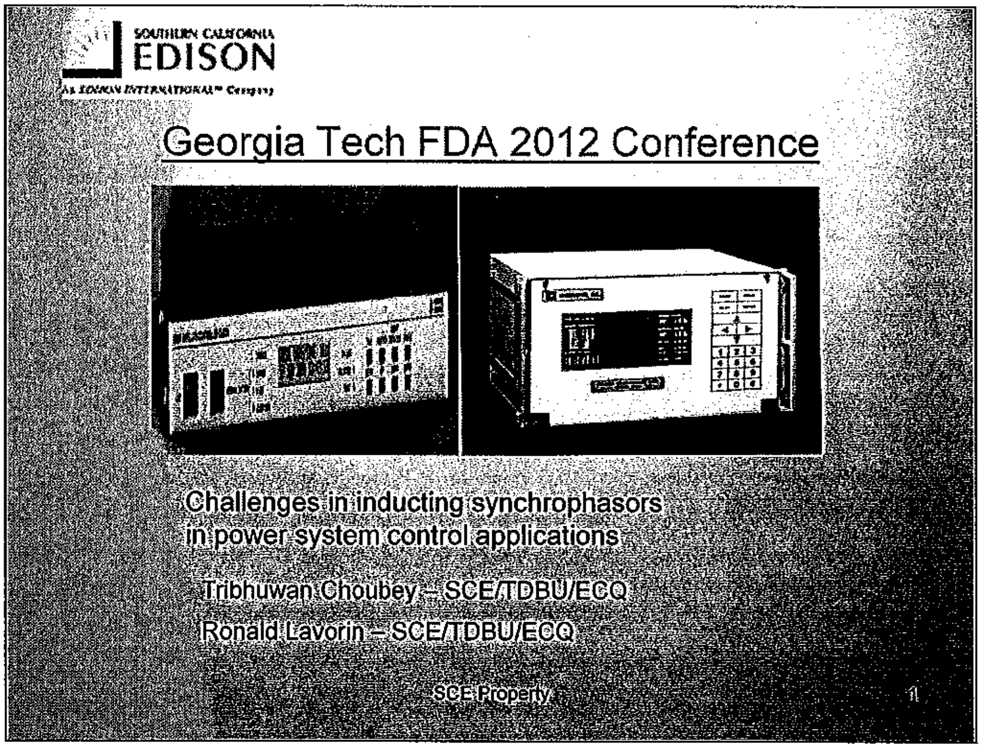


Phasor representations of voltages and currents at key locations throughout the power system define the state of the network. The Macrodyne Model 1690 Phasor Measurement Unit (PMU) provides instant access to this information providing new opportunities to understand and improve the performance of today's power systems.

Capable of both recording long duration electrical disturbances in phasor format and providing continuous phasor measurements in support of real time applications, the PMU adds a new dimension to power system monitoring.

Performance

Through the use of integral GPS (Global Positioning System) satellite receiver-clocks, PMUs sample synchronously at selected locations throughout the power system. Sequence phasors are continuously calculated and made available for system operators. Phasor values are also forwarded to a central master station where the phasor at several busses can be monitored with respect to a selected reference phasor or absolute time.

An extensive selection of flexible software triggers enables the PMU to capture disturbances on the power system in phasor format to support system studies and post disturbance analysis.

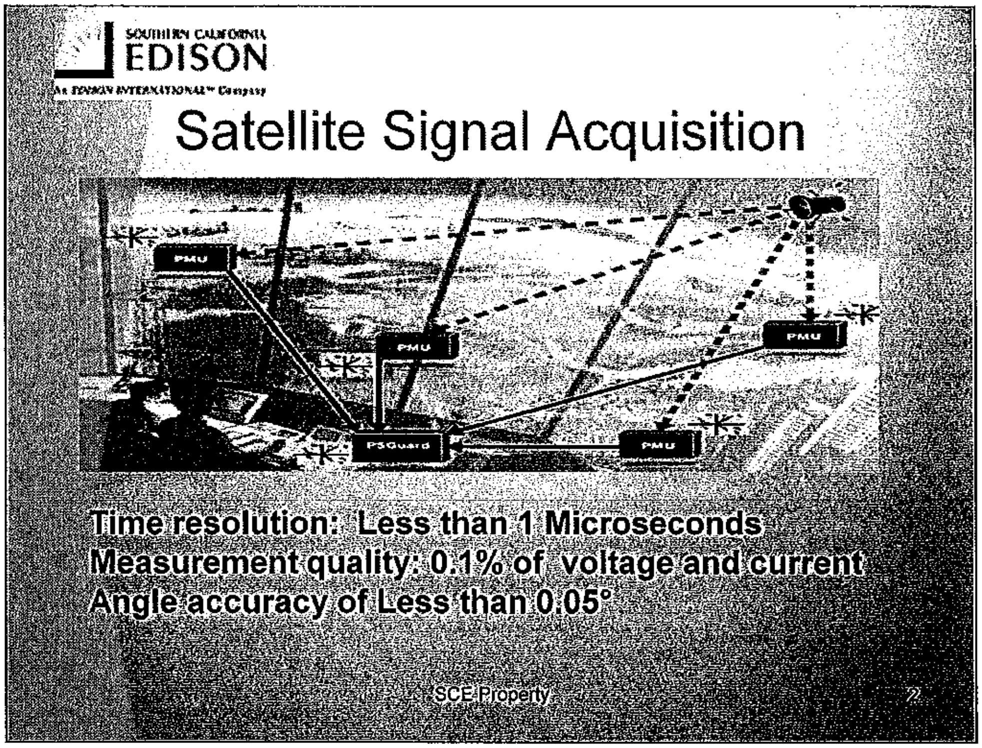
Remote triggering capability between units allows for the capture of disturbances on selected units or all units for a system level overview of an event.

==
======

The IEEE 1344-1995 in Annex F and IEEE C37.118 describe a modification to IRIG-B that incorporates additional information in the data, making this time code format more useful. Specifically, the extensions include 27 additional bits of information, including year, leap second, daylight-saving time, Coordinated Universal Time (UTC) offset, time quality, and parity bits. Synchrophasor systems require the use of these extensions. Additionally, typical synchrophasor systems monitor time quality bits to ensure that an accurate time reference is provided to the PMU, thus allowing precise angle measurements.

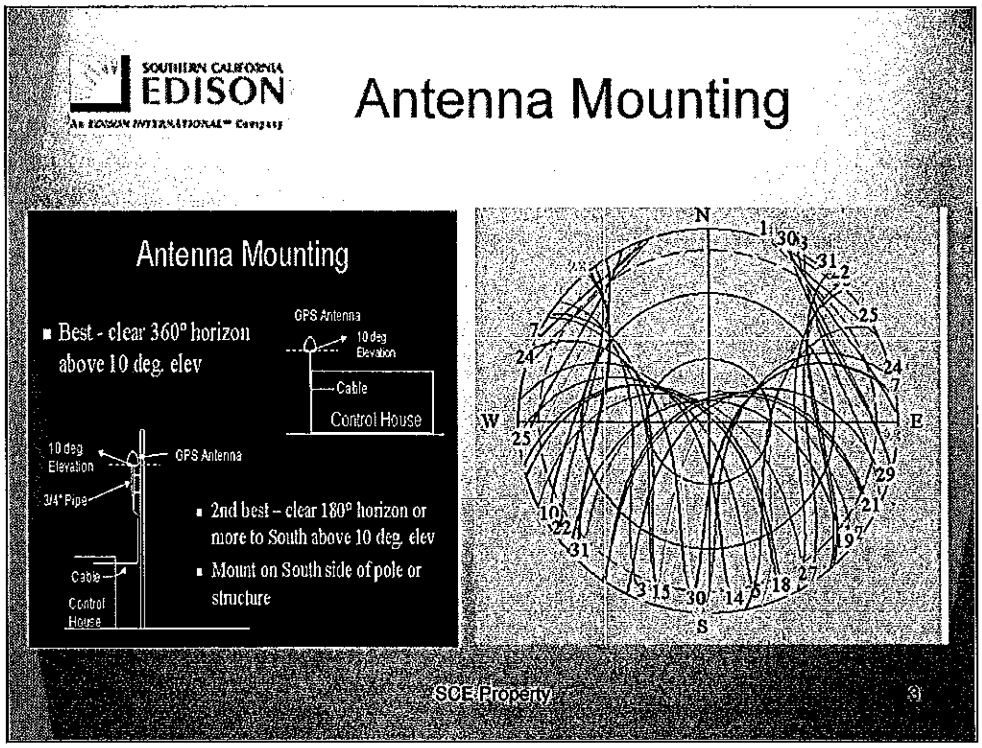
==

Convenience outputs from the PMU's integral GPS receiver-clock, including the one pulse / second GPS synchronizing signal, PMU sampling clock, an IRIG-B time code, fiber-optic time code and a one pulse / minute signal are readily accessible to support other substation applications requiring precise time coordination.



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 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."

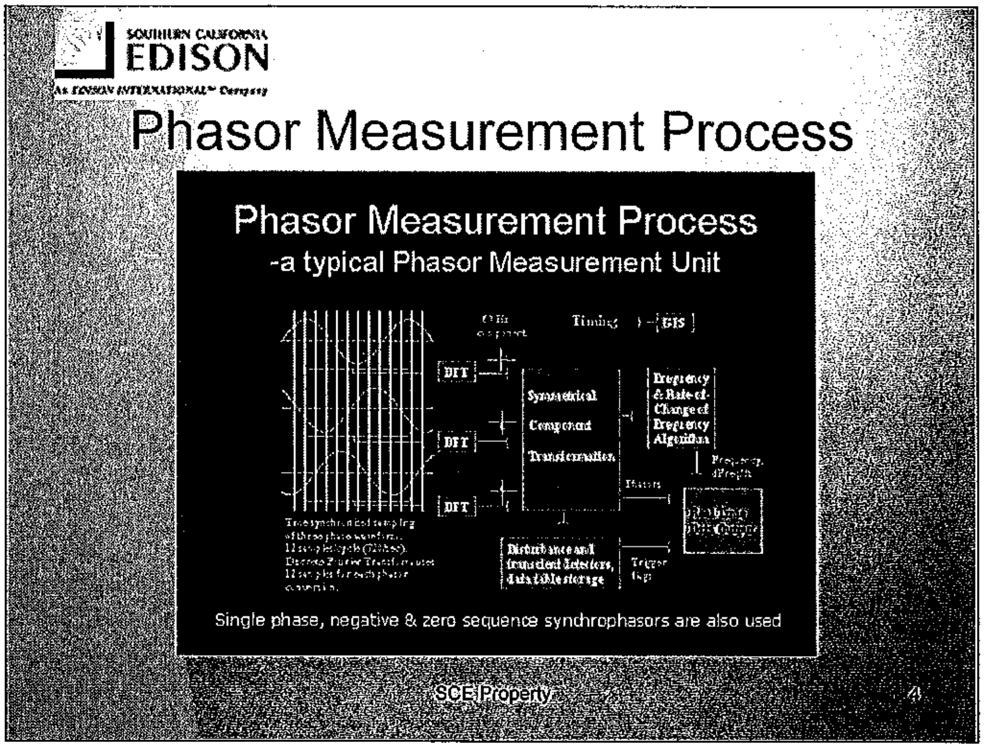


<u>Many PMUs input time from GPS directly, which requires an antenna open to GPS signals and a cable to the PMU within signal limitations. Antennas ideally have a clear sky view (free from obstructions) above a 15 degree elevation. In most cases this is difficult to achieve, and compromise factors need to be followed.</u>

Recommended antenna mounting locations on pole or roof. Plot of GPS satellite trajectories for 45° North latitude shows that best coverage is to the south.

