed delivery.

The fault location function does need the data to be delivered within seconds. It must be data tagged to a specific time or event so it can be compared to coincident data. If the data is not delivered then the function is threatened. However, the function is meant to streamline fault location and shorten outage time therefore redundancy is not an obvious requirement. If the data is lost then the portion of the power system under question would have to be inspected. The outage will occur anyway so redundancy will not eliminate outages but may shorten them.

The developing fault function has less stringent requirements on the data. This is periodically polled data that if not delivered correctly the first time has many chances at resending. Speed requirements are minimal. Security requirements are important, if error data is accepted it may make trending difficult or impossible. Redundancy is unnecessary as failed delivery of data can be resent. If a monitor itself fails then the function cannot be performed but if replaced in a reasonable amount of time, the trending can continue.

Standards that exist

- IEEE Std C37.111-1999 IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems.
- IEEE Std 1159.3 Recommended Practice for the Transfer of Power Quality Data.
- IEEE Std C37.114-2004 IEEE Guide for Determining Fault Location on AC Transmission and Distribution Lines.

Gaps

None identified.

Cyber security

Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not “require” adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

F: Time local and wide-area

Purpose: Distribute accurate time to protective relays, Phasor Measurement Units (PMUs), Merging Units (MUs), Digital Fault Recorders (DFRs), SCADA locally and over wide-area.

Function:
Some protective functions rely on samples of analog values provided by geographically separated devices (e.g. line differential). Sample synchronization for these devices is essential for correct protection decisions.
Other metering and protection functions may use synchrophasor data, i.e. phasors relative to UTC time. PMU devices calculating synchrophasor data require precise synchronization to UTC time.
Fault recorders and SCADA functions require UTC time for event time stamping and timed controls.

Example Operational Conditions and related measurements.
Absolute time (referenced to UTC) is necessary for

- Synchrophasors data for metering and protection
- Digital Fault Recorders
- Merging Units used for Voltage and Current values.

Relative time is necessary for

- Current sample synchronization when the specific application can correlate current phasors between the acquired values. (line differential protection)

Operational Characteristics: How often data is required
Data (time) can be delivered periodically; the rate depends on quality of local oscillator at the receiving device. For IEEE C37.238 devices time is transmitted once a second.

Sources for the data
Grandmaster clock devices that are traceable to UTC, e.g. via GPS, can provide accurate time to all devices in a substation. These include Grandmaster clocks, grandmaster-capable Ethernet switches, PMUs, etc.

Devices that need to communicate
Sources of the accurate time need to distribute time to protective relays, PMUs, MUs, DFRs, SCADA, etc.

Data latency requirements for real-time data or historical data (Real-time = <5sec, Normal time <30 sec, Non-time critical <1 minute)

- Real-time data is necessary for PMUs (+/-1us timing accuracy of UTC).
- Real-time data is necessary for sample synchronization, e.g. MUs (+/-1us, relative time)
- Real-time data is necessary for event recorders (+/-1ms of UTC)
- Real-time data is necessary for visual indications (+/-100ms of UTC)

- Data (time) latency is corrected by the IEEE C37.238 protocol. Delays comparable to synchronization interval (1s) degrade or destroy time distribution service.

Note that communication path latencies can be asymmetrical, i.e. different in transmit and receive directions.

Requirements for Data Quality

Time at the grandmaster must be delivered without any changes. The message is updated en-route with path delay corrections. Updated data must be delivered without any change.

Reliability

Data that is questionable due to FSC check, grandmaster ID, message sequence ID is marked as invalid and discarded by the receiving device.

Dependability

All data used for power system protection must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of message are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Redundancy

Support for alternate source of time is required. Switching mechanism from one grandmaster to another is needed. System also should be able to be separated into operational time-synchronized islands upon failures or during maintenance. After separation it should be possible to converge these islands into a complete system with minimum disturbance to time and, therefore, operation.

