MODELING, CHARACTERISATION AND DATA EXCHANGE SECURITY OF PMU

Thesis submitted to

DELHI TECHNOLOGICAL UNIVERSITY

FOR

THE AWARD OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

By

POONAM JUNEJA

(2K17/Ph.D./EE/19)

Under the Supervision of

Prof. Rachana Garg and Prof. Parmod Kumar

Department of Electrical Engineering

Delhi Technological University

Delhi-110042

April 2024

DECLARATION

This is to certify that the thesis titled **“**Modeling, Characterisation and Data Exchange Security of PMU**”** was carried out by Ms. Poonam Juneja under the supervision of Prof. Rachana Garg and Prof. Parmod Kumar, Delhi Technological University, Delhi, India.

The interpretations put forth are based on my reading and understanding of the original texts and they are not published anywhere in the form of books, monographs or articles. The other books, articles and websites, which I have referred, are acknowledged at the respective place in the text.

For the present thesis, which I am submitting to the university, no degree or diploma has been conferred before, either in this or in any other university.

Date: 10/9/2023
Place: New Delhi

Ms. Poonam Juneja
2K17/Ph.D./EE/19
Department of Electrical Engineering
Delhi Technological University
Shahbad Daulatpur, Delhi-110042, India

CERTIFICATE

This is to certify that the thesis titled **“Modeling, Characterisation And Data Exchange Security of PMU”** submitted for the award of the Doctor of Philosophy is original work to the best of our knowledge. The work was carried out by Ms. Poonam Juneja under our guidance and has not been submitted in parts or full to this or any other University for the award of any degree or diploma. All the assistance and help received during the course of study have been duly acknowledged.

Prof. Rachana Garg	Prof. Parmod Kumar
Department of Electrical Engineering	Department of Electrical Engineering
Delhi Technological University	Maharaja Agarsen Institute of Technology
Shahbad Daulatpur, Delhi-110042, India	Rohini, Delhi-1100, India

ACKNOWLEDGEMENT

It has been both fascinating and incredibly fulfilling to write this thesis. First and foremost, I want to express my gratitude to God for giving me strength and support throughout my life and for always paving the route for my continued education.

I want to sincerely thank my supervisors, Prof. Rachana Garg and Prof. Parmod Kumar, for all of their support in helping me complete this thesis work. They provided invaluable advice, explanation, recommendations, and support during the entire process. They were incredibly encouraging and supportive as I was writing my thesis.

For their tremendous assistance and invaluable guidance throughout the entire study on this thesis, I would like to extend my sincere gratitude to Prof. Uma Nagia, DRC Chairman, and Prof. Rachana Garg, HOD, Electrical Engineering, Delhi Technological University (previously Delhi College of Engineering).

I would like to express my gratitude to Vice Chancellor Prof. Prateek Sharma for helping to create a conducive environment at Delhi Technological University for me to complete my study. All SRC members have my warmest gratitude for their invaluable advice and ongoing support during my research.

Sincere appreciation to Delhi Technological University administration for providing me all the facilities I needed to successfully complete my assignment. I want to express my gratitude to the EED, Central Library, and Central Computer Center office employees for their invaluable assistance and support. I also want to express my gratitude to the founding chairman of the Maharaja Agrasen Institute of Technology, Dr. Nand Kishore Garg, for his unwavering support.

My parents, Mrs. Reshma Zakhmi and Mr. J.P. Zakhmi, and my mother in law Ms Kamlesh Kumari have given me so many dreams, blessings, and opportunities. All of my successes had been largely a result of their confidence in my talents. I find myself overwhelmed while trying to express my thanks to my spouse, Mr. Saurabh Juneja, who inspired me to believe in myself. He has consistently offered comments and a critical appraisal of my work. I owe my children Saanvi and

Samaira a debt of gratitude for their unwavering support, unwavering faith, and patience during this time of study. Additionally, I would want to express my gratitude to my brother Mr. Chirag, my niece Ms. Arshia Arora, and their unofficial support in the pursuit of this research project.

