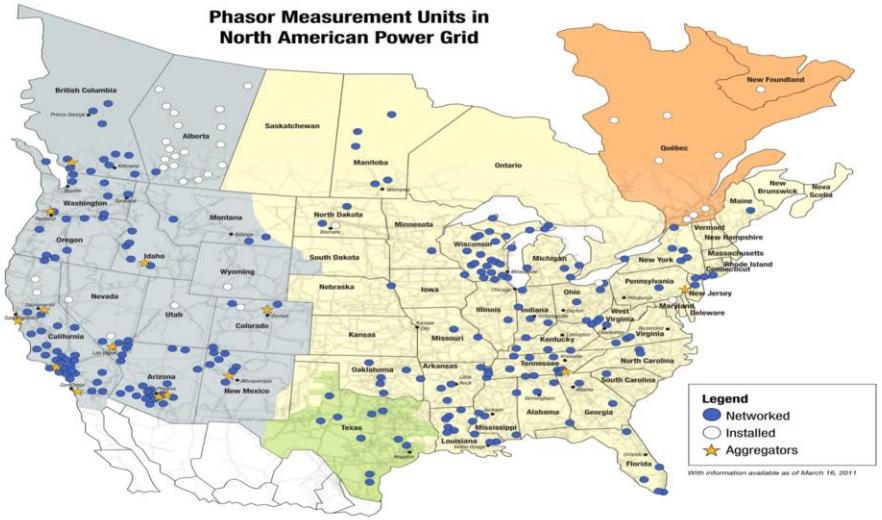
**Georgia Tech FDA 2013 Conference**

Vulnerabilities and Challenges on PMU and WAMS deployment

Authors:
Tribhuwan Choubey SCE/TDBU/C&Q
Ronald Lavorin SCE/TDBU/C&Q

Abstract:
Smart Grid is a conglomeration of cyber systems to cater for the need of distributed measurements, wide area visualization, monitoring and control to maintain the reliability, stability and security of the Grid, while catering to high power demand under already strained transmission, distribution and communication resources. Major subsystems of the Grid, like Generation facilities, substations, control centers and data centers are dispersed in a wide area and need robust networking and efficient communication. Phasor Measurement Units (PMU) and Wide Area Measurement Systems (WAMS) play a major role in providing a wide area visibility as well as a snap shot of the GRID to engineers for analysis of the system disturbances as well as producing developing trends towards dynamic instability or cascading outages. However these tools depend on judicious deployment across the network as well as efficient communication and data processing.
This paper attempts to bring out various vulnerabilities and challenges on the way of deployment of these technologies and countermeasures, being explored to meet the challenge effectively. Some of the numerous vulnerability/ challenges could be cited as below.

- NERC CIP Cyber Security implementation to minimize cyber threats
- Innovations in Communication technology to maximize throughput
- Judicious deployment of measurement, monitoring and control systems
- Inter-operability and data sharing among partner entities and regulators
- Robust modeling tools for accurate interpretation of developing trends
- Deployment of accurate time stamping and analysis tools

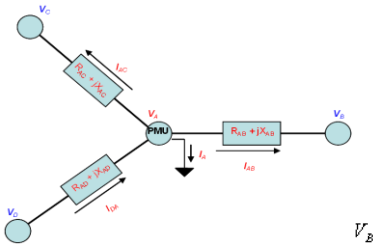



Kema conducted an independent study to analyze current status of various PMU applications deployment, potential deployments, infrastructure and cost gaps and also business benefits. Based on the analysis short term and long term deployment roadmaps were being developed.

Naspi (North American Synchrophasor Initiative) leads the initiative with exploring Synchrophasor applications to improve Grid reliability.

PMU placement rule 1: All neighboring lines emanating out of the node where a PMU is placed are deemed observable.

