MAINTAINENCE OF WIDE AREA MONITORING SYSTEM AND PHASOR MEASUREMENT UNITS FROM CYBER ATTACKS IN POWER SYSTEM

[1]Preethi Sontakki,[2] Dr.M.S.Shashikala

[1]PG student, [2] Head of Department
Department of Electrical and Electronics Engineering,
JSS Science and Technology University, Mysuru,India.

Abstract: ***Phasor Measurement Unit (PMU) and Wide Area Monitoring system (WAMS) in Power system network play significant role in measuring, monitoring and accessing real time data and any disturbance to these components through cyber intrusion will lead to loss of valuable data and grid instability. Architecture and data frame of PMU/WAMS is implemented on IEEEC37.118 standard, the security at each level differs from hardware to software hence the categorization of layers and securing the layer from cyber intrusion is required through set of procedures and maintenance tools. The approach is to implement set of maintenance tools based on the architecture model and data frame layers of PMU/WAMS.***

Index Terms —Frame structure, Kalman Filter, Maintenance, and Network analyzer.

I. INTRODUCTION

Present Indian power system network is one of the largest power network, to monitor and control this wide power system network the physical systems like PMU's and WAMS are installed. The introduction of PMU's and WAMS to the grid which mainly rely on Information and communication system[1] which are major potential for new set of risk for cyber attacks, in this situation it is necessary to adopt set of practices for maintenance of PMU's and WAMS free from cyber intrusion. For continuous evaluation of performance of power system equipment, different maintenance are carried out which reduces the down time increases reliability of system similarly it is necessary to adopt maintenance procedure for cyber threats. Analysis of physical system PMU's and WAMS from external intruders is necessary as it might attempt to cause malfunctioning or damage to equipment [2][3]. PMU are required in Electrical Utility for dynamic and real time measuring monitoring of critical parameters for power system such as voltage, voltage angle, current, frequency and load angle.PMU provides synchronized measurement of power system parameters along with a timestamp from a global positioning system (GPS) clock. WAMS are essentially based on new data acquisition technology of phasor measurement and allow monitoring of Transmission system conditions over a large area to detect and counter act grid instabilities. This paper presents the basic architecture and communication layers of PMU's and WAMS, based on architecture and communication layers, maintenance tool are described and to be taken up to detect and prevent cyber attacks in PMU/WAMS.

II. ARCHITECTURE AND DATA FRAME STRUCTURE OF PMU

Figure shows the block diagram of a PMU. The power systems measurements, i.e. Voltage and Current phasor, are acquired through CTs/PTs located in field and are passed through an anti-aliasing filter so as to restrict the signal bandwidth according to sampling theorem. The input is then converted into digital format in accordance with IEEE C37.118 [4] standard specifications which is finally sent to the phasor estimation unit. In GPS clock, a crystal oscillator is used to supply clock pulses. The phase locked oscillator corrects for any error between pulses per second and clock frequency, finally the time stamped phasor measurement is sent to the PDC via communication interface. PMU have high sampling rate from 30 to 120 samples per second Figure 1(a) show the Block diagram of PMU and Figure 1(b) shows the IEEE C37.118 data world model.