Standards that exist

- IRIG Standard 200-04. IRIG SERIAL TIME CODE FORMATS – SEPTEMBER 2004, Timing Committee, Telecommunications and Timing Group, Range Commanders Council, US Army White Sands Missile Range, NM 88002-5110
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- IEEE Std 1588-2008 IEEE Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.
- IEEE C37.238-2011 IEEE Standard for Use of IEEE Std. 1588 Precision Time Protocol in Power System Applications
- ITU-T G.8265.1-2010 Precision time protocol telecom profile for frequency synchronization
- IEEE Std 1815-2010 IEEE Standard for Electric Power Systems Communications – Distributed Network Protocol (DNP3)

Gaps

- Wide-area precise time distribution (non-GPS).
- Cyber security.

Cyber security

Cyber Security is important but currently not supported by IEEE C37.238. The actual time at grandmaster is not a secret. However if an authorized device will masquerade itself as a grandmaster and transmit wrong time, disastrous outcome is likely for protection and other functions relying on correct time. It is possible to add authentication signature as an extension, but key distribution issues remain. There is no need to encrypt timing data. The use of VLANs addresses data security. IEEE 1588 provides an experimental extension for cyber security. Cyber security assessment for IEEE 1588 and IEEE C37.238 are under way at NIST-lead groups.

Security should be considered for the clock's user authentication to prevent unauthorized user access (specifically reconfiguration of offsets, clockID/IP and priorities).

G) Application using Synchrophasors

Description, Function and Purpose:
Synchrophasors (phasor measurements synchronized to an universal time) are used for power system monitoring, control and protection applications. Local and wide-area application examples include:

- Oscillation monitoring,
- Oscillation damping,
- Voltage stability monitoring,
- Thermal transmission line monitoring,
- Volt/var optimization,
- Island detection,
- Synchrocheck,
- Differential angle protection.

Operational Characteristics: How often data is required (continuous, event driven, random, sampled):
Data reporting rate varies from 1 to120 measurements per second.

What are the data sources?
Phasors (magnitude and angle) are obtained for CT, VT analog inputs.

What are the devices that need to communicate?

- Phasor Measurement Units (PMUs), standalone or as a part of multifunctional IED
- Phasor Data Concentrators (PDCs), at substation (aggregate) level and control center (super PDC)
- Control Center devices with processing and application functions

Is the data real-time, retrieved from archive or both?
Both archived and real-time data is used.

What information does the data need to contain.

- Phasor measurements (phase and magnitude)
- Timestamps
- Timesync and data quality information
- Note that precise synchronization to an absolute time (with 1us time accuracy) is needed

Requirements for Data Quality
None identified.

Reliability
Data reported must be reliable, especially if it is used for protection or other critical applications.

Security (errors are able to be detected)
Error detection mechanisms are embedded into the IEEE C37.118 protocol

Dependability
All data used for power system protection must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of messages are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Speed

- Data reporting rates vary depending on number of phasor measurements to be sent per second (1 to 120).
- Latency is a critical factor especially if synchrophasor data is used for protection applications or control applications such as oscillation damping.
- Two PMU types P and M have been introduced in the new IEEE C37.118.1 and IEEE C37.118.2 Standards to differentiate the amount of filtering required for a wide range of applications.

Redundancy
Redundancy is required. Duplicate data to be sorted out.

Standards that exist

- IEEE Std. C37.118-2005 Standard for Synchrophasors for Power Systems
- IEEE C37.118.1-2011 Standard for Synchrophasor Measurements for Power Systems, December 2011
- IEEE C37.118.2-2011 Standard for Synchrophasor Data Transfer for Power Systems, December 2011
- IEC TR 61850-90-5 Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118, May 2012.

Gaps
Phasor Data Concentrator requirements and Cyber Security requirements are not covered in the existing standards.