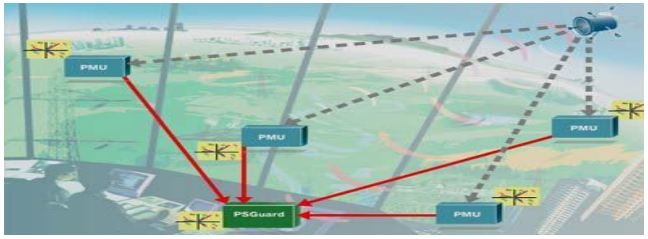
PMU placement rule 2: All neighboring buses to a PMU Bus are deemed observable.




$$V_B = V_A - I_{AB}(R_{AB} + jX_{AB}); \quad V_C = V_A - I_{AC}(R_{AC} + jX_{AC}); V_D = V_A + I_{DA}(R_{AD} + jX_{AD})$$

Satellite Signal Acquisition

Each GPS satellite simultaneously transmits its location and the current synchronized time. The signals arrive at a GPS receiver at slightly different times because some satellites are farther away than others. The GPS receiver observes the amount of time it takes for the satellite signals to arrive and estimates the distance to the GPS satellites. Typically, at any one time, 8




**Time resolution:**

Less than 1 Microseconds Measurement quality: 0.1% of voltage and current Angle accuracy of Less than 0.05°

satellites are visible from any point on the ground.

A typical GPS receiver requires four satellite signals to get a three-dimensional lock. Once calculated, many receiver algorithms assume that the receiver never changes altitude. In this state, the receiver estimates the distance to at least 3 GPS satellites for subsequent receive position and accurate time. Modern receivers simultaneously track 8–12 satellites in the GPS constellation. Averaging the information from each of these satellites allows for removing nonconforming time/position data. Annex E of the IEEE C37.118 standard states: “Overall, GPS is the only satellite system with sufficient availability and accuracy for phasor system synchronization.”

Developments at SCE

•Deployment of integrated DFR/PMU Units on 500kV and 220kV Systems to improve wide area situation awareness and control

•Migration of standalone Remedial Action Schemes (RAS) to a centralized RAS scheme (CRAS) to manage system wide stability in a coordinated way

•Implementation of unified communication scheme and SCE Net backbone to provide communication infrastructure to the current and future grid deployments and control needs

•Integration of all Operation protection and control systems under smart grid umbrella

•Advanced wide area early warning system using synchrophasor polling to reduce false trips, encroachment detection and wide area visualization

Following is the need of the applications on the network to have effective deployment to serve their purpose.

- State Estimation Application need full observability and therefore widely dispersed Synchrophasor placements
- Congestion Management Application need to be installed along Bulk Power transfer corridors
- Post Mortem Analysis applications need to cover at least Tie lines and Generation Sites
- Adaptive Relaying Applications need to cover crucial line terminals during contingencies
- Adaptive applications catering to special protection schemes or load shedding schemes need to cover interties, Generation sites and power transfer corridors
- Energy Marketing need wide dispersal covering Generation Sites, Power transfer corridors, Interconnection tie lines

Items below explain the communication needs for the applications

- Check Sync. Reclosing needs phase angle difference between Bus and Line to be measured every 250 msec and time quality error less than 100 micro seconds: needs mapping into GOOSE message
- Wide area out of step needs large angle difference and acceleration measurements from multiple stations requiring performance speed below 20 to 50 ms and communication rates between 30-120 data sets per seconds
- Synchrophasor based Backup Protection would need 25 to 60 datasets per sec communication speed between remote location to protection PDC
- Synchrophasor data sets from all the terminals involved in a multi terminal fault calculation need to be communicated as a GOOSE broadcast

Inter-Substation Communication

There are several functions that require measurements among multiple substations, specifically, Wide Area Out of Step protection, Double Ended Fault Location, and Black Start Line Synchronization. The functional requirements for each of these is outlined below:

Wide Area Out of Step

In this application, synchronized measurements from multiple different substations must be communicated either between selected substations or among several substations communicating a common location. Whereas in check sync reclosing, an angle difference of less than a setting was required, in Wide Area Out of Step, large angle differences and their acceleration are measured against settings. Magnitude of the phasor is not a major concern but may be used as a blocking/enabling function. The primary difference between Wide Area out of step is the speed of performance. In order to maintain stability in a swing condition, decisions need to be made in the 20 to 50 ms time frame. To meet these criteria, inter-substation communication rates from 30 to 120 synchrophasor data sets per second are required. Similar to check sync, before an action is taken, the application must validate the accuracy of the measured angles through the Time Quality parameter on each measurement.