I would like to thank all my seniors and my friends, Dr. Pallavi, Ms Supriya Sharma, Dr. Simmi Sharma and Ms. Manvi for their co-operation and informal support.

I am appreciative of everyone who helped me conclude my dissertation studies, whether directly or indirectly. While it is impossible to name everyone, I nevertheless want to recognize their commitment to this work.

Poonam Juneja

(2k17/Ph.D./EE/19)

ABSTRACT

The reliability and security of operational data sets are crucial considerations when evaluating a Phasor Measurement Unit (PMU). It is an intelligent device that provides real-time monitoring and measurements of electrical parameters in power systems and is an essential part of managing and operating SCADA systems and smart grids. Additionally, it can be used to detect micro-grid islanding, islanding, and isolation. In a broad area power system network, it is necessary to gather online real-time data referencing a synchronous frame without interruption. This requires PMU to be reliable and required accurate values of the parameters. As a result, the reliability and sensitivity of PMUs have been evaluated and calculated. Additionally, based on the uncertainties in each of its many modules, fuzzy logic analysis is performed to assess the dependability of the phasor measurement unit (PMU). This is constructed with a logic gate representation, and the Markov reliability model is implemented. The theory and configuration of PMU for synchronization detection are also examined with regard to compilation and operation.

PMU is an intelligent, integrated system made up five modules and two sub modules such as module-1(Data Acquisition module), module-2(Global Positioning System), module-3(phasor processor) module-4(communication module), and module-5(Power Supply). Further Module-1 comprises of sub-modules viz. transducers, anti- alias filter, and analog to digital converter (ADC), Module-2 comprises of sub-modules GPS receiver, crystal Oscillator/ switch, Module-3 comprises of sub- modules hardware and software of Central Processing Unit (CPU), Module-4 has MODEM for communication and Module-5 is power supply. Each unit has a certain function, and depending on how frequently they fail and need repairs, they are available. The PMU is rendered useless and ineffective due to fault in any unit. Five PMU modules can, therefore be referred to as "series modules." Data is collected and transferred from the power system (the Data Acquisition module or system) to the CPU through the transducer, filter, and ADC. The ADC's start and stop functions are controlled by a GPS. The transducers gather information from the CT and PT as well as about the status of the circuit breaker, location of isolator, and other variables. The CPU analyzes the output of the ADC and timestamps it with the current time prior to transmission, while alias filters reduce data- and information-introduced noise. The time stamping of data is controlled by the GPS signal. If the GPS receiver malfunctions, the crystal oscillator will continue to run until the 50 Hz error does not increase by

more than 31 microseconds per hour. For the working of all modules power supply unit is needed.

A mathematical model of the PMU and its modules is constructed using Markov probability theory. The failure and repair rate of all sub-modules are calculated and the resulted rate is taken as the failure and repair rate of their respective modules. This is done in order to streamline the calculations. From the analysis of the result it has been observed that GPS module is the most critical module. Digital data is time-stamped and synchronized by the satellite-based Global Positioning System (GPS). In this study using time diagram of the failure rate and repair rate is also provided, along with the encountering frequency of each module. Through the use of a random number generator, the stipulated failure and repair rates, and simulation studies, the dependability of the PMU was evaluated. The proposed model is simulated in Mat lab version 7.

This study suggests a novel and creative method of assessing the PMU performance indicator. An interval type-2 fuzzy logic system (IT2FS) with several cut sets is used to determine RAM. With this, uncertainty is transformed into a set of prospective data points. When assessing the PMU's overall performance, it also takes into account the GPS receiver's failure and a subpar switch. Performance graphs are made to give a visual picture of the risk and possibility for design improvement associated with the PMU. In order to improve the quality of PMU modules, it is crucial to detect design defects.