Most of the signals will come from the south (in the Northern hemisphere) from the horizon to about 15 degrees north of vertical (Figure 2). Small obstructions more that 15" away from the antenna should not cause a problem, but a large flat obstruction within a few hundred meters could act as a reflector and cause multi-path problems. The antenna should be mounted with a clear view to the south and as far north as possible. Check around the mounting location for structures—such as a flat metal roof—that is oriented so that it could reflect a satellite signal to the antenna (keeping in mind satellites will traverse most points in the sky). Also check for

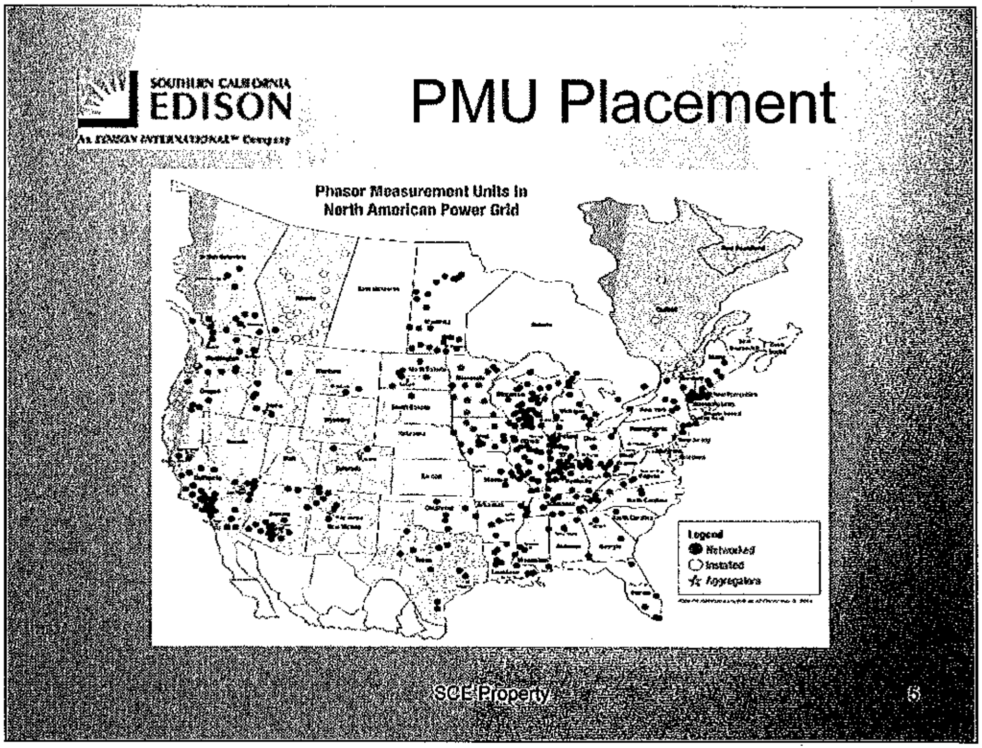
obstructions that can block the signal, and high power signal sources that could saturate the GPS input. Some GPS receivers have been operated successfully with the antenna mounted inside a building, receiving signals through the roof. In other situations mounting the antenna by a southerly facing window has been successful. Many less than optimal installations will experience some signal outage which degrades the measurement, so the safest option is an open air sky-view installation. The 1.5 GHz signal attenuates rapidly in a cable, and most vendors recommend limiting cable runs to less than 150 ft. There are alternatives for longer cable distances, such as high power antenna or in-line amplifiers and low loss cable. In many substations, roof access for cables is difficult, so a PMU should be located with this in mind. For an externally mounted antenna, it is advisable to incorporate a lightning arrestor into the design. Some PMUs input time from a local source, such as a GPS receiver, using a local signal type such as IRIG-B [5], 1 PPS, Have-Quick, IEEE 1588, or something similar. Some of these signals degrade rapidly in a cable, and all signals are delayed in cables, so excessive cable runs should be avoided. When using this type of PMU, consult the vendor as to what signals they require and whether the delays are compensated. Use a signal source that will provide the required signals at the accuracy at the PMU required for meeting timing requirements. For example, IRIG-B may be specified and can be used in any of its modulated forms, but the DC level-shift or the Modified-Manchester coding forms will allow the highest accuracy.



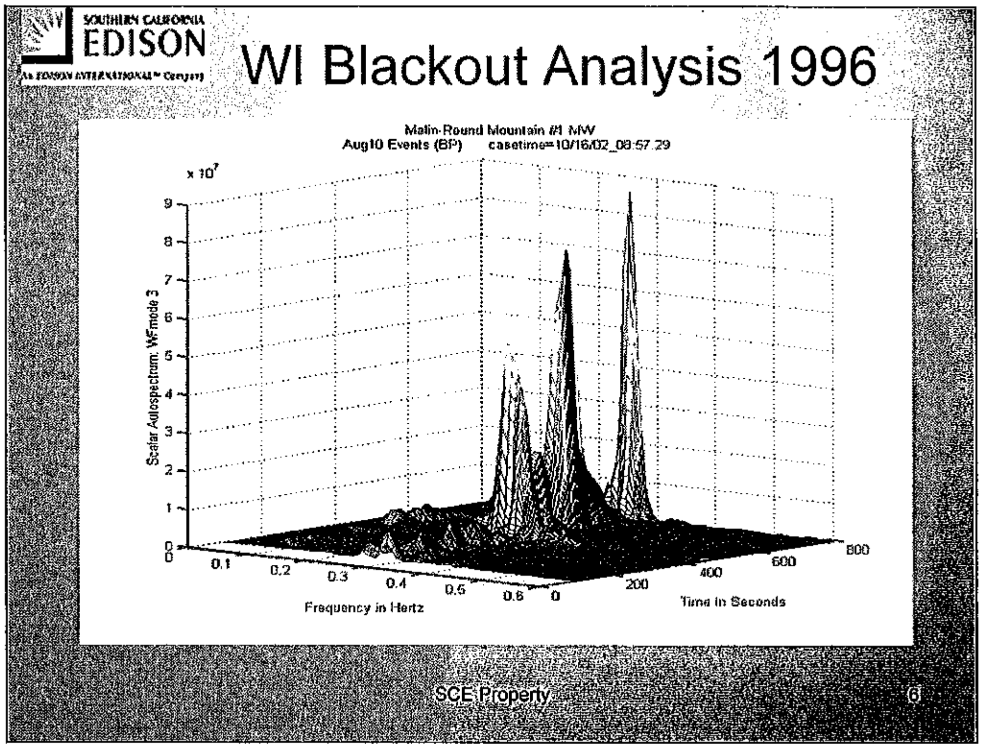
Operation

Voltage and current inputs to the PMU are derived from standard CT and PT secondaries. Input signals are isolated, filtered and sampled at an effective rate of 48 samples per cycle of the fundamental frequency. The internal GPS satellite receiver-clock coordinates the sampling process to ensure that data is sampled at the same instant in time by PMUs installed at remote locations throughout the power system.

A recursive DFT algorithm is used to calculate the local positive sequence, fundamental frequency and, voltage and current phasors from the sampled data. The resultant time tagged phasors are immediately available for local and / or remote applications via the standard RS-232 serial communications ports.



- 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.
- Over 200 PMUs installed on North American Power Grid (NASPI report to NERC).
- About 1000 PMUs expected to be installed and networked by 2014 (NASPI report to NERC).



1. Event August 10, 1996

When cascading outages occur in power grids, for example, the August 1996 Western Blackout

and August 2003 Northeastern Blackout, system situation decays over a period of time.

Spectral information obtained from Fourier analysis of August 1996 (blackouts clearly show two signs of this type of decay: increasing dynamic intensity and

Decreasing frequency. This serves as a means to monitor system dynamic status.

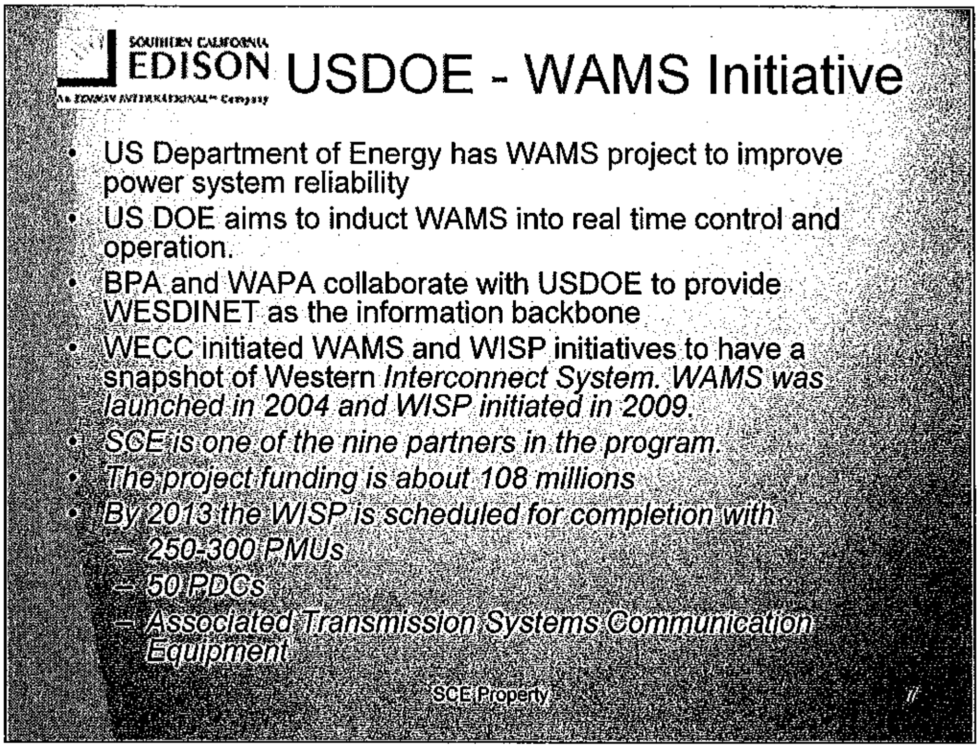
Ambient Activity...Keelan Alston Trip Oscillation Activity....Breakup Oscillation

Increasing Oscillations and decreasing Frequencies.

Early warning symptoms from 400 to 800 seconds = 6 minutes starting at Keelan Aston Trip...

Damping drop from normal 8% to 3.5%..lasting for 6 minutes and finally dropping to 0

Deterioration in damping is a positive sign of system stability problems. This can be used as a trigger to remedial action.



WESDINET – Western System Dynamic Information Network

USDOE - United States Department of Energy

BPA – Bonneville Power Authority

WAPA – Western Area Power Authority

WAMS – Wide Area Monitoring Systems; Link - http://www.osti.gov/bridge/servlets/purl/204701-kOaANH/webviewable/204701.pdf

SCE installed PMU's at most of its major 500 kilovolt and 230 kilovolt substations, technology that measures stress in the transmission grid based on the angle between the alternating current waveforms. Currently SCE is monitoring 20 PMU's collectively receiving approximately 150 phasors of data at a collection rate of 30 samples per second for each phasor. The amount of information collected and archived can be extreme, and the storage of this data as individual files typically makes its analysis difficult. SCE plans to install up to 8-10 PMUs I every year for the next few years as part of the WECC Synchro-phasor project.