Backup Protection

Backup protection on a power line is always installed for the case when a primary protection fails to perform its function. In the past, one popular form of backup protection was a distance element (known as Zone 3) that looked some electrical distance

past the end of the protected line. Given the availability of high-speed synchrophasor measurements, it is now possible to perform synchrophasor-based backup protection. Synchronized measurements can be streamed from one location to a Protection PDC (PPDC) at a data rate of 25 to 60 synchrophasor datasets/sec. The PPDC, receiving the multiple synchronized datasets, would have pre-formulated backup zones of protection where backup current differential calculations could be performed and surgical backup protection effected.

Power system low frequency oscillation detection (0.1 to 5 Hz) from hundreds of PMUs in the area would require 10 data sets per sec

For sub-synchronous frequency range on a 60 Hz system (15-45 Hz) oscillation detection 120 data sets are required to be communicated per sec

PDC-PDC communication could require communication speed up to 240 datasets per sec depending upon application

Operator interphase could be required to meet a data request rate up to 250 msec

Buffering would be required to maintain data transport reliability

WAMS – PMU Vulnerabilities

- Denial of service attacks on communication network rendering computational resources ineffective
- Injection of False measurement data to provide erroneous Grid snapshot to EMS operator
- Malicious data injection in between state estimation cycles to escape detection and inducing state estimation model errors
- Traffic analysis attack renders the system data for vulnerability analysis by attacker
- Signal processing challenges
    - Sampling rate collision – sampling rate for post mortem applications are much greater to that for the control applications
    - Resolution collision – Analysis applications need higher resolution in raw data processing than control applications
    - Availability of validated state of the art algorithm and post processing tools for processing wide area PMU data

Data Communication Challenge

- Communication infrastructure needs to be more flexible to move data at much higher speed requiring better communication bandwidth
- Time stamped data filtering irrespective of route is essential for transportation of right data packet to the application in need to perform right action in right time
- Data overhead due to internal fragmentation

Data Security

- Digital Communication links SONET/ T1/ Microwave/ Fiber Optics have their own vulnerabilities against cyber attacks through firewall penetration
- Flexible and open protocol structure ensuring interoperability, latency needs and security: marriage of GOOSE Messaging, C37.118, IEC61850, IP, UDP
- Changing security needs with open Grid systems would require end to end data integrity and Quality of Service: Meet CIP cyber security standards reqmt
- Public key based signing techniques a potential solution to the data integrity problem is not compatible to the low end legacy sensors
- In addition the algorithm adds to the latency issues on the network when compounded with data sharing and aggregation between control centers
- Network adaptability, in terms of latency is required to meet contingencies under attack or link failures

Data Sharing and Protection

- Each Interconnection should have a library of Synchrophasor data for base line analysis as foundation for event detection and real time remediation
- Application of uniform data naming and format conventions with an eye on interoperability
- Develop function specification and testing protocols for PMU and PDCs