The failure rate of the PMU module has not been sufficiently described by the manufacturers. There is a lack of clarity regarding the percentage of PMU modules that fail during operation. The ever-changing external factors contribute to the dynamic nature of the information processing. Firstly the fault tree model of PMU, which is a representation of system failure, is developed. To take into account the redundancy factor Petri Net is implemented using AND/OR transformation rules. The reachability graph is also developed. Fuzzy Petri Net (FPN) is developed which is an extension of Petri Net that permits the modeling of system with uncertain or imperfect data. FPN provide dynamic as well as redundant feature to the model. This FPN has been utilized to assess the dynamic reliability of a PMU when repair or failure rate are uncertain. With FPN developed the sprouting tree algorithm (STA) can be used to analysis it. This generates a Petri Net’s state space representation. FPN based STA is a hybrid method that

incorporates the benefits of FPN and STA to solve optimisation problems involving uncertain or imprecise data.

Data from PMUs must be used for monitoring and controlling is widely used power systems. A PMU is a smart device that keeps track of information about the power system, including the flow of energy between utilities and grids. The communication protocol used for the Data Acquisition module, IEEEC37.118 is centralized and unencrypted. In order to address the power exchange disparity, the role of Blockchain technology in the PMU is identified . With the help of a variety of MYSQL database management systems located in the AWS cloud, the thesis presents a novel approach for creating a distributed and scalable data model based on Blockchains. The method manages the heterogeneity within the database of different nodes contributing to the information flow using PMU data translated into a JSON data representation. The model's use of password and Blockchain as encryption techniques makes it cyber-secure. The coding language used is python.

The research work presented in the thesis is expected to provide good exposure to modeling, characterization and data security of PMU.

TABLE OF CONTENTS

Chapter – I Introduction

Chapter – II Literature Review

Chapter – IV Risk Assessment of PMU

Chapter – V Uncertain Data Processing of PMU Modules Using Petri Net

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

PMU	Phasor Measurement Unit
GPS	Global Positioning System
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
RBD	Reliability Block Diagram
PT	Place/Transition
CPN	Colored Petri Nets
PT	Petri Nets
TPNs	Timed Petri Nets
SPNs	Stochastic Petri Nets
PMU	Phasor Measurement Units
EMI	Electromagnetic Interference
CT	Current Transformers
VTs	Voltage Transformers
AFE	Analogue Front End
ADC	Analog to Digital Converters
DSP	Digital Signal Processing
GPS	Global Positioning System
CPU	Central Processing Unit
MODEM	Modulator Demodulator
RTU	Remote Terminal Unit
IT2FS	Interval Type2 Fuzzy Logic System
AI	Artificial Intelligence
FOU	Footprint of Uncertainty
RAM	Reliability, Availability, and Maintainability
T1FLS	Type1 Fuzzy Logic System
FPN	Fuzzy Petri Nets
STA	Sprouting Tree Algorithm

IRS	Immediate reachable set
MFA	Multifactor authentication
AWS	Amazon Web Services
SIEM	Security Information and Event Management
IPS	Intrusion Prevention System
IDPS	Intrusion Detection and Prevention System
DAO	Decentralized Autonomous Organizations
DeFi	Decentralized Finance
NFT	Non Fungible Tokens
SHN	Smart Hierarchical Network
IOT	Internet of Things
P2P	Peer to Peer
FPGA	Field Programmable Gate Array
MDA	Message Digest Algorithm
SHA1	Secure Hash Algorithm 1
SHA2	Secure Hash Algorithm 2
SHA3	Secure Hash Algorithm 3
BLAKE2	BLAKE2 cryptographic hash function
MAC	Message Authentication Code
POW	Proof of Work
JSON	JavaScript Object Notation
AWS	Amazon Web Services
MW	Megawatt (unit of power)
MREB	Maharashtra Electricity Board Electricity board of the state of Maharashtra, India
WREB	Weston Regional Electricity Board (referring to a specific regional electricity board, possibly overseeing the area where the transmission is being monitored)

LIST OF SYMBOLS

μ	Repair rate
λ	Failure rate
P	Probability
$f(s)$	Frequency encountering state
T	Mission time
α– cut	Degree of Fuzzy set
Σ	Standard deviation
ϑ	Finite set of proposition
γ	An association function that map from transition to certainty factor
δ	An association function that map from place to truth degree [0, 1]
θ	An association function that map from place to proposition
α_i	Truth degree of antecedent/consequent
c_m	Certainty factor
R_m	Fuzzy rule
Q	Set of successful nodes
Z	Truth of proposition
β	Threshold value