On-going activities include:

- North American Synchrophasor Initiative (NASPI) PSTT documents
- IEEE PC37.242 Draft Guide for Synchronization, Calibration, Testing and Installation of Phasor Measurement Units (PMU) for Power System Protection and Control, June 2012
- IEEE PC37.244 Draft Guide for Phasor Data Concentrator Requirements for Power System Protection, Control and Monitoring, June 2012

Cyber security

Cyber security requirements are not covered in the existing standards. These are covered in the Technical Report IEC TR 61850-90-5.

H) Application using GOOSE: Local and wide-area over a fiber optic network

Description
Generic Substation Events (GSE) is a control model defined as per IEC 61850 which provides a fast and reliable mechanism of transferring event data over entire substation networks.

Purpose:
When implemented, this model ensures the same event message is received by multiple physical devices using multicast service.

Function.
Generic Object Oriented Substation Events (GOOSE) is a communications control model mechanism in which any format of data (status, value) is grouped into a data set and transmitted where processing by the receiver must take place within 4 ms. The speed of the data transfer creates the potential to replace protection, control and monitoring substation automation functions typically served by conventional point-to-point copper wiring between:

- a relay and the primary equipment – e.g. reclosing
- relay to relay – e.g. breaker trip coordination
- a relay and the bay control unit – e.g. interlocking

Operational Conditions and related measurements.
GOOSE messages perform protection, monitoring and control functions within the range and typical values of environmental conditions and loading of conventional substations. GOOSE messages are suited to functions requiring fast response and commands.

Example: Blocking Based Bus bar Protection. (Zone protection coordination – if IED in primary zone fails, then next preferred IED performs backup contingency protection)

- Feeder Relay measures current, detects a fault, and sends multicast GOOSE message to indicate start of instantaneous over current protection.
- Main incoming relay (subscriber) receives multicast message as blocking function input, inhibiting the main incoming OC function, and allowing the feeder to operate, thus isolating the bus fault and maintaining service to other feeders.
- Except if the incoming relay detects an OC AND does not receive GOOSE "start" alarm, then change settings group on incoming line relay to act as secondary trip.
- Except if feeder relay is configured for auto reclose operation, then initiate auto reclose function – potentially controlled by GOOSE messaging
- Except if bay controller detects substation equipment is in "not ready" state, then bay controller executes alarm or automated sequence of actions to change /adapt substation state to ready for corrective action - potentially through GOOSE messaging.

Operational Characteristics

1. How often data is required between objects?
   - Data can be delivered via a "report by exception" for, 1) a change in analog data, 2) a state change of binary inputs or, 3) a calculation.
   - The standard IEC 61850 – 5 defines the characteristics of these events

2. What are the data sources?
   - Database Process Objects defined for system objects in the substation including station controllers, clocks, communication process units, etc.
   - Data sets (composed of data objects, attributes) of commands and measured values defined for the logical nodes of the physical and logical devices.

3. What are the devices that need to communicate?
   - Station Level IEDs – Station Controller, Station HMI, Gateways, RTUs
   - Bay Level IEDs – Protection relays, meters, etc
   - Process Level – Non Conventional Instrument Transformers & Merging Units

4. Is the data real-time, retrieved from archive or both?
   - GOOSE messages are updated in real time.
   - All GSEs are time stamped, archived and reported for review & retrieval.
   - Merging Units that supply the IED with measured values via the process bus for use with GOOSE messaging must fulfill the IEC 61850-9-2 (for both real-time and archived data) .

5. What information does the data need to contain? (IEC 61850 defines message types and further classifies messages into performance classes.)
   a. Message Types:
      - Type 1 Fast Messages (Status bits, Commands)
        - Type 1A : "Trip"
        - Type 1B " All Others: Examples: ""Close", "Reclose order", "Start", "Stop", "Block", "Unblock", "Trigger", "Release", "State change"
      - Type 2 Medium Speed Messages - where the time at which the message originated is important but where the transmission time is less critical.
        - Single measurements, such as a r.m.s. value for current and voltage
        - Time-tags set by the sender, to trigger timers in the receiver
        - Normal "state" information also belongs to this type of message.
      - Type 3 Low Speed Messages - complex messages that may require being time-tagged. This type should be used for slow speed auto-control functions, transmission of event records, reading or changing set-point values and general presentation of system data.