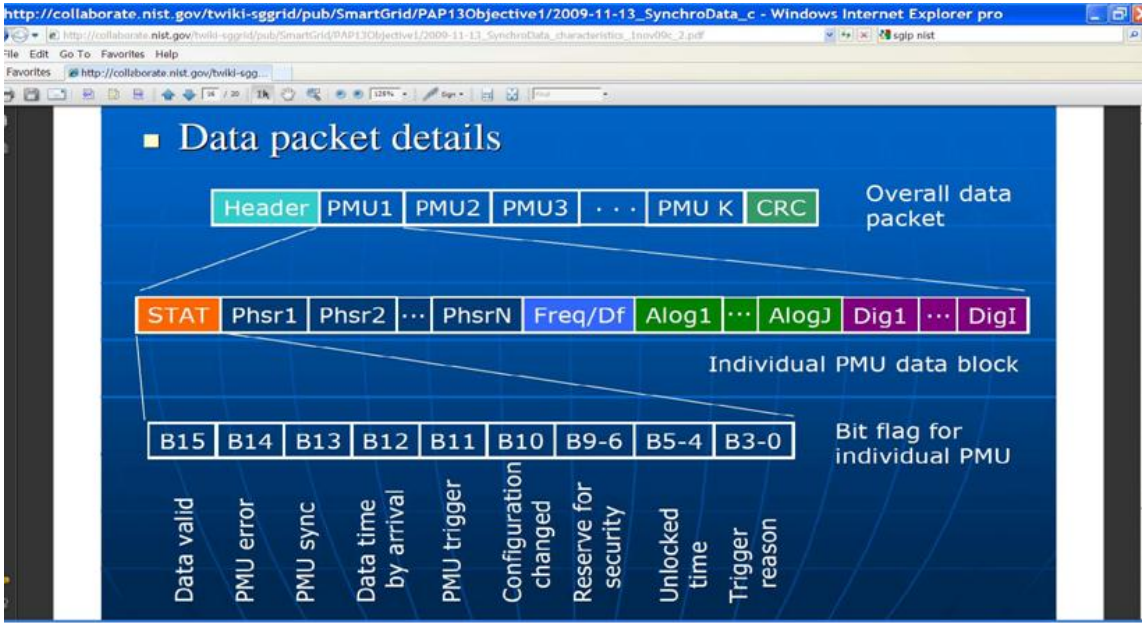
Data Security

- Trust management across organizations and third parties as well as maintenance of confidentiality is important to maintain data integrity
- Support to Special Protection System (SPS) applications is a reasonable goal in terms of time response (over several cycles) compared to protective relaying to prevent damaging oscillations (less than 1 Hz).
- Control action needs to be taken within 1 second of the occurrence of the event for SPS, but within a few milliseconds for protective relaying.
- Communication infrastructure must meet the need for integrity, Quality of Service , trust and latency requirements
- Meeting end to end latency requirement would need a guaranteed-rate packet transport scheduling algorithm rather than first come first serve algorithm
- This means that public internet is ruled out as a viable option as a communication platform, because of lack of authentication control as well as guaranteed rate packet transportation algorithm
- TCP/ IP networking thereby is not suitable for this communication because of unreliable delivery scheduling and timeout strategies to manage congestion
- Ongoing research is targeting to find alternate communication architecture which could meet the security and latency requirements of power system controls
- Secure data aggregating algorithm is also a topic of research to protect substation devices against malicious attacks

and accidental failures

- Smart Grid Interoperability panel is also working on communication architecture which could potentially provide a platform for induction of WAMS into production
- SGIP is in the process of modifying C37.118 to explore the use of UDP /IP multicast data streams instead of TCP/IP
- Network for the future need to handle traditional utility power delivery applications with vast amount of data from smart Grid applications including WAMS
- The time division multiplexing digital architectures need to upgrade to multicasting backbone architecture to accommodate a data transportation speed of 1-10GB/seconds

C37.118 Packet Data




Command frame

- Start/stop data, send other information

Data frame

- Phasor measurements
- Frequency measurement
- Analog data (user specified data type)
- Digital indications (Boolean,, 1-bit values)

Configuration frame

• Describes data frame, with scaling & naming

Header frame

• Text descriptions, user format

4 data types defined in C37.118:

Phasor measurements: Polar or rectangular components

Frequency: Absolute (F) & rate of change (dF/dt)