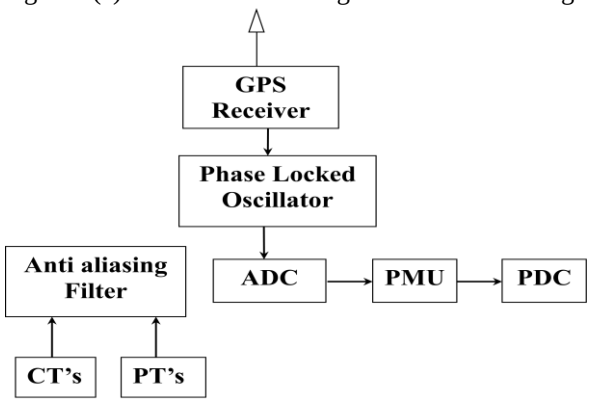


Fig.1(a). Block diagram of PMU

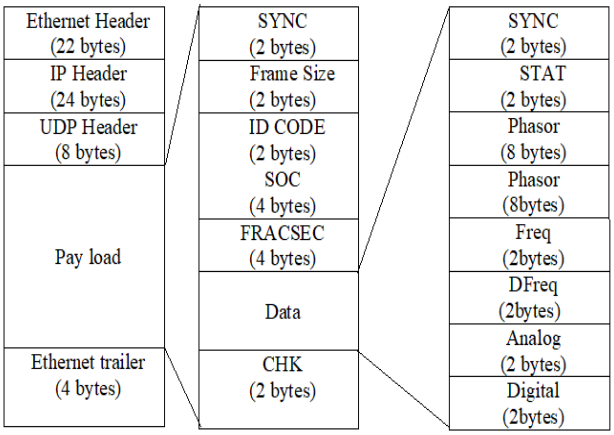


Fig.1(b). IEEEC37.118 data world model

III. WIDE AREA MONITORING SYSTEM

WAMS is the measurement technology consists of geographically dispersed phasor measurement units which collects data from PMU's and stores in PDC for data management. WAMS perform the function of obtaining data and extracting value from that data. The data Frame work shown in fig 2 show the IEEE C37.118 [4] Time-series Frame Work[4]-[5] for managing of synchronous measure data ,specifies communication requirement for real time data exchange among measurement ,concentration and application devices, It gives the detail on Protocol ,message configuration, time stamp and rate of change of frequency(ROCOF).

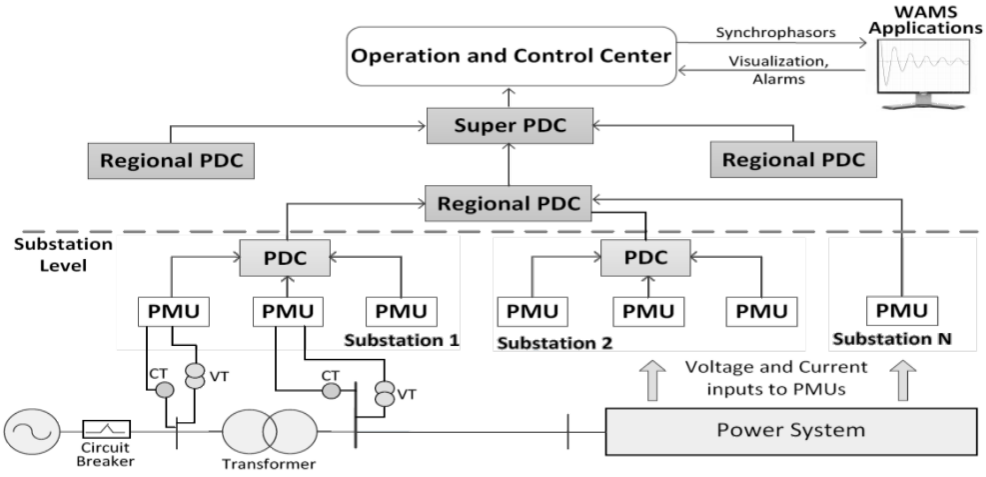


Fig.2. Layout of WAMS architecture

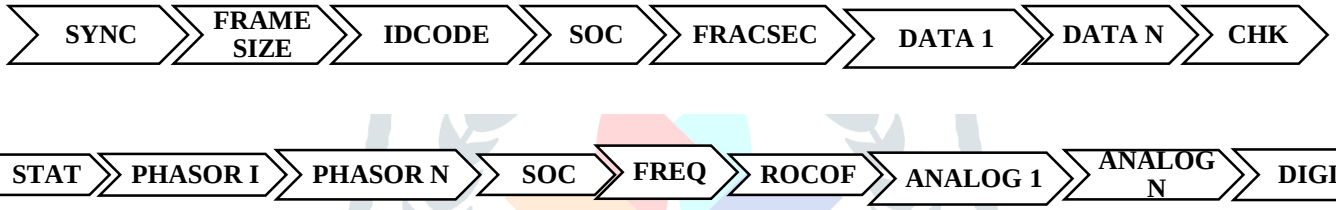


Fig. 3. Data Message Frame Structure

TABLE I - WORD DEFINITION OF FRAME TYPES

Field	Size(Bytes)	Comments
SYNC	2	Frame synchronization word. Leading byte: AA hex Second byte: Frame type and version, divided as follows: Bit 7: Reserved for future definition, must be 0 for this standard version. Bits 6–4: 000: Data Frame 001: Header Frame 010: Configuration Frame 011: Configuration Frame 2 101: Configuration Frame 3 100:Command Frame (received message)
FRAMESIZE	2	Total number of bytes in the frame. 16-bit unsigned number
IDCODE	2	Data stream ID number, 16-bit integer
SOC	2	Time stamp, 32-bit unsigned number
FRACSEC	2	Fraction of second and Time Quality
CHK	2	CRC-CCITT, 16-bit unsigned integer.

IV. AREAS VULNERABLE TO CYBER ATTACKS

Based on the above architecture level and data frame layers the areas exposed to cyber attacks are described below .Apart from this layer there are further areas such as a) Based on the risk high or low risk assessment [2]-[3] b) contingency issues.