CHAPTER - I
INTRODUCTION

1.1. INTRODUCTION

The Phasor Measurement Unit is an intelligent device that measures and monitors electrical parameters in a power system in real time. It typically measures three critical parameters of electrical quantity: magnitude, phase angle, and frequency. These measurements can provide a comprehensive view of the power grid's behaviour, allowing for early detection of problems and more efficient maintenance and operation of the grid. Intelligence embedded in such devices requires risk assessment as an integral part of system design requirements. A smart device is degraded if it continues to execute a function within acceptable limits lower than the specified values or if it can perform only a portion of its essential functions. There may be multiple states of degradation of PMU causing degradation of system's performance. In some instances (viz., GPS receiver of PMU), if the level of deterioration exceeds a certain threshold, the system may not function properly, this may be deemed as a system failure.

In wide area power system network it is important to acquire online real time data in reference to synchronous frame uninterruptedly. Phasor measurement unit is one such intelligent device. It comprises of five modules and two sub modules such as module-1(Data Acquisition module), module-2(Global Positioning System), module-3(phasor processor) module-4(communication module), and module-5(Power Supply) as shown in Fig. 1.1. Further Module-1 comprises of sub-modules viz. transducers, anti- alias filter, and analog to digital converter (ADC), Module-2 comprises of sub-modules GPS receiver, crystal Oscillator/ switch, Module-3 comprises of sub-modules hardware and software of Central Processing Unit (CPU), Module-4 has MODEM for communication and Module-5 is power supply. Failure of either module can make the PMU unavailable to carry out the desired functions. Thus, PMU can be considered as functionally series connected device of modules as the failure of any one module will lead to failure of whole unit.

Further, the precision of components used in PMU design and assembling may gradually vary with operation and age. This diminishes the performance, dependability, and safety of the PMU. Thus, there is a need for the Modeling and Characterization study of PMU regarding reliability and sensitivity. Reliability is "the probability that an item can execute a necessary function under specified conditions over a specified period."[1] In contrast, sensitivity is the percentage change of output when one or more parameters varies for any reason [2].

The phasor measurement unit (PMU) is a time synchronized smart device that measures frequency, voltage, current, and active power in a distributed power system spread over a wide area. These parameters are critical for line monitoring and control of power system Thus, for the successful power system operation, PMU availability must be high. A single PMU for this purpose generally has an availability of about 95%. This can be enhanced to more than 99% by using dual PMU in hot standby mode. The unit that can fail and is loaded identically to the operational team is called a "Hot Standby Unit.[3]-[10]

PMUs provide valuable data that can be used to improve grid reliability, increase efficiency, and facilitate the integration of renewable energy sources. Additionally, they can detect and isolate power outages and other anomalies thus improving grid stability and reducing the likelihood of blackouts. So risk assessment of PMUs using fuzzy type 2 can be done. PMUs also play crucial role in maintaining the stability, reliability, and efficiency of the power grid. They are likely to become even more critical as the grid continues to evolve and incorporate new technologies. They are advanced measuring devices deployed at various points in the power grid to provide synchronized voltage, current, and frequency measurements. These measurements are taken at a high rate, typically once every 30-60 milliseconds, and are used to monitor the behavior of the power grid in real-time. The synchronized measurements provided by PMUs allows detecting abnormal conditions, such as power outages, and provide the data necessary for advanced control algorithms to respond quickly and effectively.[31]-[40]

Manufacturers define the PMU's parametric values in intervals. These parametric values could deviate from the design value due to environmental and operational conditions. Hence, PMU module parameter values are always within the region of uncertainty. To account for the uncertainty in the parametric set, a soft computing technique such as fuzzy logic is necessary.

This prompted the examination of the PMU's risk performance using an Interval type-2 Fuzzy Logic (IT2FS).