- Type 4 Raw Data Messages - This message type includes the output data from digitizing transducers and digital instrument transformers independent from the transducer technology (magnetic, optic, etc.).
- Type 5 File Transfers This type of message is used to transfer large files of data for recording, information purposes, settings, etc.
- Type 6 Time Synchronization Messages - This type of message is used to synchronize the internal clocks of the IED in the Substation Automation System (SAS). This includes those synch messages used for protection and control classified as T1, T2, and time synch for Power Quality, Types classified as T3, T4, T5.
- Type 7 Commands – "Other than described in Fast Trip." This type of message is used to transfer control orders, issued from local or remote HMI functions, where a higher degree of security is required.

b. Performances Classes.
   - P1 Distribution Type Substations
   - P2 Transmission Type Substations
   - P3 Transmission Type with time synchronizer and CB differential

GOOSE messages, as a control mechanism can deliver info contained in all types and classes of messages, however, because of their purpose and function, GOOSE messages tend to contain information typical of Message Types 1, 2 and 7 in all 3 performance classes.

Data latency requirements for real-time data or historical data

Latency is often used to mean any delay or waiting that increases real or perceived response time beyond the response time desired. This description is consistent for substation systems.

In this context, in order to maintain or exceed the performance of existing substation control systems operated either via human interfaces or automated control sequences, the GOOSE messaging transfer time should be less than 3ms for a Trip GOOSE command and 20ms for a Block GOOSE command as specified in IEC 61850-5 'Communication requirements for functions and device models'.

Example: By monitoring only the GOOSE messages on a substation communication network, a protection engineer, may retrieve archived packet data allowing post event historical correlation of the protection relay's real-time internal signals for 2nd harmonic inrush current detection and CT saturation which the relay's automated control sequence used to detect the blocking signal along with the trip signal.

Requirements for Data Quality

Operators require

- The right amount of data at the right time in order to perform and verify successful completion of control commands

- Process, station and network control data required to correctly manage objects based on user defined or automated sequences
- Real-time trend and process disturbance analysis data to perform and verify corrective actions
- Alarm data to initiate maintenance activities
- Power quality data to maintain contractual delivery requirements

Speed

The IEC 61850-5 standard defines in Annex B Table 5 28 types of PiCOMs (pieces of information for communication) along with transfer times that define the network response /cycle time in number of micro seconds. These PiCom Types are further classified according to the message Types 1 through 7 and Performance Classes P1, P2 and P3. The speed/transfer time for types common to GOOSE messages include:

- Type 1A **-** The requirements for Type 1A Trip messages are the most important.
  - For Performance Class P1, the total transmission time shall be in the order of half a cycle. Therefore, 10 ms is defined.
  - For Performance Class P2/3, the total transmission time shall be below the order of a quarter of a cycle. Therefore, 3 ms is defined.
- Type 1B **-** All other fast messages are important for the interaction of the automation system with the process but have less demanding requirements compared to the trip.
  - a) Performance Class P1, total transmission time shall be less than or = 100 ms.
  - b) Performance Class P2/3, total transmission time on order of one cycle, or 20 ms.
- Type 2 –Medium speed messages -
  - The total transmission time shall be less than 100 ms.
- Type 7 – Command Messages. **-** This type of message is based on Type 3, low speed messages with additional password and/or verification procedures. These command messages propagating over some control levels from the operator down to the switchgear or to some other controllable object may be converted to messages requesting Type 1 Fast Message properties at least on process level.
  - The total transmission time shall be less than 500 ms for Type 3 messages.
  - The transmission for Type 1 messages are proposed above.