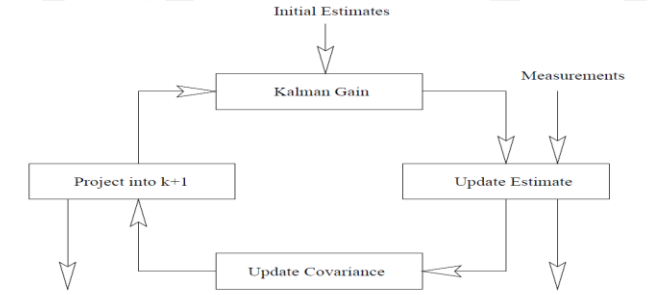
1) **Hardware layer**: includes components such as convertor, embedded system, controllers and filters for Acquisition and processing data. The PMU and WAMS as shown in Figure 1 and 2 process all these components for acquitting and processing data and then send the data to PDC centre where data analysis takes place.
2) **Firmware Layer**: This layer includes data and instruction that controls hardware.
3) **Software Layer**: It includes different software /application packages. The application software are built on different coding language this performs action of data compilation and carry out various data analytics.
4) **Network Layer:** Consist of protocols, modem, routers server, client profile application, uses WAN and LAN access point, most of the vulnerability may arise due weak communication protocols, unsecure red WLAN network ,weak TSL(Transport security Layer) and issue of certificates.

V. MAINTENANCE PROCEDURES FOR PREVENTING THE CYBER ATTACKS

In order to address the threats faced by electric grids there must be relevant information about the threats so that necessary protection measures can be implemented, this can be done by developing intelligence ,one of the such initiative by India in developing National Critical Information Infrastructure Protection centre (NCIIPC) under this act CERT(computer Emergency Response team)was framed to report the cyber threats incidents further extending to electric grid the IEGC (Indian Electricity Grid Code) clause 4.6.5 which defines to identify the cyber asset and prevent it from attacks this clause becomes one of basic tool in carrying out the maintenance, the IS standard 16335:2015 framed for power control system and security where it identifies critical assets in generation Transmission, Distribution and in Electrical trading system and critical assets and major critical assets involved in entities like Generation transmission are PMU's and WAMS.

A) **Hardware Layer:** this layer may get corrupted due to fault in the system or intrusion of external intruders, both of this can identified by statistical tool and filters, the filter such as Kalman Filter [9] as an estimator of state vector .here the difference between real output of the PMU and one estimated by Kalman filter is compared and result is residual error. The statistical processing of this error helps in detection the fault and isolation of fault attacked to the grid by intruders. The Kalman filter model algorithm and equation is shown in fig 4. The inverse of covariance matrix follows the χ^2 (chi square) distribution and using this function Kalman filter can be set as observer for detection of attacks in phasor measurements.

B) **Software Layer**: the code for analyzing the data must be carried out in a secured way. The formulation of code to be such that any external intervention of "bugs" like spoofing Man in Middle attack to be complied and debugged not allowing the harsh ware such as Stunex, Havex and recently introduced virus ransom ware to attack the application software. The OS (operating system) installed Windows/Linux needs to be original not pirated Windows/Linux



Description	Equation
Kalman Gain	$K_k = P'_k H^T \left(H P'_k H^T + R\right)^{-1}$
Update Estimate	$\hat{x}_k = \hat{x}'_k + K_k (z_k - H\hat{x}'_k)$
Update Covariance	$P_k = (I - K_k H) P'_k$
Project into $k+1$	$\hat{x}'_{k+1} = \Phi \hat{x}_k$ $P_{k+1} = \Phi P_k \Phi^T + Q$

Fig 4 Block Diagram shows basic working of Kalman filter algorithm for detecting cyber attack in PMU

C) **Network Layer:** one of the important layer and where the loss of data or data manipulation, error in communicating signals, communicating g to external intruders takes places at this layer. PMUS are installed with GPS tracking the threat may arise is the location may be diverted by external intervention to avoid all these issue it is to follow the TCP/IP(Transport control protocol/Internet protocol) is a suite of communication protocol for interconnecting devices in the context the devices interconnected are PMU's at number of substation then to PDC to WAMS and ISO/OSI(Open System Interconnection)model defines network frame work to implement protocols in seven layers from Physical-Datalink-Network-Transport-Network-Presentation-Application layer and also incorporating the IEEE standards for Ethernet communication IEEE 802.3 /WLAN IEEE 802.11.A part from this the installation of Network analyzer tools for troubleshooting ,analysis, software and communication protocol .