The redundancy of sub- module of PMUs is another key factor to be taken into consideration while evaluating its reliability. Petri Nets may be extremely useful when studying and analysing complicated systems like power systems, especially when combined with specific devices like PMUs. This combination can provide significant advantages. A Petri Net's dynamic structure is analogous to the dynamic structure of a tree that is sprouting new branches. When it comes to coping with the inherent unpredictability of the transmission of information along the branching path of a sprouting tree, fuzzy logic reasoning is the most effective method.[61]-[80]

The correctness of data received by the power system operator from PMU is the prime factor for the smooth operation of the power system and the implementation of advanced functions. Data exchanged during communication should not be breached by unauthorized disclosure or cyber-attacks. Therefore, the data received should be secured. Key features of the data transfer should include confidentiality, integrity, and availability. These requirements can be met by Blockchain technology.[100]-[120]

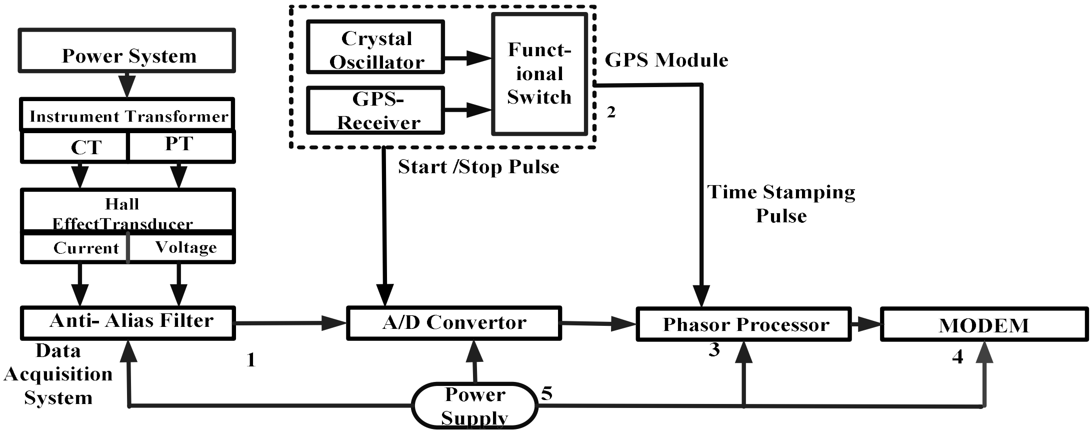


Fig.1.1: Functional Block Diagram of PMU

1.2. Reliability and Sensitivity Studies

Reliability, sensitivity, and thermal characterizations are some of the essential features of PMU.

i) Reliability refers to the likelihood that the device will run without failure for a set period under specified operating conditions.

ii) A system's reliability is the capacity to operate without failure for an extended length of time under specified operating circumstances with minimal downtime for repairs and preventative maintenance.

iii) The capacity of the equipment to retain specific attributes under specified conditions for some time is presumed to be the reliability of the equipment.

1.2.1. Reliability Analysis

Availability is a criterion of evaluation for a repairable system that considers both the dependability and maintainability of the system. When a system is available, it means it will work as intended when it is needed. It is when a system will not be in a failed state or undergoing maintenance when needed [9]. The numerical value of availability is a probability ranging from 0 to 1. The system's failures and repair time are considered for the availability calculations.

$$Availability = \frac{OperationaltimeofPMU}{OperationaltimeofPMU + DownTime} * 100 = \frac{\text{mean time between failures } (MTBF)}{Meancycletime} \tag{1.1}$$

MTBF is the Mean time between failures and is the function of the failure rate (λ) and can be written by:

$$MTBF = \lambda^{-1} \tag{1.2}$$

Thus, the reliability can be computed using eqn.(1.3)[8]

$$Reliability = e^{-\lambda t} \tag{1.3}$$

If σ_i is the stress because of operating conditions, then the failure rate can be evaluated by eqn.(1.4)[8]

$$\lambda = \lambda_b (\prod_{i=1}^{n} \sigma_i) \tag{1.4}$$

where σ_i represent the product of all the stress factors appropriate for a specific functional block of PMU. The various stress factors$\sigma_{e,}, \sigma_q, \sigma_s, \sigma_t and \sigma_v$ correlate to the power rating, operating environment, device quality, reverse voltage, device index factor, and temperature. The total failure rate of a, PMU, λ_{PMU}can be evaluated by the addition of the failure rate of all the blocks.