The system at SCE is a real time interface that talks directly with the Phasor Data concentrator (PDC) through InStep's SyncPhzr interface then relays the information to InStep's eDNA Data Historian. The SyncPhzr interface provides the ability to archive and integrate phasor information using the standard IEEE

C37.118 protocol. The data is then displayed visually on displays and reports to operators and other engineers throughout the company.

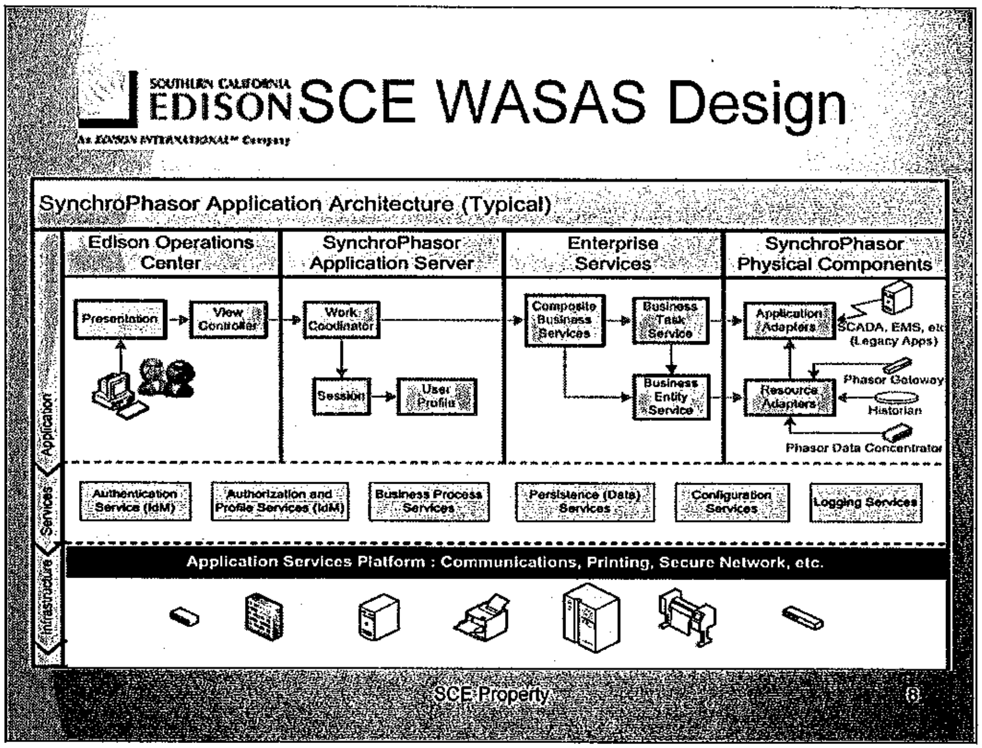
The storage system of the eDNA Historian allows for three very efficient archives of the data to be stored and used simultaneously by all users:

First archive: allows all of the data to be stored in its original collected resolution from all the PMUs on the system for a configurable period of time such as 120 days (rolling archive).

Second archive: provides a one second snapshot of the data that can be stored online for any desired period of time.

Third archive: provides storage of events so that a configurable amount of pre and post event data can be maintained online forever; used for determining faults in the system.

The eDNA historian can be easily interfaced with the EMS state estimator and supports the ability to seamlessly integrate time synchronized snapshots of this high fidelity data. InStep's CHaD object database software provides for the ability to organize the Phasor information using an object oriented approach. This provides for the ability to produce templates for the graphical displays using the meta data model that CHaD provides. Data can easily be exported out of the eDNA historian into the standard IEEE Phasor file format (DST). This will allow for direct and efficient comparisons of this data with historical data from other systems that do not have an advanced real-time database solution in place.



- Separate presentation, application, and data interface layers
- Interfaces between Presentation and application layers, Application and data input adapter

•Interface to NASPINET

==

PMU Site Selection Criteria – WECC Recommendation

Category Requirement Voltage Measurements

1. Major Transmission Paths

Transmission paths that have a rating equal to or greater than > 300 kV - 3-phase bus voltage - 3-phase currents in each

800 MW (amount is new) 3 line that is a part of the transmission path and meets voltage threshold

2. HVDC lines and Lines and links that have a >+/- - 3-phase phase links (new) rating equal or greater than 150 MW >+/ 200 KV 3 bus voltage

- 3-phase currents at its terminals

3. Large EHV station EHV substations that have > 300 kV - 3-phase (new) more than seven transmission elements (lines, transformers)

Connected 3 bus voltage - 3-phase currents in each transmission element

4. Large generating Substations that have total > 200 kV - 3-phase power plants more than 1000 MW of generating capacity connected

3 bus voltage - 3-phase currents in each powerhouse line

5. Individual Generator units greater than MW (Note > 200 kV - 3-phase bus voltage - 3-POI 13 generating units 150 see 2) 3 phase currents

6. Intermittent Generator units greater than Any - 3-phase bus voltage generating units - 3-(new) 100MW 3 phase currents at POI

7. Critical generating facilities Power plants whose outage will reduce a rating of a major transmission path (defined above) > 200 kV - 3-phase bus voltage

- 3-phase currents at POI by 5% or 100 MW

8. Dynamically Controlled Devices Synchronous condensers, static VAR compensators and all FACTS MVA > 200 kV - 3-phase bus voltage

- 3-phase currents devices greater than 100 rating not otherwise included.

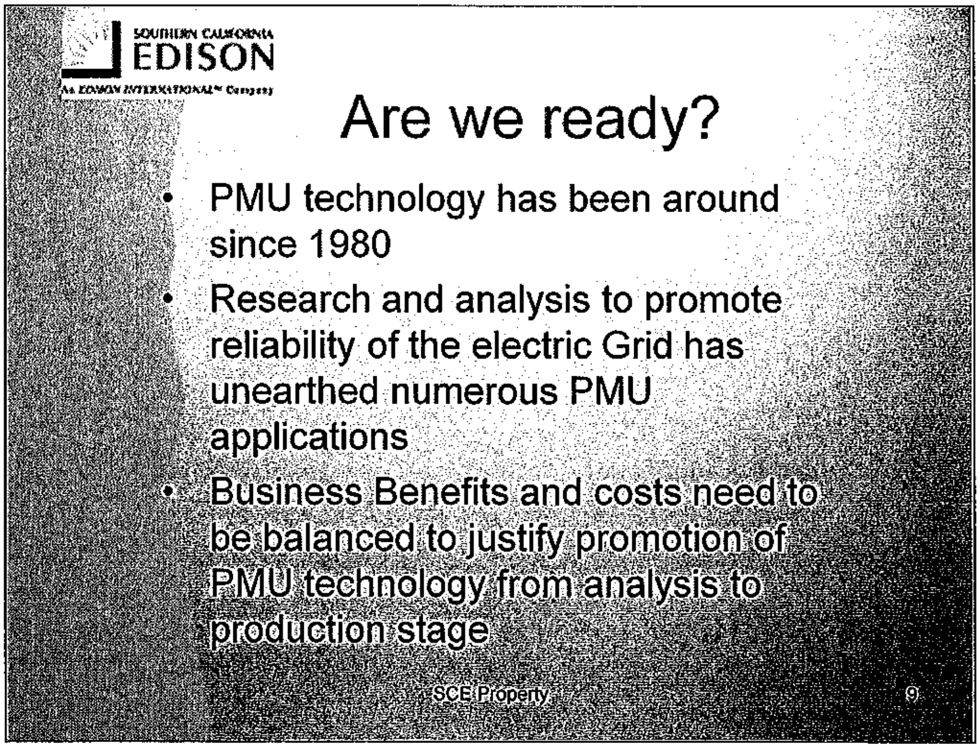
9. Large Load Centers Load serving lines of one or more substations that have a combined of greater than 750 MW

> 200 kV - 3-phase bus voltage, - 3-phase currents in served load load transformers

10. RAS control elements (new) A substation where either measurements are taken to initiate a response-based RAS action or a

RAS action is applied (including > 200 kV - 3-phase bus voltage - 3-phase current in transmission elements are a

14 power plants armed for RAS that are part of a RAS scheme



Synchrophasor technology is changing rapidly, sparked in large part to major investments in phasor system deployment by the electric industry with matching funds from the U.S. Department of Energy's Smart Grid Investment and Demonstration Grants. Eleven grants for synchrophasor technology, following seven years of DOE R&D investments in phasor technology devices and applications, will add almost 1,000 new PMUs onto the grid in every U.S. interconnection, expansive new phasor data communications networks, and implementation of many real-time and planning applications to use these data. The SGIG awardees are working with the North American SynchroPhasor Initiative, a voluntary collaboration between industry, vendors, academics, NERC and DOE, to facilitate coordination, shared learning, problemsolving and accelerated standards development to enhance project success. By the time these

projects conclude in 2014, several of these applications should have become production-grade

and fully accepted in control rooms across the nation.

==

Bulk power system operations (those occurring within 24 hours of real-time) use synchrophasor

systems in several different ways that have differing levels of reliability and readiness

requirements. These are:

- Automated control of system equipment or operations
- Decision support, as to provide intelligent, analytically-based diagnoses, analyses and options that help operators respond to grid events
- Situational awareness tools, to help operators understand what is happening across a region (or at specific grid assets) in real-time
- Tools or information that are incorporated into operational standards and requirements
- Pilot or research-grade tools
- Planning and off-line tools, such as those used for system and power plant modeling.

A tool that will be used for decision support or automated control must meet much higher

standards than one that is informational and considered to be research-grade rather than

production-grade. But a number of factors affect whether a hardware or software system is

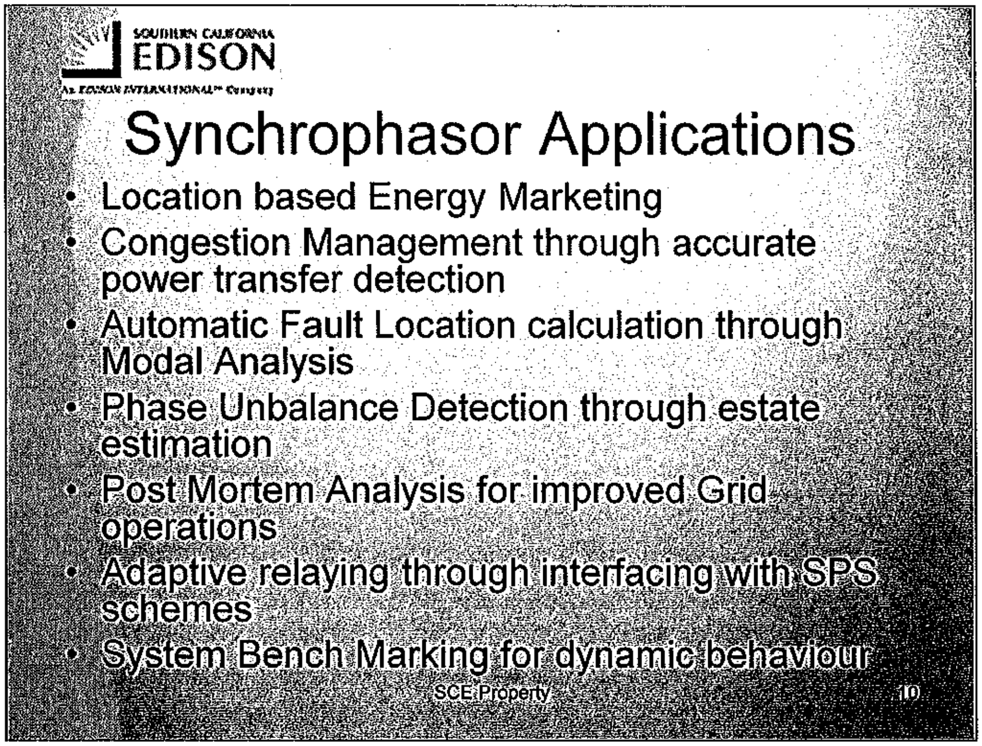
technologically ready, reliable and trusted for operational use. These are:

- Operational availability and reliability
- Data quality
- Relevance and value for its targeted use
- Alarming for availability (failure)
- Physical and/or cyber-security
- Testing

□ Training for operators and support staff

□ Technical support (internal and vendor).