Time Accuracy

GOOSE messages, if used for the purpose of time synchronization for protection and control events, must not degrade the time performance accuracy requirements for system wide synchronization

- The IEC 61850-5 defines in 13.7.6.1 time performance class requirements
  - T1 +/- 1ms for time tagging events,
  - T2 +/- 0.1ms for time tagging of zero crossings and of data for the distributed synchrocheck. Time tags to support point on wave switching.

Reliability

- GOOSE messaging requires mechanisms to assure data integrity - including those defined for Ethernet systems, virtual networks, and also schemes for enhanced retransmission.
- Systems must support short blast multicast messages that are more difficult to process.
- Reliability of the protection scheme is directly related to reliable delivery of the GOOSE message.

Security (data integrity)

- The Substation Automation communication system shall deliver reliable data in the presence of transmission and procedural errors, varying delivery delays, and equipment failures in the communication facilities. It must thus provide:
  - detection of transmission errors in the noisy substation environment;
  - recovery from link congestion;
  - optional support for link, media and equipment redundancy.

- The integrity and consistency of the data delivered by the SAS shall be as defined for integrity classes I1, I2 and I3 (3.5 of IEC 60870-4). The use of a specific integrity class shall be determined by the application that uses the delivered data.
- GOOSE messages are mapped into Ethernet frames. The Ethernet 4 -Byte Frame Check Sequence addresses data integrity and the need for GOOSE control mechanism to verify that errors are detected.

Dependability

- Redundant communication according to the IEC 62439 Standard
- In case of communications failure the target recovery time is zero seconds. There will be no communication interruption if one line fails and the other link simultaneously provides communication.
- IEC 62439 – 3 – Specifies Parallel Redundancy Protocol (PRP) and High availability seamless redundancy (HSR). This standard is approved, but an amendment on PRP is under development.

Standards that exist:

The IEC 61850 standard meets the NIST Framework for interoperability and the standard completely defines the GOOSE and GSSE messaging data structure, etc to allow system developers to plan and execute data transfers (status, measures and commands) between the various data objects of a physical IED (system objects) and the data sources/system objects receiving the served data.

Standards that don't exist

None identified.

Gaps:

None identified.

Cyber security

IEC 62351 – 6 addresses cyber security of the IEC 61850 protocol. Requirements will be included in Edition 2 of the IEC 61850 standard.

- Work groups that need access include Designer/Developers, Installers, Commissioners, Operators and maintenance technicians.
- Risks if data or access is breached:
    - Misoperations leading up to major outages
- Impact of security on the requirements:
    - Misoperations leading up to major outages

I) Load Curtailment (Shedding)

Description: Load Curtailment (Shedding) Supervision based on Smart Grid data

Purpose: Produce changes to the Load Curtailment settings based on real-time conditions of the power system.

Function: Adjust the Load Curtailment settings based on the existing operating scenario. By receiving data from Smart Grid components, the required load, voltage and frequency levels may be obtained in an optimal manner.

Operational Characteristics: How often data is required
Status data can be delivered on an event driven; report by exception basis. Analog voltage, current, frequency, and load data can be delivered on a continuous basis.

What are the data sources?

- Status/position of breakers, mid-circuit sectionalizing switches (automatic and manually operated), and tie switches. These will be located at the substation and along the feeder.
- Status of any Distributed Resource generation.
- Relay protection status
- Equipment operational status (i.e. maintenance records indicating temporary equipment de-ratings)
- Revenue, net, or generation meters
- Weather monitors
- Weather forecast messaging
- Regional or local lightning detection
- Voltage sensors
- Current sensors
- Series capacitor banks
- Shunt capacitor banks
- Voltage regulators
- Transformer tap changers
- Series inductors
- Shunt inductors
- System Integrity Protection Schemes (SIPS)

What are the devices that need to communicate?