.$\lambda_{system} = \sum \lambda_{i(functionablock)}$

Reliability, availability, and maintainability are essential criteria for the performance evaluation of PMUs and risk assessment regarding RAM (reliability + availability + maintainability).

When two or more components are arranged in parallel to perform the same function, reliability can be increased. This is referred as redundancy. Redundancy can be standby or active, meaning that both parallel elements load or operate simultaneously. In the latter scenario, only one redundant element is loaded or functional, and the second redundant element is only activated in the event that the first one fails. The benefit of standby redundancy is that it loads and deteriorates only one component. The drawback is that this type of configuration typically requires a switch or other such component, which raises the price and may also make the system less reliable.

1.2.2. Sensitivity Analysis

Sensitivity analysis is an analysis of how various sources of uncertainty in the model input can be assigned to the uncertainty in a model's output, whether it be numerical or not [9]. It is a crucial component of all risk assessments, both qualitatively and quantitatively. This analysis is helpful since it enhances the model's forecast. Sensitivity analysis is a valuable technique that assists decision-makers in determining their level of sensitivity and selecting the best course of action in response to variations in one or more parameter input values. Sensitivity analysis is a performance assessment method used to assess how changes in the system's parameters affect the system's performance [10].Few sensitivity analysis techniques, such as partial differentiation, partial correlation, and regression techniques, are used by most investigators. By using partial differentiation, one can determine the normalized sensitivity of a quantity, or the percentage change in the quantity's value for every 1% change in the parameter of interest.

1.3. Type 2 fuzzy system

The data provided by manufactures are uncertain in nature thus this uncertainty in the parametric set is taken into account and a soft computing technique such as fuzzy logic is necessary. This also prompted the examination of the PMU's risk performance using an Interval type-2 Fuzzy Logic (IT2FS) system. It analyses PMU data set uncertainty similar to the brain processing uncertainty information[60]. It can therefore be dubbed as "risk assessment based on artificial intelligence". To account for ambiguity and uncertainty of PMU sub-module’s parametric values fuzzy logic system, a soft computing technology is used. In consideration of IT2FS the study adopted α - cut approach for evaluating the risk assessment, reliability indices, and RAM sensitivity of PMU. Reliability, availability, and maintainability are three qualities that can be used to assess the performance of a PMU (RAM).

1.4. Uncertain Data Processing of PMU Modules Using Fuzzy Petri Net

The failure rate of the PMU module has not been sufficiently described by the manufacturers. There is a lack of clarity regarding the percentage of PMU modules that fail during operation. The ever-changing external factors also contribute to the dynamic nature of the information processing that takes place. The fuzzy reasoning Petri Net (FPN) is the ideal tool for evaluating the uncertainty in dynamic state of failure rate of PMU[66]. Petri Nets are type of mathematical modeling tool that can be utilised for the purpose of describing and evaluating complicated systems. PMUs, or phasor measurement units, are devices that are utilised in the field of power systems to perform the functions of measuring and monitoring a wide variety of electrical quantities. Voltage, current, and frequency are the components that make up these variables. Petri Net's dynamic structure is analogous to the dynamic structure of a tree that is sprouting new branches. This study has used the sprouting method which offers design and system engineering insight into the failure flow of PMU components.

1.5. Data exchange security

While reliability and sensitivity characterizations estimate the risk capability of PMU, the data set transfer security from one PMU to another PMU or PMU to power system operator is maintained by Blockchain technology. The problem of enabling safe transactions in decentralized Smart Grid energy trading without depending on a trustworthy third party was examined by N. Aitzhan and D. Svetinovic [120]. The implementation of a decentralized energy trading system allowed for the anonymous negotiation of energy pricing and the safe execution of transactions through the use of Blockchain technology, which is encouraged in order to enhance privacy and security. Blockchain technology is a framework for storing public transactional records, or blocks, across several databases, or the "chain," within a peer-to-peer network of nodes[92]. This type of storage is commonly known as a "digital ledger." The digital signature of the owner authorizes each transaction in this ledger, ensuring its authenticity and preventing any manipulation.Hence, the data in the digital ledger is extremely safe. Blockchain transactions take place on a peer-to-peer network of computers (nodes) that are dispersed throughout worldwide. Every node contributes to the network's security and operation while keeping a copy of the Blockchain.