These factors can be expressed as metrics and used to express goals or targets for the quality and reliability of a synchrophasor system or other operating reliability tool. In the case of synchrophasor technology, the different system elements — hardware, software applications, communications and business support — are each at very different levels of readiness relative to these metrics. For instance, PMUs are a long-established and well-supported technology (that is now being stretched to meet new performance requirements), but most phasor data applications are relatively young and are still research-grade with a need for more experience, testing and availability.



Synchrophasor data can be used to enhance grid reliability for both real-time operations and offline planning applications, as listed below; this report explains the purpose and benefits of each application, assesses its readiness for use, and offers references for further information:

Real-time operations applications

□ Wide-area situational awareness

□ Frequency stability monitoring and trending

□ Power oscillation monitoring

□ Voltage monitoring and trending

□ Alarming and setting system operating limits, event detection and avoidance

□ Resource integration

□ State estimation

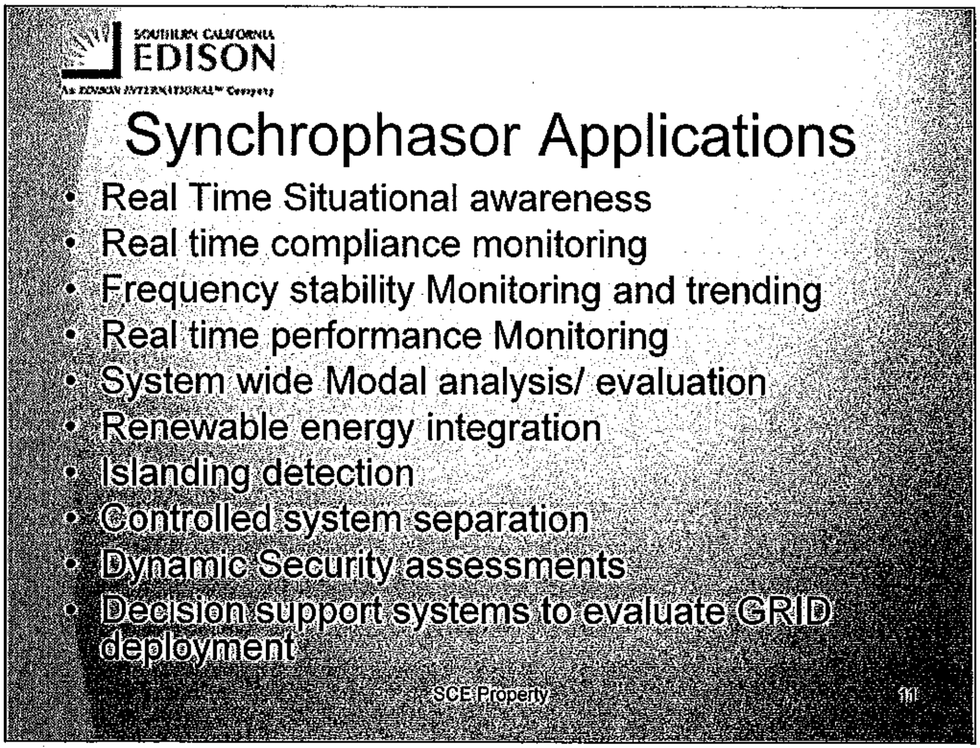
□ Dynamic line ratings and congestion management

□ Outage restoration

□ Operations planning

Planning and off-line applications

- Baselining power system performance
- Event analysis
- Static system model calibration and validation
- Dynamic system model calibration and validation
- Power plant model validation
- Load characterization
- Special protection schemes and islanding
- Primary frequency (governing) response



The applications of WAMS data can be categorized as:

- Real time monitoring
- Control
- Model validation

The suggested and running WECC applications for WAMS data2 include:

- Real time observation of system performance
- Early detection of system problems
- Real time determination of transmission capacities
- Analysis of system behavior, especially major disturbances
- Special tests and measurements, for purposes such as

special investigations of system dynamic performance

validation and refinement of planning models

commissioning or re-certification of major control systems

calibration and refinement of measurement facilitiesRefinement of planning, operation, and control processes essential to best use of

transmission assets

The suggested and running real time applications for phase angle measurements2 includes:

Basis for high quality bus frequency signals

Validation of system dynamic performance

Angle-assisted state estimation

System restoration

Operator alerts for high-stress operating conditions

Arming of special stability controls

Supervision of fast stability controls

Real time power flow control (e.g., phase shifters, slow thyristor controlled series capacitor (TCSC))

Modulation inputs for "bang-bang" stability controls (e.g., phase-plane controllers)

Modulation inputs to other controller types.

Wide area stability control system (WACS)

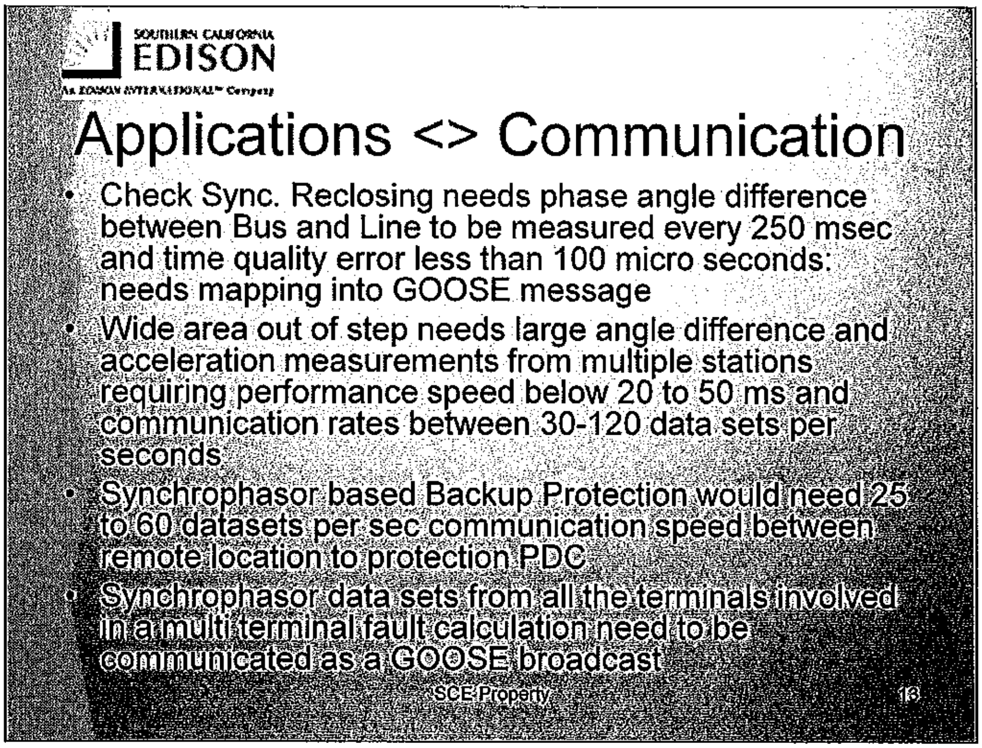
SOUTHERN CALIFORNIA EDISON

An EDISON INTERNATIONAL Company

Applications <> Placement

- 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 Marketting need wide dispersal covering Generation Sites, Power transfer corridors, Interconnection tie lines

SCE Property 12



Ref:

Control application resolution requirement - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.1663&rep=rep1&type=pdf

Smart Grid Functional Specification on communication:

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:

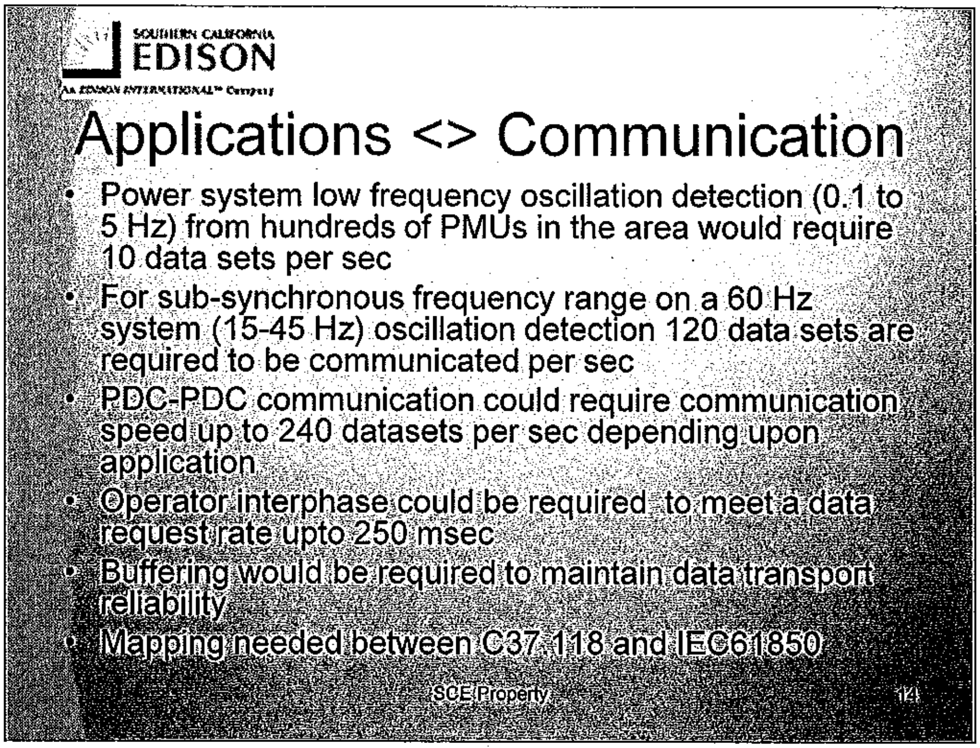
4.1 Wide Area Out of Step

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 this 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.

4.2 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.



SGIP – Synchrophasor communication functional specification

4.3 Black Start

Black Start is the situation where the power system has collapsed and must be restarted from reliable sources such as gas turbines, battery storage, and hydro generation. When bringing these generation sources on-line and creating a synchronized system, synchronization must often occur between different islands of power. By measuring the absolute voltage angles, a Wide Area Check Sync function can be performed. The functionality of the reclose operation is the same as that described for intra-substation Check Sync with a similar synchrophasor reporting rate of 4 datasets/sec.

4.4 Double Ended Fault Location

For a fault on a line, datasets of synchronized voltages and currents at the time of the fault can be captured from all line terminals (typically 2 or 3) and used in multi-terminal fault location calculations. Synchronized measurements used in this manner enable greater accuracy in the fault calculation as measurement errors due to fault impedance and terminal voltage angle differences can be compensated. The captured datasets are to be communicated either among the involved relays or between the involved relays and a central repository (e.g. – a Phasor Data Concentrator). A calculation is made and the results shared – either as a client-server message or broadcast via GOOSE to any involved subscribers. There is no streaming required in this application, only the sharing of the fault dataset after the event. Note that there should be multiple storage buffers in order to accommodate fault-reclose-fault-reclose-fault-lockout scenarios.