- Circuit breakers
- Sectionalizing switches
- Tie switches
- Distributed Resources
- Revenue, net, or generation meters

- Weather monitors
- Lightning detection systems
- Voltage sensors
- Current sensors
- Series capacitor banks
- Shunt capacitor banks
- Voltage regulators
- Transformer tap changers
- Series inductors
- Shunt inductors
- System Integrity Protection Schemes (SIPS)

Is the data real-time, retrieved from archive or both?
Real-time

What information does the data need to contain?

- Date and timestamp
- Position status of switch, bus tie, circuit breakers, etc
- Voltage level
- Frequency level
- Current level
- Load level
- Protective relay status
- Series capacitor banks status
- Parallel capacitor banks status
- Voltage regulators status
- Transformer tap changers status
- Series inductors status
- Shunt inductors status

Requirements for Data Quality
The data must be transported without any change. If the data is not available the last known data will be held over with a flag to indicate that it is stale. End devices that use the data will determine the behavior based on the quality. For load shedding, it might be preferred to revert to a normal operating voltage scenario or to freeze at the present voltage or frequency level should the data become unstable or stale.

Reliability
Data that is questionable due to error detection, checksum or security violations will be marked as invalid. The end device that will use the quality data could determine the outcome. Using the last known good data to determine the setting group, reverting to a specific setting group, reverting to the normal operating voltage or frequency, or freezing the voltage or frequency at the present level are options.

Dependability
All data used for power system protection and load shedding must use a communication network that can deliver data reliably. A reasonable expectation is between 99 and 100% of messages are delivered. Better than 99% will be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability.

Standards that exist.
The use of standard protocols will allow interoperability between the various components that make up the data sources and the receptor of the data. Standard data protocols that meet the NIST framework are IEC 61850 and DNP. Standard transport and connection methods include IP and serial.

Gaps
None identified.

Standards that don't exist
None identified.

Standards that need to be "enhanced" or updated that have not been identified by NIST
Presently each state has it owns rules governing what voltage levels and frequency are to be provided to the customer. In order to have a nationwide impact, rules may need to be established on a federal rather than state basis. The overall impact may differ if the rules say that a certain minimum voltage level must be maintained at all times versus rules that would allow a lower minimum voltage level during times of a declared system emergency.

Standards indicating how low of a voltage consumer type equipment is allowed before the device no longer functions correctly need to be enhanced.

Cyber-Security
Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not "require" adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

J) System Integrity Protection Schemes

Description: System Integrity Protection Schemes (SIPS) based on Smart Grid data

Purpose: Communicate data to dynamically change SIPS arming selections based on the prevailing operating conditions, as well as initiate and transmit control actions throughout the distribution system.

Function: SG communications can provide the ability to adjust SIPS arming selections based on prevailing transmission and distribution system operating conditions, and transmit control actions to various distribution system elements. As the penetration of distributed generation connected to the traditionally radial distribution system continues to increase, SG communications is required to initiate targeted and coordinated control actions (e.g. load rejection, generation rejection, reactive power control, system separation/microgrid formation, etc) rather than tripping an entire feeder which may be counter-productive.

SIPS controller(s) at a distribution station may initiate control actions across the downstream distribution system in response to (1) commands it receives from a transmission system SIPS, or (2) distribution system instability, overload or other adverse conditions that the controller(s) detect using data received via SG communications. The controller(s) would need to determine the distribution system topology and SIPS arming selections either based on data received from the distribution management system (DMS), or directly from the distribution system elements, or a combination thereof.

Operational Characteristics: How often data is required
Status data can be delivered on an event driven, report by exception basis. Analog voltage, current, frequency, and load data can be delivered on a continuous basis, whenever predefined dead-bands are violated. Synchrophasor data may need to be communicated on a continuous basis.

What are the data sources?