TABLE II. NETWORK ANALYSER TOOLS

Wireshark	Most widely used open source tools for UNIX/Windows used to analyzing TCP D ump ,monitoring local networks
Snort	Network intrusion detection and prevention and traffic analysis
Net filter	Packet filter implemented in the standard Linux Kernel

A part from the above mentioned maintenance measure the simple measures that one needs to follow as situational awareness tools to enhance the sector's ability to identify threats and coordinate the protection of critical infrastructure Cyber hygiene is a set of practices designed to maintain cyber security and keep out the "bugs" from a digital system certain set of practices need to be followed mandatory.

a) Deleting data from cloud storage when it is no longer.
b) Prohibiting the download of non-essential applications, containing viruses.
c) Procumbent of sensitive equipment from overseas as well as for the procurement of electronic products by Government or its agencies for Power sector carried out by following Guidelines mandating clearance from Security Agile.
d) Securing all information through strong password and periodically changing of password is easy maintenance tool and also easily neglected.
e) Frequently analyse the data collected at PDC, the analysis of this data will give information of the timestamp, loss of data at particular timestamp and detecting weather data lost due to external intrusion or faulty equipments.
f) Cyber intrusion Test on the PMU's need to be carried at Factory Acceptance Test. Real Time simulators are available for testing the cyber intrusion on real time and hardware in loop system based. The Central Power Research Institute (CPRI) in India provides this facility of testing phasor measurement for cyber attacks.

VI. CONCLUSION

Cyber threat to present Power system network is intangible threat; it is difficult to measure the consequences of cyber related power outages thus in this paper the maintenance tool for cyber attack is presented in view to avoid cyber attacks to PMU's and WAMS which are critical part of power system. Cyber attacks may lead to unwanted tripping causing reliability issue in power system it not only accounts for power loss but also assets damage and damage to PMU's and WAMS components will further lead to more downtime in order to reduce all these mentioned factor and for reliable secured power supply it becomes important to condition monitoring and maintaining PMU's / WAMS free from the external intruders/ hackers various type of layer level maintenance have been proposed to overcome mentioned problems .one of the biggest threats in present scenario is to implement first the service and later invest for security to overcome this solution needs to takes place at the beginning stage of implementation then carry out the basic maintenance tools to secure PMU/WAMS from cyber attacks. The future scope of this paper is to carry out analytical study on cyber attacks in Indian power system their impact and prevention.

REFERENCES

[1] Electric Grid Security and Resilience ."Establishing a Baseline for Adversarial Threats" ICF June 2016.
[2] Mission support "Cyber threat and Vulneraliblty analysis of the US Electric Sector"Idaho National Laboratory August 2016."Transforming the Nation's Electricity System", The Second Installment of the Quadrennial Energy Review, January 2017.
[3] Chih-che Sun,ChenChing Liu and Jing Xie, "Cyber-Physical system security of a Power Grid:State-of-Art" MDPI electronics 2016
[4] IEEE Standard for Synchrophasor Data Transfer for Power Systems, IEEE Std C37.118.2™-2011(Revision of IEEE Std C37.118™- 2005), IEEE Power and Energy Society.
[5] Chih-che Sun,ChenChing Liu and Jing Xie, "Cyber-Physical system security of a Power Grid:State-of-Art" MDPI electronics 2016
[6] Du, P.; Makarov, Y.V. PMU-Based Wide-Area Security Assessment: Concept, Method, and Implementation.IEEE Trans. Smart Grid 2012,3, 1325–1332
[7] Muhammad Shoaib Almas, "Synchrophasor Applications and their Vulnerability to Time Synchronization", Electric Power and energy system KTH, Royal Institute of Technology, Stockholm Sweden, 2017.
[8] Yi Lu, Qiang Yang, Wenyuan Xu, Zhiyun Lin, Weniun Yan "Cyber Security Assessment in PMU-based State Estimation of Smart Electric Transmission Networks", 2015 27th Chinese Control and Decision Conference (CCDC).
[9] Junjian Qi, Ahmad F. Taha, and Jianhui Wang, "Comparing Kalman Filters and Observers for Dynamic State Estimation with Model Uncertainty and malicious cyber attacks" IEEE May 2016
[10] Uttam Adhikari,Thomas Morris,IEEE, and Shengyi Pan, "WAMS Cyber-Physical Test Bed for Power System,Cybersecurity Study, and Data Mining, IEEE Trans. Smart Grid Vol 8 NO 6 Nov 2017.
[11] Mission support "Cyber threat and Vulneraliblty analysis of the US Electric Sector" Idaho National Laboratory August 2016.