Cross cutting Requirements:

7.1 User-configurable datasets shall be available

7.2 Data in a dataset must be "coherent", that is, all data is synchronized to the same point in time

7.3 The PMU and PDC shall have support for multiple clients

7.4 The Time Stamp shall be based on the Second of Century – starting Jan 1, 1970 and shall provide support for a modulo-based fraction of second, support for Time Quality as defined in IEEE C37.118, and shall be able to identify and account for leap seconds

7.5 A mechanism shall be provided to map the Status word from C37.118 into IEC 61850 semantics

7.6 A mechanism for detecting/reporting missing data shall be provided

7.7 The implementation shall be capable of providing a high degree of data integrity

7.8 An option for tamper detection and data confidentiality shall be provided

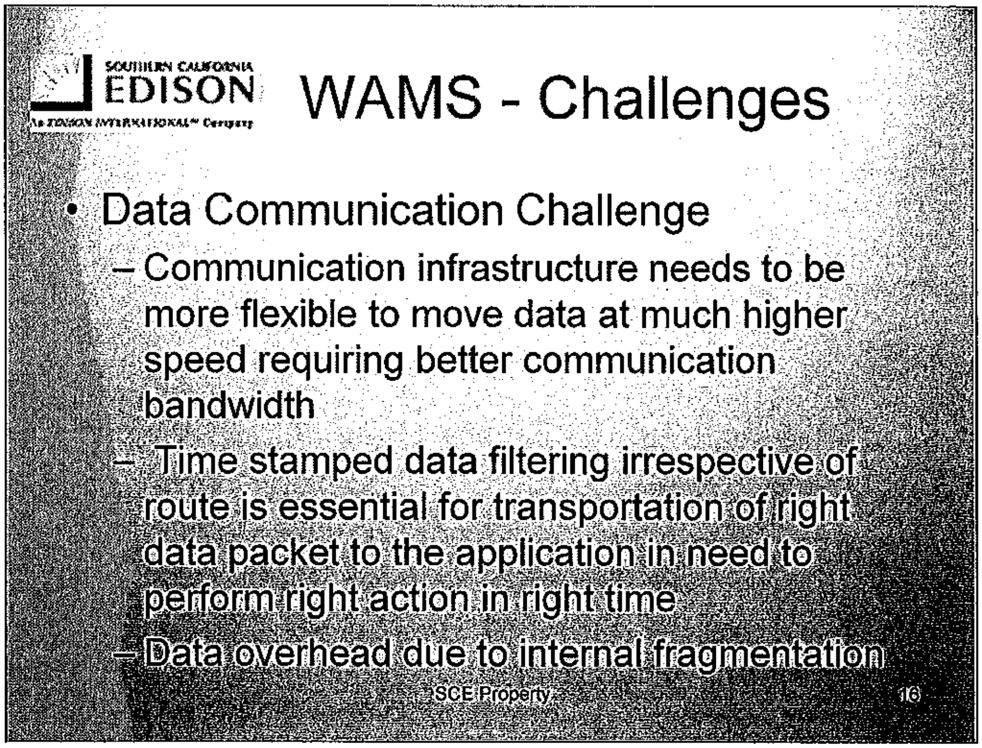
7.9 Control capability from the PDC to the PMU shall be provided

7.10 Synchrophasor files shall be named per the IEEE C37.232 File Naming Convention

7.11Synchrophasor file output shall be formatted per the recommendation in the appendix of COMTRADE

WAMS - Challenges

- 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



1. The present communication architecture supporting control of the electric power grid makes it difficult to use the wealth of data collected at high rates in substations, retarding their use in new applications for controlling the grid. A flexible, real-time data network would make it possible to use these data for many more control and protection applications, having the potential to increase the reliability of the grid and increase its operating efficiency. Example applications that could use these data include: decentralized load frequency control; closedloop voltage control; transient and small-signal stabilization; and special protection schemes taking advantage of data gathered over a wide area. Such applications and the flexibility of the underlying communication network imply greater sharing of data between the utilities making up the grid as well as performance, availability and reliability

requirements.

Mechanisms for managing security, trust, timeliness and path redundancy are thus important

components of communication networks to support these control applications.

2. Devices in substations periodically publish status and analog measurements, called

status variables in the architecture; control centers and devices in other substations subscribe

to a selected set of status variables. A publisher may produce data at a higher rate than a

subscriber cares to receive them in which case the network will filter the data stream down to

the required rate, reducing demands placed on network and subscriber resources. The network

supports multiple subscribers to each status variable's stream of data using multicast

techniques.

Conventional communication systems based on SCADA and point-to-point communication

are already known to have security vulnerabilities, [8]. A pub-sub architecture for power grid

communication potentially poses quite different QoS and security requirements than those

that arise in conventional power grid communication: the new architecture will support a

vastly richer set of interactions between power grid entities than is typical with today's

architectures.

4. We set out to show empirically that GridStat can fulfill

the data communication needs of a PDC. We used the

recommendations of the EIPP real time task team, [14], as

a basis for our evaluation of GridStat. Those requirements

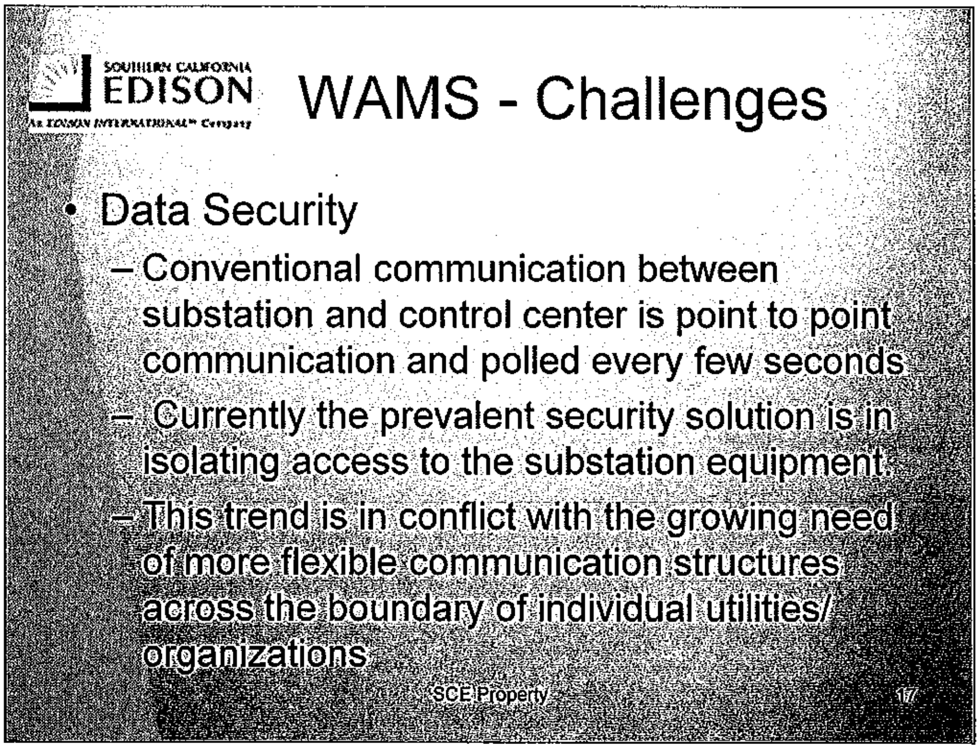
specify that a PDC should be able to receive each PMU's data 30 times a second. Further, to be useful for real-time monitoring, data must be collected from at least twelve different sources. For real time adaptive control applications the communications infrastructure is expected to add approximately 10ms to the overall time delay of PMU data delivery. To meet short-term needs, therefore, GridStat should be able to provide a PDC data from at least 12 PMU publishers at a rate of 30 per second while contributing less than 10ms of delay. In the longer term there will be many more PMUs on the grid so tests were done with 100 PMU data streams.

The Wide-Area stability and voltage Control System (WACS) project of the Bonneville Power Administration, Ciber, Inc. and Washington State University uses PMUs as sensors in a real-time system for stability and voltage control, [19]. Calculations from that project provide a time budget for creation, delivery and processing of PMU measurements in the Western Interconnection. The budget is based on the need to respond to a disturbance within 750-1500ms. Of this time budget approximately 67 ms is attributed to communication latency and jitter using the project's current point-to-point communication infrastructure. WACS uses a dedicated communication network to collect input from its sensors. Other projects using networked PMUs for control include [18] and [10].

To date none of the power systems projects using PMUs has adopted a middleware framework for its communication infrastructure. For example, the Data Distribution Service (DDS) for Real-time Systems Specification by the Object Management Group addresses communication of signals, streams and states, [16]. Existing implementations of the specification are targeted to the LAN environment and do not address QoS management issues associated with the wide area, [17, 21]. The PASS system was designed for monitoring the status of a communication network, [22]. It does address QoS in the wide area but does not provide independent QoS specification for each subscription.

Table 1. Delays over 10ms

Experiment	End-to-end over 10ms	Percentage
30/s Single Path	173	0.034%
30/s Redundant Paths	2527	0.505%
60/s Single Path	108	0.022%
60/s Redundant Paths	3808	0.762%



Communication between substations and control centers.

Communication between substations and control centers today is the domain of SCADA

systems. Equipment at substations, including so-called Intelligent Electronic Devices (IEDs),

reports status and measurements, such as voltage, current and power transfer, to a SCADA

Remote Terminal Unit (RTU) in the substation. A SCADA master at the control center polls

the RTU every few seconds to retrieve the measurements. An Energy Management System

(EMS) at the control center displays the measurements and status to operators. The operators,

in turn, issue commands to the substation equipment (e.g., to open or close a breaker, or

change transformer tap).

Even this very simplified description reveals fundamental requirements for the performance

of the control center.

1. Control center displays for operators must accurately reflect the system state so that
control decisions are appropriate.

2. Substation equipment carries out legitimate commands, and only legitimate commands, within specified time delays.

3. Certain control decisions and state information are commercially or otherwise sensitive and are not to be revealed to unauthorized parties.

On the other hand, the two-second (or even four-second) SCADA polling cycle and the
almost entirely manual control system suggest that sub-second latency is *not* a requirement
for these communications in today's systems.

Historically, the obstacles that the power industry has addressed in meeting the first two
requirements have been primarily ones associated with the reliability of substation equipment
and communication systems. Problems include sensor failures, communication link failures,
misconfiguration of substation equipment and databases that describe it, etc. Solutions include
redundancy of communication links and use of software technology called *state estimators* to
form an accurate picture of the system state based on partially incorrect information.

These solutions primarily address threats to the requirements posed by unreliability of
equipment and errors by human beings. In recent years, malicious interference is increasingly
recognized as a threat to achieving the requirements. To date, the security approaches taken to
preventing malicious interference are based on attempting to guarantee that the SCADA
system is a closed, isolated system and on that basis making assumptions such as:

1. Physical access to substation equipment is limited to authorized parties.

2. Physical access to the communication hardware and links is limited to

authorized

parties.

3. Authorized parties are always trustworthy.

4. SCADA networks are not interconnected with networks to which unauthorized parties

have access.

5. Because links are used exclusively for SCADA communication there are no issues

associated with allocation of bandwidth for different purposes.