- System Integrity Protection Schemes (SIPS)
- Status/position of breakers, mid-circuit sectionalizing switches (automatic and manually operated), and tie switches.
- Distribution Management System (DMS)
- Status of any Distributed Resource generation.
- Relay protection status
- Equipment operational status (i.e. maintenance records indicating temporary equipment de-ratings)
- Revenue, net, or generation meters
- Regional or local lightning detection
- Voltage sensors
- Current sensors
- Voltage regulators

- Transformer tap changers
- SVC/STATCOM controllers
- Series/shunt reactors/capacitors

What are the devices that need to communicate?

- System Integrity Protection Schemes (SIPS) controllers
- Distribution Management System (DMS)
- Circuit breakers
- Sectionalizing switches
- Tie switches
- Distributed Resources
- System dispatcher computers
- Revenue, net, or generation meters
- Lightning detection systems
- Voltage sensors
- Current sensors
- Voltage regulators
- Transformer tap changers
- SVC/STATCOM controllers
- Series/shunt reactors/capacitors

Is the data real-time, retrieved from archive or both?
Real-time and archived.

What information does the data need to contain?

- Control signals (trips, switching commands, etc)
- Position status of switch, bus tie, circuit breakers, etc.
- Voltage level
- Frequency level
- Current level
- Load level
- Synchrophasor data
- Protective relay status
- Voltage regulators status
- Transformer tap indications
- Series/shunt reactors/capacitors breaker statuses
- Date and timestamp

Requirements for Data Quality
The data must be transported without any change. If the data is not available the last known data will be held over with a flag to indicate that it is stale, and the SIPS cannot rely on this data. End devices that use the data can determine the behavior based on the quality. For load shedding, it might be preferred to revert to a normal operating voltage scenario or to freeze at the present voltage or frequency level should the data become unstable or stale.

Reliability
Data that is questionable due to error detection, checksum or security violations will be marked as invalid and should not be used for SIPS functionality. Relying on invalid data can potentially lead to transmission and distribution system instability, miscoordination, unintended island formation or equipment overloading. Hence the reliability, as well as performance, of the Smart Grid communications is very critical for correct SIPS operation.

Dependability
All data used for power system protection and SIPS must use a communication network that can deliver data reliably. A reasonable expectation is between 99% and 100% of messages are delivered. Better than 99% should be delivered within the required latency window. Data that is considered as critical will require a redundant communication path or an alternate means to obtain the data to achieve this dependability. If critical SIPS data is communicated over the same medium as other non-critical data, SIPS data should have higher priority.

Standards that exist.
The use of standard protocols will allow interoperability between the various data sources, controllers and actuators. Standard data protocols that meet the NIST framework are IEC 61850, IEEE C37.118 and DNP. Standard transport and connection methods include IP and serial.

Gaps
None identified.

Standards that don't exist
None identified.

Standards that need to be "enhanced" or updated that have not been identified by NIST

Cyber security
Locations that qualify as a NERC Critical Cyber Asset (CCA) require special consideration. It may not be possible to implement communication between field data and the substation equipment due to the definition of the physical security parameters. While locations that are not CCAs may not "require" adherence to NERC requirements, the use of a sound encryption and authentication is a recommended practice.

III Summary: Applications vs. Communication Dependency Matrix

The following is a matrix summary of specific power system protection applications that use the Smart Grid communication infrastructure and their dependency on key communication requirements. The dependency is identified by a rating between 3 and 0. 0 being a function that does not depend on the specific communication function and 3 where the function is completely dependant on the communication function.

The column to the far right in the matrix has the highest level of dependency on communications for a given requirement. This number is useful for determining what requirements should apply to the network architecture if all of the applications were to be implemented. The user can easily tailor the table to the applications they plan on using.

The row at the bottom of the matrix shows the overall dependence on communications in order for the application to function at a high level and deliver the benefits that the function can offer. The data in the matrix shows that the functions that rely on either real time data or produce a real time output are very dependant on communication. Functions that use archived data such as locating and power quality have a dependency on communications but are less time sensitive. These functions can tolerate a communication path with lower reliability as long as the data is delivered. For these functions, delays in the communication will produce delays in obtaining results, however delays are acceptable.