Analog

- Various – defined by user
- Single value continuous - control value, MW, etc..
- 16-bit integer or 32-bit IEEE floating point
- Phasor & frequency units defined in standard

Digital

• Boolean status represented in 16-bit word

Limitations:

- Security is not addressed
- Configuration of PMU devices is not included in the protocol
- Protocol will not scale to very large systems
- Communication methods are designated outside of the standard

61850-C37.118 mapping need:

61850 needs to

• Provide mapping & methods for phasor data

• Provide sufficient information for phasor use

C37.118 needs to

• Adapt to compliment 61850 methods

We need to

• Provide recommendations for operations outside of 61850

• Have a game plan for implementation

Communication Mode --------

Data sent on command: Data, configuration, and header

Requires two way connection

• TCP, UDP, serial

Spontaneous – data sent continuously without stop

• Data output pre-enabled, sent to pre-set destination. Requires only one-way communication. Configuration must be separately supplied

• UDP, serial

Network Communication Mode:

TCP

• Client connects, receives config, header, & data on request

• All communication through one TCP session

TCP-UDP

• Same as TCP but data sent separately on UDP

UDP-UDP

• No connection, client sends commands to server port

• Server sends config, header, & data to requesting host

Spontaneous

• UDP only, broadcast, unicast, multicast

Transmission Control Protocol (TCP): § Point-to-Point : One sender, one receiver

§ Connection Management - Connection oriented: handshaking (exchange of control messages) initialize sender, receiver state before data exchange

§ Reliable, in-order byte-stream data transfer - loss: acknowledgements and retransmissions

§ Flow control: sender won't overwhelm receiver - Pipelined

§ Congestion control: - Senders "slow down sending rate" when network is congested

Solutions to Challenges

•Induction of PMU data into WAMS could result into better observation of the system state through dynamic state modeling resulting in early detection of bad data or cyber attacks

•WECC has sponsored PDC WAMS link for the utilities to have a library Wide area snap shot of the Western Power Grid at secured nodal access points through distributed firewalls over NASPINet

•SGIP completed PAP13 tasked to map C37.118 with IEC61850 standard resulting into new C37.238 (Standard Profile for Use of Precision Time Protocol) published in July 2011 and IEC-61850-90-5 published in May 2012

•Dynamic State modeling in place of Static state modeling to detect spurious data injection and better forecasting

•Multilevel data authorization and authentication scheme which covers application level data authorization would detect and eliminate bad data injection to corrupt measured data

•Spoofing of GPS signals resulting into bad time synchronization could be offset with redundant time synchronization schemes, on synchronization error detection

•DFR/PMU/WAMS leading to control applications are considered to be NERC CIP impacted and need to be compliant to the cyber Security requirements

References


•PMU Specs - http://www.naspi.org/resources/pstt/martin_1_define_standard_pmu_20080522.pdf.

•North American Phasor Initative: PMU Installation http://www.naspi.org/pmu/pmu.stm

•Cyber Security Requirements challenge - http://www.naspi.org/meetings/workgroup/2009_february/presentations/nerc_cyber_security_mix_20090205.pdf

•WECC initiative - http://www.wecc.biz/committees/StandingCommittees/PCC/061709/Lists/Minutes/1/Revised_Draft_Proposal_WAMS_Network_Jan14_2009_v1.pdf

•SGIP PAP13 communication Mapping Plan– http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP1361850C27118HarmSynch

Contributors

•Tribhuwan Choubey & Ronald Lavorin – Compliance & Quality Group, SCE

•Acknowledgements – Sincere thanks to Reference Sources who have exposed this growing menace

•Presenter's (Tribhuwan Choubey) Bio – Electrical Engineering degree from BHU, India; 35 years experience in system design and testing in Steel, Aluminum and Power Sector, Disturbance Analysis and Smart Grid Cyber Security applications; Working with NIST on cyber security architecture and requirements of SGIP.