There is considerable accumulated evidence that existing SCADA systems do not satisfy

these assumptions [8], leading to the conclusion that the electric power infrastructure is

threatened by malicious attack delivered through its control system. In the last decade the

extent to which the closed system assumptions were not being met has been recognized and

considerable effort by utilities has gone into remedying the situation. New operational and

auditing practices have improved the situation. More recently, products providing "bump-inthe-

wire" encryption have become economically feasible and have seen increasing

deployment.

The trend toward operating transmission systems closer to the their limits, toward outsourcing

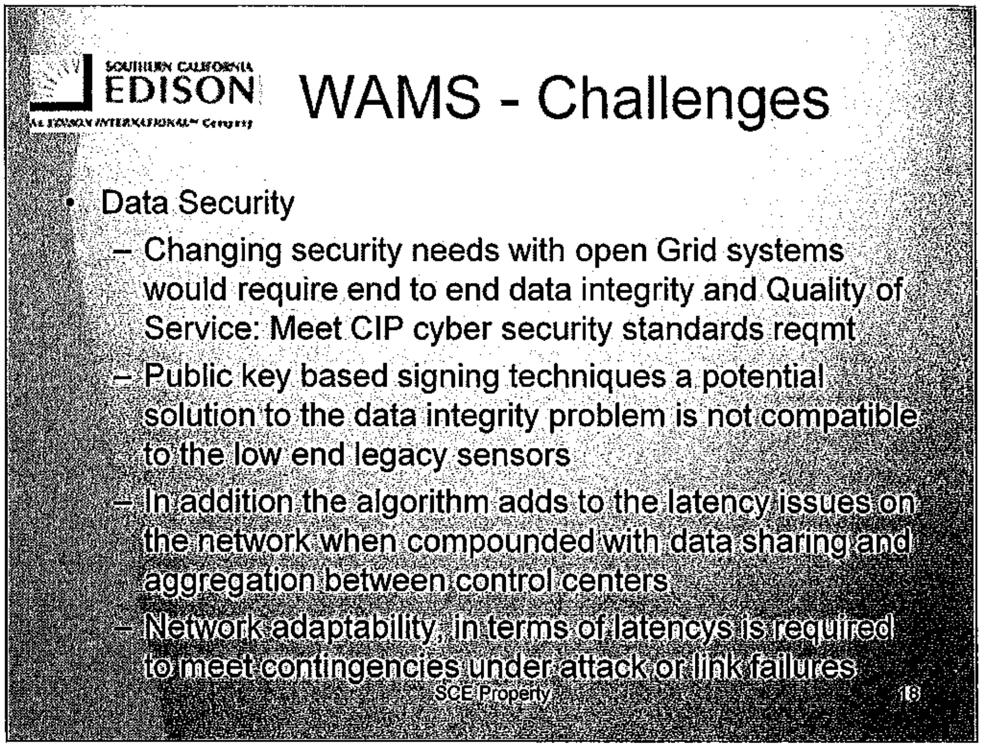
of key maintenance and configuration operations, and toward separation of the businesses of

generation and transmission would be better served by the more flexible communication

infrastructure discussed here. However, the security assumptions of existing SCADA systems

are in conflict with the evolving need for communication that crosses organizational and

geographic boundaries. For the new communication architecture it is appropriate, therefore,



The long-term challenge for synchrophasor technology is to prove its value for operations and

planning, to justify continued industry investment and ownership in production-grade, fully

utilized systems. The RAPIR team offers several recommendations for near-term industry

priorities and actions to advance this goal:

□ The NERC Operating Committee and Planning Committee should receive regular

briefings on successful applications of synchrophasor technology.

□ Establish a library of grid disturbances and events, characterized in phasor data, to be

used for analysis and training resources for operators and planners.

□ Develop ten operator training models built around these system events.

□ Understand and improve phasor data availability and quality and develop data validation

methods and tools.

□ Undertake and complete baselining analysis, using actual synchrophasor data, for every interconnection, to serve as the foundation for event detection, alarm-setting, and most

other key real-time operations applications.

□ Continue and complete interoperability standards development and adoption.

□ Develop consensus functional specifications and testing protocols for Phasor

Measurement Units and Phasor Data Concentrators.

□ Develop and use naming and data format conventions for phasor data and devices.

□ Expand the use of phasor data to validate and calibrate system and asset models.

□ Develop goals, guidelines and tests for interoperability of inter-area, inter-party phasor

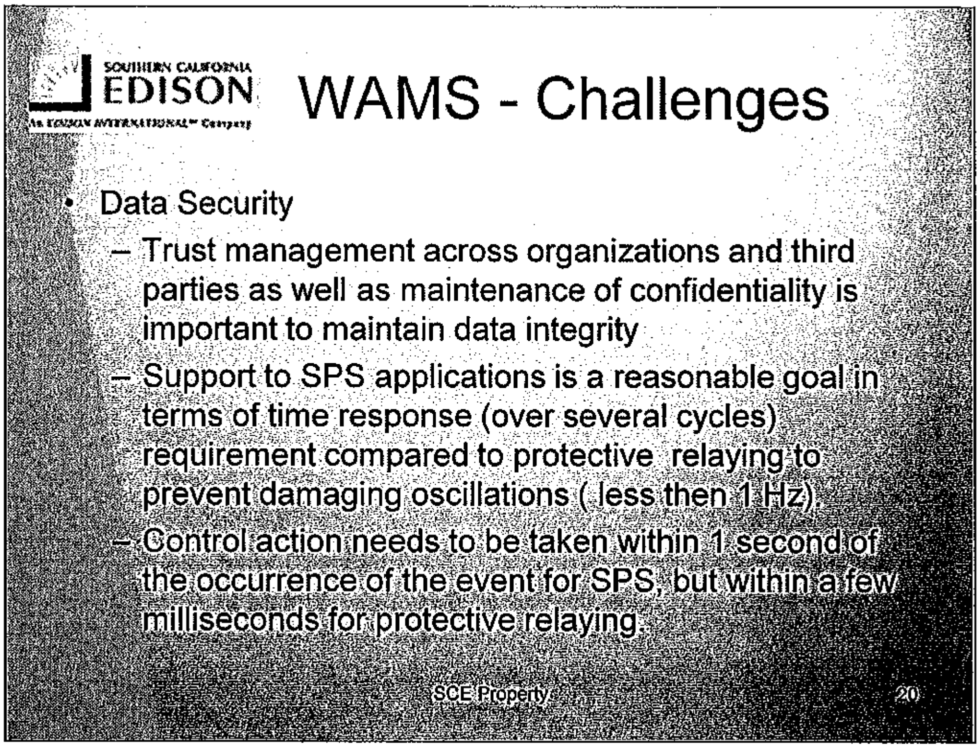
system communications and data, and use them to support communications system

implementation.

□ Adopt methods for phasor data-sharing and protection.

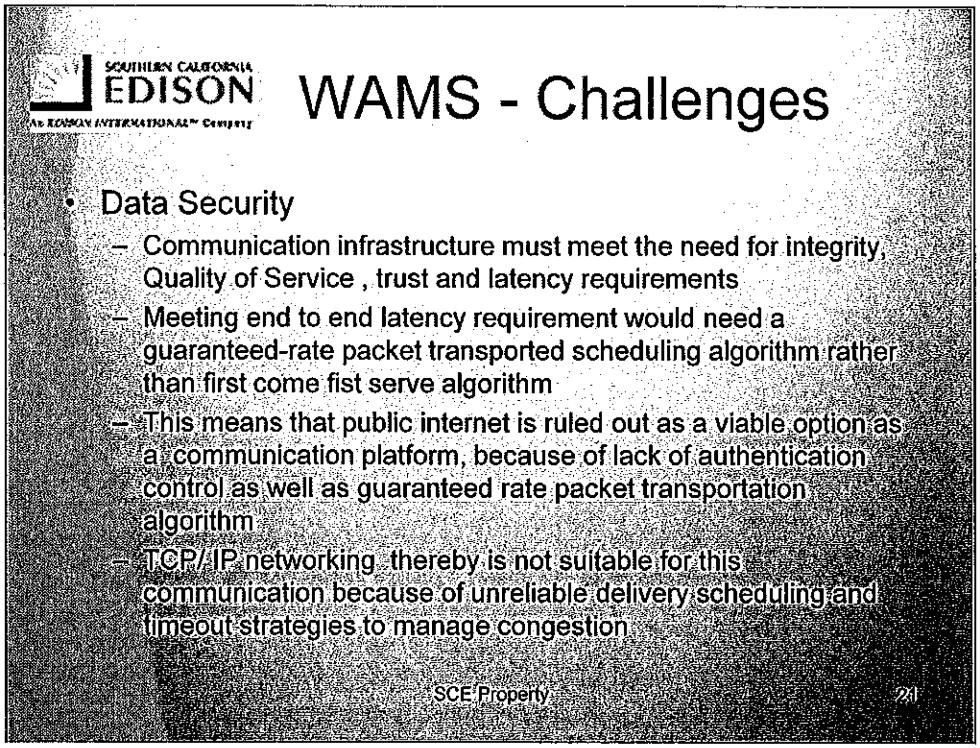
WAMS - Challenges

- 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



To prevent outages due to this phenomenon, power system engineers have created special protection schemes (SPS) that attempt to prevent the oscillations from growing, instead of waiting for the oscillations to force critical equipment to trip offline. A special protection scheme involves taking a specific action, such as tripping a generator, soon after a specific triggering event that may occur hundreds of kilometers away. Because the damaging oscillations have low frequency (often substantially below 1Hz) and the concern is preventing the buildup in amplitude of oscillations over several cycles, the communication timing requirements for special protection schemes are less stringent than those for local protective relaying. Support for SPS is a reasonable goal for a wide-area power grid communication architecture.

Because a SPS provides protection against only a predefined event at high cost and complexity, recent research has been investigating approaches that allow reaction based on sensing the response of the power grid to arbitrary disturbances, followed by corrective action such as capacitor bank switching, generator tripping, or load shedding, [13]. Related ideas include detection and mitigation of small-signal instability, [14], and fault location by detecting and triangulating based on frequency disturbances, [15]. These schemes detect anomalous behavior of the grid by monitoring the outputs of several PMUs (or frequency measurement devices in the case of [15]) and deriving indications of problems such as low voltage, incorrect frequency, or oscillations. Based on location of the problem, specific discontinuous or continuous control actions can be taken. In the Western US power grid it is estimated that control action needs to be taken within about 1 second of the occurrence of the disturbance to suppress transient instability.



The requirements identified above have several implications for QoS, security and trust and their interactions which we now elaborate.

The communication infrastructure should support CIA properties for all messages as needed by the applications. The major challenges to doing this are 1) providing these properties using computationally underpowered devices; 2) establishing an authentication infrastructure that efficiently supports the operational needs of the utility industry while providing authentication for people working in many different businesses and organizations in many different roles *and* for thousands of different devices; 3) establishing and maintaining policies that allow appropriate monitoring and control to occur.

While we do not propose that power grid communication be implemented using the *public* Internet, the cost of *internet technology* makes its use in *private* networks very attractive. We assume, for the time being, a private cyber infrastructure for the power grid based on internet technology and we look specifically at the security implications of the power grid control requirements for such a network.

The hard real-time latency requirements imply that network resources must be actively managed: best effort service is not good enough. Meeting end-to-end latency requirements for existing subscriptions means that first-come first-serve is not adequate as a scheduling discipline in nodes of the forwarding network: a guaranteed-rate packet scheduling discipline is required, [16,17]. A corollary of these observations is that the public Internet, lacking both admission control and guaranteed-rate forwarding, is not viable as part of the power grid's control communication infrastructure. Policy mechanisms will be needed as part of the communication infrastructure to ensure that subscriptions needed for safe operation of the power grid are always admitted. Also, determining which subscriptions are most needed and which are merely nice to have will be a part of the engineering process in designing control systems in the future. The question of which subscriptions are most needed is compounded when one considers that the answer may change as power flows change.