Table 1 Application vs. Communication Dependency Matrix

0 = no dependence on communication function
1 = some dependence on communication function
2 = moderate dependence on communication function
3 = completely dependant on communication function

Applications ->	Dynamic Settings	Reclosing Supervison	CVR	Fault Locating	Power Quality	Time	Synchro-phasors	GOOSE	Load Curtailment	SIPS	Highest Common Denominator
Communication Requirement											
Event Driven Data - Report by Exception	3	3	1	2	2	1	3	3	3	3	3
Continuous Data Flow - Streaming	1	2	3	0	1	3	3	3	3	3	3
Real-time data (less than 1 sec) In/Out	2	3	3	0	2	3	3	3	3	3	3
Archived Data (more than 15 seconds) In/Out	1	1	1	1	2	0	1	1	1	1	2
Latency (sensitivity to round trip time)	3	3	1	1	1	3	3	3	3	3	3
Data Integrity (sensitive to retries)	3	3	1	1	2	3	3	3	3	3	3
Speed (relys on consistant bandwidth)	3	3	1	1	1	2	3	3	3	3	3
Redundancy (requires redundant path)	2	1	1	2	1	3	3	3	2	3	3
Need for Two way communications	3	3	2	1	0	0	0	3	3	3	3
Need for Peer to peer communications	2	1	1	1	0	1	0	3	0	3	3
Dependable communication needed for dependable function	3	3	2	2	1	2	3	3	3	3	3
Cyber Security (negative outcome risk, 3 is high risk)	3	2	1	1	2	3	3	3	3	3	3
Reliability (overall reliance on communication for application function)	3	3	3	2	2	3	3	3	3	3	

IV How to use this information:

The matrix compilation is the result of the review by technical experts in the Power System Relay Committee. It is based on their viewpoint on how the applications would be affected by the performance of a communication path. As utilities study these applications they should use these results in the matrix and the descriptions as a starting point and compare the dependencies to their own needs. Upon compiling a similar matrix, the user can determine the "highest common denominator" for their communication network and the specific application they plan on implementing.

The individual communication technologies used for communication have many characteristics that can facilitate an application or prevent it from operating correctly. Some of these characteristics are due to the communication technology choice itself and some due to how and where the technology is implemented. It is outside the scope of this report to identify the characteristics of each communications technology, the relevant standards and best practices for the Smart Grid. How and where technologies are used is a critical step in the detailed design of each branch of the communication infrastructure. Additionally while cost is always a consideration, adherence to requirements should be a gate criterion.

Appendix: Template

Smart Grid is an evolving set of technologies. As such, this report is only a snapshot of the applications that the working group felt was likely to be implemented at the writing of this report. While there may be opportunities to update this report as additional applications become applicable and additional communications technologies become available it is unlikely that any report can be all inclusive. Below is a template so the user can customize this report to meet their own needs.

The following template was used for this report.

Outline Template:

Protection Application

- Description, Function and Purpose
- Operational Characteristics
  - How often data is required (continuous, event driven, random, sampled)
  - What are the data sources?
  - What are the devices that need to communicate?
  - Is the data real-time, retrieved from archive or both?
  - What information does the data need to contain.
- Requirements (Data Quality)
  - Reliability
  - Security (errors are able to be detected).
  - Dependability
  - Speed
  - Redundancy
- Standards that exist
  - Standards in the NIST framework document as "ready"
  - Standards in the NIST framework document that are assigned to a PAP (Priority Action Plan)
- Gaps
  - Standards that don't exist
  - Standards that need to be "enhanced" or updated that have not been identified by NIST.
- Cyber security
  - Requirements (NERC, basic or not needed)
  - Work groups that need access
  - Risks if data or access is breached
  - Impact of security on the requirements.