Even on a private IP network the standard TCP byte-stream protocol is inappropriate for most of the applications described here. Although TCP provides reliable delivery its delivery model (do not deliver byte *n* to the application until byte *n-1* has been delivered), its retransmission, window management, and timeout strategies geared to congestion control, render it unsuitable for real-time control.

The design of the communication infrastructure must also consider malicious threats to

meeting QoS requirements. Denial of service through consumption of network resources is a

threat that must be countered. Even though use of the public Internet has already been shown

to be inappropriate, the control network design should suppose that at least from time to time,

if not permanently, the two networks become connected. It must be assumed therefore that

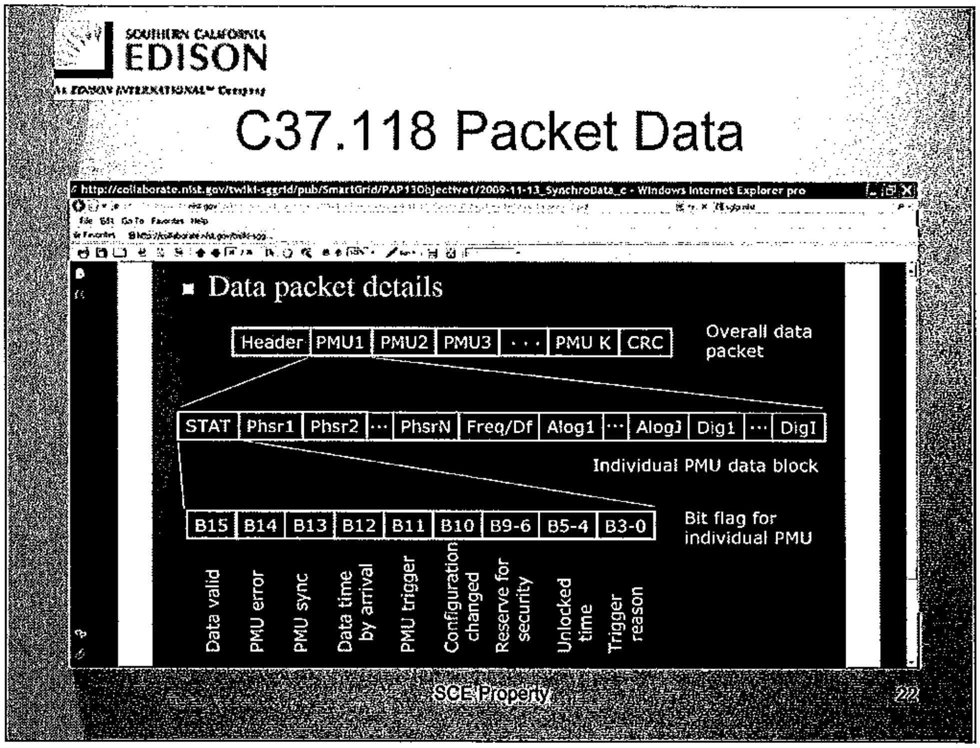
packet injections are possible so denial of service attacks cannot be prevented, but must be

thwarted. Security mechanisms will have to be leveraged to prevent unwanted traffic from

consuming network resources.

TCP/IP – TCP/IP is a low-level protocol for use mainly on Ethernet or related networks. Most of the higher-level protocols use TCP/IP to transport the data. TCP/IP provides a highly reliable connection over unreliable networks, using checksums, congestion control, and automatic resending of bad or missing data. TCP/IP requires time to handshake new connections and will block if missing data is being resent.

UDP/IP – UDP/IP is a low-level IP protocol that provides low-latency communication across Ethernet or related networks. UDP/IP does not provide any error-control or resending of missing or bad data. The Application will need to check data for correctness. UDP/IP however, does not require time for handshaking and will not block, making it ideal for real-time data communications.



C37.118 Message Details:

==========================

Command frame

• Sttartt//sttop datta,, send otther iinformattiion

Datta frame

• Phasor measurementts

• Frequency measurementt

• Anallog datta (user speciifiied datta ttype)

• Diigiittall iindiicattiions (Boollean,, 1-biitt vallues)

Confiigurattiion frame

• Descriibes datta frame,, wiitth scalliing & namiing

Header frame

• Textt descriipttiions,, user formatt

=======================

4 datta ttypes defiined iin C37..118:

. Phasor measurementts

• Pollar or recttangullar componentts

Frequency

• Absollutte (F) & ratte of change (dF//dtt)

Anallog

• Variious – defiined by user

• Siinglle vallue conttiinuous - conttroll vallue,, MW,, ettc..

16-biitt iintteger or 32-biitt IEEE flloattiing poiintt

• Phasor & frequency uniitts defiined iin sttandard

Diigiittall

• Boollean sttattus representted iin 16-biitt word

==

Limitations:

Securiitty iis nott addressed

Confiigurattiion of PMU deviices iis nott iinclluded

iin tthe prottocoll

Prottocoll wiillll nott scalle tto very llarge systtems

Communiicattiion metthods are desiignatted

outtsiide of tthe sttandard

=====================================

61850-C37.118 mapping need:

61850 needs tto

• Proviide mappiing & metthods for phasor datta

• Proviide suffiiciientt iinformattiion for phasor use

C37..118 needs tto

• Adaptt tto compllimentt 61850 metthods

We need tto

• Proviide recommendattiions for operattiions outtsiide

of 61850

• Have a game pllan for iimpllementtattiion

================================

Communication Mode --------

Commanded – datta sentt on command

• Datta,, confiigurattiion,, and header on command

• Requiires ttwo way connecttiion
• TCP,, UDP,, seriiall
Sponttaneous – datta sentt conttiinuouslly wiitthoutt sttop
• Datta outtputt pre-enablled,, sentt tto pre-sett desttiinattiion
• Requiires onlly one-way communiicattiion
• Confiigurattiion mustt be separattelly supplliied
• UDP,, seriial

==

Network Communication Mode:
TCP
• Clliientt connectts,, receiives confiig,, header,, & datta on requestt
• Allll communiicattiion tthrough one TCP sessiion
TCP-UDP
• Same as TCP butt datta sentt separattelly on UDP
UDP-UDP
• No connecttiion,, clliientt sends commands tto server portt
• Server sends confiig,, header,, & datta tto requesttiing hostt
Sponttaneous
• UDP onlly,, broadcastt,, uniicastt,, mullttiicastt

================================

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 congested

(so sender won't overwhelm network)

SOUTHERN CALIFORNIA
EDISON
An EDISON INTERNATIONAL Company

Services: TCP<>UDP

Service	TCP	UDP
Connection setup	Takes time, but TCP does this to ensure reliability.	No connection required.
Guaranteed message delivery	Returns ACKs (acknowledgments).	Since UDP does not return ACKs, the receiver cannot signal that packets have been successfully delivered. Lost packets are not retransmitted.
Packet sequencing (provide information about the correct order of packets)	Sequentially numbers packets.	UDP does not insert sequence numbers. The packets are expected to arrive as a continuous stream or they are dropped.
Flow controls	The receiver can signal the sender to slow down.	ACKs, which are used in TCP to control packet flow, are not returned.
Congestion controls	Network devices can take advantage of TCP ACKs to control the behavior of senders.	Without ACKs, the network cannot signal congestion to the sender

Applications using UDP must provide some form of flow control on their own. For example, if a videoconferencing application notices that packets are being dropped, it may dynamically increase the compression ratio (and thus reduce quality) or drop packets on its own in a controlled way to match available bandwidth on the network, while still providing quality that it considers reasonable. It does not rely on UDP for this, and using TCP for flow and congestion control would be inefficient.

In fact, most real-time applications have their own special flow-control requirements that the generic control provided by TCP cannot provide. Basically, UDP-based real-time applications must be "self-regulating." RTP can rely on RTCP (Real-time Control Protocol) to control transmission rates when packets are dropped. RTCP is a feedback mechanism that helps real-time applications work within the available bandwidth of the network.

SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company

Required Data rate: TCP<>UDP

Service	TCP	UDP
C37.118 Data format	30 frames per second	30 frames per second.
10 phasor/ 2 Analog/ 1 digital/ Integer data format	2040 bytes/ seconds	23,040 BPS with 54 bytes per packet overhead
10 phasor/ 2 Analog/ 1 digital/ floating point data format	3480 bytes/ seconds	41120 BPS

24

Asynchronous serial requires 10 bits/byte, so required BPS rates are 10X the above figures.

- UDP/IP over Ethernet has a fixed size overhead of 54 bytes per packet, so actual required rate is higher than the requirement above. It ranges from 23,040 BPS for phasor/integer to 41,120 BPS for the 10 phasor-2 analog-1 digital/floating point shown above.

- Since data is sent continuously at the rates shown in the table, the communication channel must have a capacity at least that large and should be at least 10% higher than the required data rate to accommodate error correction and short dropouts. The PMU port speed will likewise have to be equal or higher than the actual data rate. In many cases this requires high serial data rates, such as 38.4 or 57.6 KBPS.

- ==================================

PMU Output Data Rates

ASSUMPTIONS: All data will be in integer format

10 phasors and two digital words will be transmitted

Data transmission rate is 30/sec

Asynchronous serial data protocol (RS 232)

10 bit/character format (1 start, 1 stop, 8 data, no parity)

Note: Serial communications send each byte as one character framed by start and stop bits. When using network communications, there is overhead with each packet but each character is transmitted as one 8-bit byte.

Data rate for Macrodyne format

40 bytes phasors

4 bytes Digital

6 bytes sample, Freq, Df/dt

10 bytes All other

60 bytes Message total

60 bytes/msg X 30 msg/sec = 1800 bytes/sec

1800 bytes/sec X 10 bits/byte = 18,000 bits/sec (BPS) actual data rate.

Data Rate for the IEEE C37.118 SYNCHROPHASOR Standard Format.

16 bytes HDR, SOC, FRACSEC, PMU_ID, CRC

2 bytes STAT

40 bytes phasors

4 bytes FREQ, DFDQ

4 bytes DIG

6 7

66 bytes Message total

66 bytes/msg X 30 msg/sec = 1980 bytes/sec

1980 bytes/sec X 10 bits/byte = 19,800 bits/sec (BPS) actual data rate.

Data rate for PDCstream (compact option)

Fixed bytes per message: 18 bytes

Bytes/PMU

Status (chan flag, PMU stat) 8 bytes

Freq, Df/dt 4 bytes

Phasors 4 bytes X #phasors

Dig status 4 bytes X dig/2 (packed in long words)

Total/PMU 12 bytes + phasors + dig

Total/message 18 + PMU X (12 + phasors + dig)

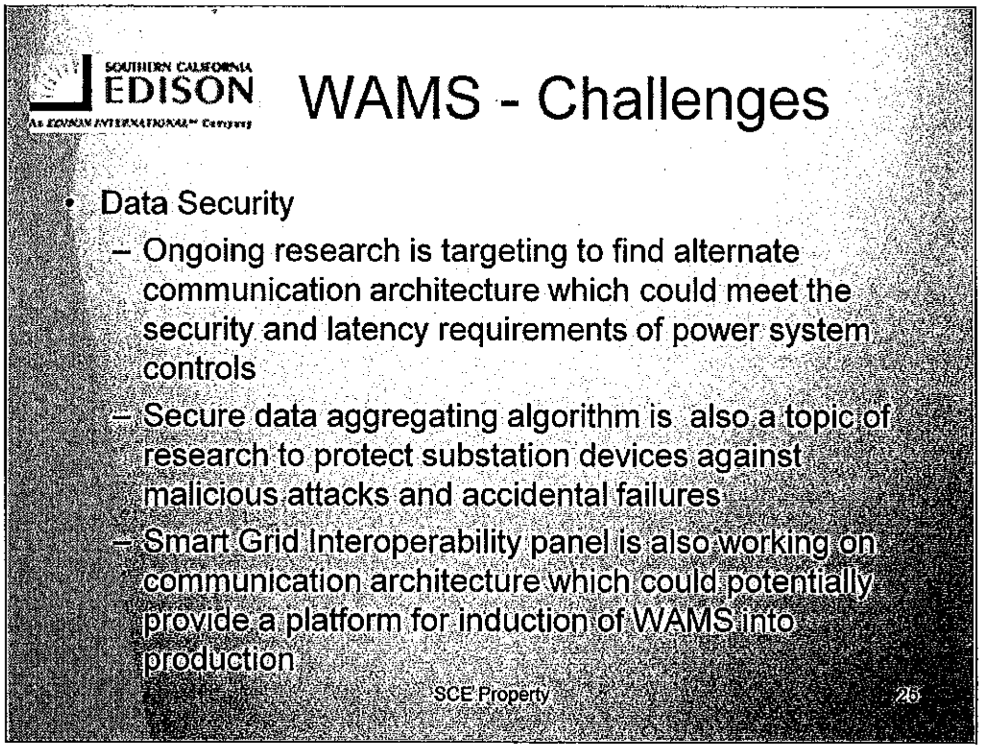
PMU with 10 phasors, 2 digitals 56 bytes + 18 = 74

74 bytes/msg X 30 msg/sec = 2220 bytes/sec

2220 bytes/sec X 10 bits/byte = 22,200 bits/sec (BPS) actual data rate.

Note: This does not include the configuration packet sent once/minute. It only adds about 1 byte/sec on average. Note also that this format is sent only on Ethernet an dis designed for multiple PMU content which makes it more efficient.

Ethernet has much more overhead per packet, but the data is packed more compactly since each byte does not require framing. The data rates will be similar with 10 byte packets as packet overhead substitutes for framing overhead. With smaller frames the packet overhead is much more significant, but the much higher wire speed makes this somewhat insignificant.



Smart grid Communication function specification:

Security in C37.118 - What is required?

a. Authentication?

b. Integrity?

c. Confidentiality?

d. Addition of hash?

Lost data recovery is not addressed by C37.118 **Proposed solution:** Recommend use of Off-the-Shelf database tools such as SQL and/or OPC-HDA/OPC-UA-HDA to retrieve missing or requested records

Initiation of TCP vs. UDP data streams not addressed **Proposed solution:** Add a bit in the PMU that, if set, streams the data via UDP, else, the data is streamed via TCP. Additionally, the address of the remote device shall be settable in the

PMU….. or use additional command frames that indicate TCP vs. UDP frame transmission

4. Support for UDP/IP Multicast

a. Configuration mechanism

b. Setting of Multicast address

c. Port /IP address recommendations

Proposed Solution: Define that the Stream command shall always be issued to a fixed address and that the Multicast IP address is to be a setting.

5. Inclusion of Latitude and Longitude data **Proposed solution:** Define new data areas in the HDR file and use the format described in the 61850 document using XML tags

6. Support for NASPI substation naming convention **Proposed solution:** Define new data areas in the HDR file

7. Transmission/Measurement of Synchrophasor Calculation and Communication Latency information **Proposed solution:** Assuming that latency doesn't change too often, make the latency measurement a data value in the CFG2 file. If changing latency is an issue, augment the synchrophasor stream to include the output time of the message. Additionally, on receipt of a

message, the time of reception is to be recorded and included in any subsequent output transmission time.

8. Need for standard Indexing of data in Historians/Databases **Observation:** This is not a C37.118 issues but it does affect interoperability. **Proposed solution:** Create an Implementation Agreement in NASPI that proposes the use the SOC and FOS (to 1usec resolution) as the record index

9. Remote PDC configuration not possible through 118 **Proposed solution:** Wait for IEC 61850

10. Identification of Bad or Missing data in a PDC stream **Proposed Solution:** The Magnitude of the Phasor is set to "-1" and the angle is set to "-360" – both invalid values

11. Mapping of Time Quality from multiple PMUs get reduced from 4 bits to 2 bits in the Status word but the mapping is different **Proposed solution:** Change the mapping of the bits as follows:

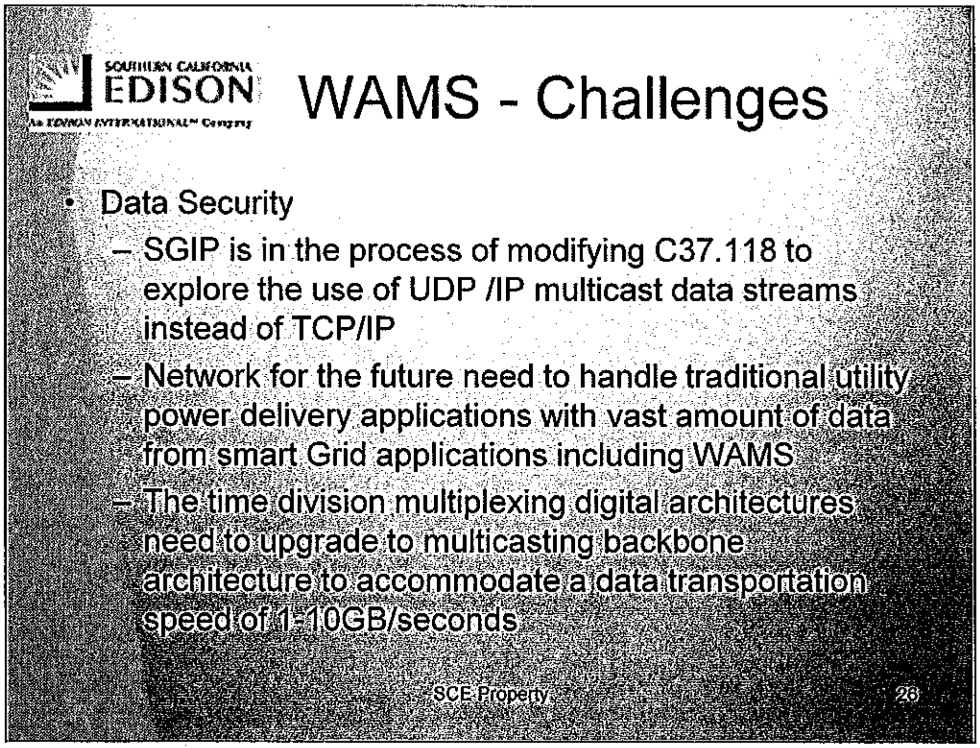
a. 00 = Synced

b. 01 = <10 usec error

c. 10 = <100 usec error

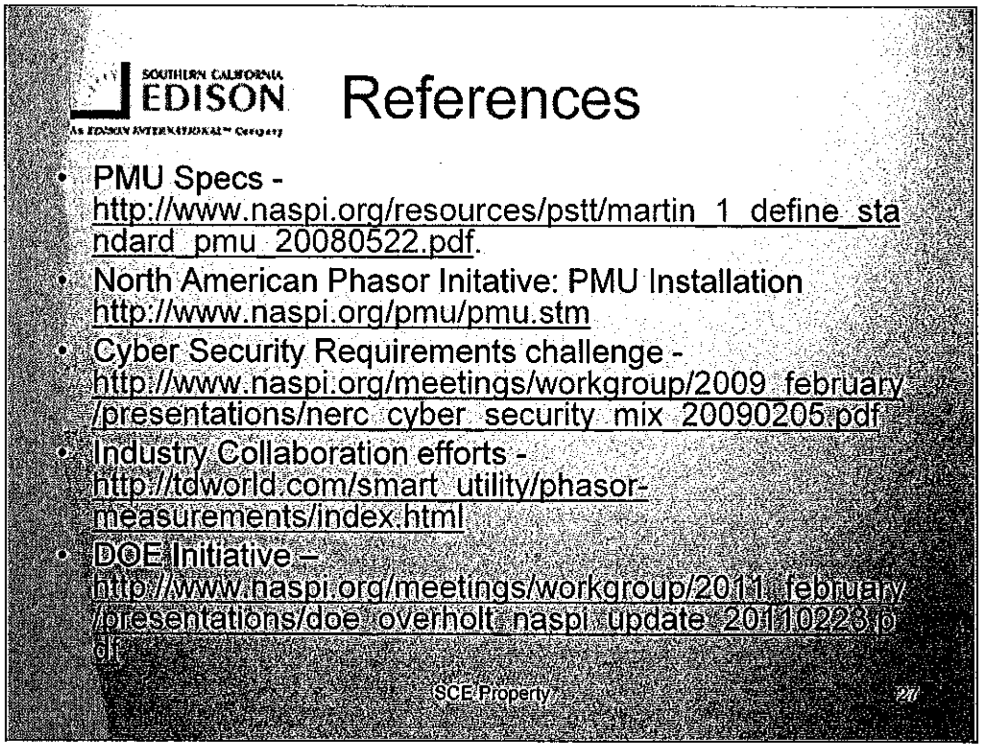
d. 11 = >1ms error

12. Data filter description should be part of the Configuration file **Proposed solution:** Add descriptive text to the HDR file that describes the latency resulting from any synchrophasor data filter. Other quantities such as the cut-off frequency, type, and attenuation may be optionally added



Today, the political and regulatory impetus for wider deployment of Smart Grid applications, especially their deployment all the way to the customer premises, has resulted in pressure on utility engineers to solve the problem of establishing robust data transport WANs to the distribution feeder and customer level. The proliferation of information technology utilizing Internet protocol (IP) transport over Ethernet has made IP the de facto standard for data transport. What is needed is a nearly ubiquitous IP transport network operating at bandwidths robust enough to handle traditional utility power delivery applications along with vast amounts of new data from the Smart Grid. These networks need to be scalable enough to handle future applications as they come.

Communications for Smart Grid data transport require that utilities address both the backbone and the spur segments. Most electric utility communications backbones today are based largely on traditional time-division multiplexing (TDM) digital architectures. TDM technology, while highly reliable, was originally developed for the transport of point-to-point constant-bit-rate voice communications and is not necessarily suited to cost-effective transport of point-to-multipoint "bursty" data traffic required in an IP environment. The Smart Grid will require that these backbones be upgraded to backhaul Ethernet/IP data traffic at speeds ranging from one to 10 gigabits per second in a highly reliable manner. Rather than replacing their legacy TDM networks, many utilities will opt initially to overlay these existing networks by overbuilding gigabit Ethernets on unused fiber, and licensed or unlicensed broadband wireless networks over existing microwave paths.



Vendor systems:

ABB : PSGUARD

http://www.epcc-workshop.net/archive/2005/paper/pdf_monday/WideAreaMeasurements/Zima_WAMS.pdfen

Macrodyne:

Installation Notes:

http://www.naspi.org/pmu/pmu_installation_bpa.pdf

SOUTHERN CALIFORNIA EDISON
An EDISON INTERNATIONAL Company

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; 33 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.