1.6. MOTIVATION

The blackout of 2012 has pressurized/forced Indian researchers to innovate the electric power grid into a smart power grid. Further, the development of distributed generation resources integrated with the primary power grid needs to continuous monitoring, regulation, and control of the power grids. Remote terminal units (RTU) were used earlier. However, these devices don’t meet the needs of the smart grid. Phasor measurement units and time-synchronized devices meet the requirements of a modern complex smart grid with renewable energy resources. Thus, the PMU shall be highly reliable and able to identify the type of fault, its location, and severity. This has motivated to carry out modeling and characterization studies and explore the security of data (stored in the cloud) and information exchange through PMU.

1.7. RESEARCH OBJECTIVE

Phasor measurement unit is an intelligent and synchronized device that can capture power system data in online real-time mode and stamp it with references to GPS frequency. PMU is a comparatively new device and, therefore, needs to be evaluated for its reliability and performance under parametric variation of its modules. Further, PMU transfers the data to the state energy control center/regional energy control center using appropriate communication channels. This communication channel may be microwave, satellite, or web. The researchers are also exploring the use of cloud for storing the data and process advanced power system functions through the energy control centers. The desired need is to exchange data and process them as per contract. Thus, the present research aims to develop mathematical model of PMU under deterministic and uncertain conditions, compute its reliability and sensitivity, and also to conduct simulation studies to estimate the reliability of the PMU by simulating the failure and repair rate of random behavior of the system and also ensures secure data transmission without breaching the security.

1.8. RESEARCH GAP AND PROBLEM IDENTIFICATION

To meet objectives, a literature review has been carried out, and the following research gaps are observed.

(i) There is a need to evaluate the reliability and sensitivity of the phase measurement unit (PMU).

(ii) Further, the parametric value and technical data defined by manufacturers are uncertain and need some intelligent method to consider the uncertainty in the PMU data. The present practice of defining the parametric value and technical specifications of PMU by the manufacturers lies in the set of ranges. PMU models based on Type-2 fuzzy system/IT2FS may be explored. Also the Petri Net model could be developed.

(iii) The data set/information captured by PMU is transferred to the energy control centre. This necessitates a need to provide security to the data, information, and processing as per the contract.

Based on the literature review and technological gaps observed, the following problems are identified:

1. PMU modeling, performance analysis, and simulation studies.
2. Sensitivity and risk assessment of PMU using Markov model and fault tree graph theory
3. Petri Net model of PMU to access the performance and dynamics of events.
4. Intelligent model of PMU using Interval Type 2 Fuzzy System.

1.9. RESEARCH METHODOLOGY

To compute and simulate the above-proposed problems, the following methodology will be explored for the present research work:

i) Literature review of PMU architecture, modeling, sensitivity, reliability techniques, Petri Net, Blockchain, and fuzzy Petri Net.

ii) Analysis of various techniques and tools such as MATLAB /Petri Net/ Fuzzy Logic type-2 for PMU modeling.

iii) Risk assessment using the Markov dynamic model for PMU.

iv) Exploring Blockchain technology for modeling PMU and data/information exchange security.

1.10. ORGANIZATION OF THESIS

Chapter I present the introduction of PMU, motivation, objectives and problem identification of the research work. The organization of the thesis is also presented in this chapter.

Chapter II presents the literature review of mathematical modeling and characterization evaluation of PMU, Modeling using Fuzzy Logic system, Petri Net model and its applications, Data security using Blockchain technology. This chapter presents the current research and methodology to identify the research problems, develop ideas, and ensure that the proposed research work is not a replicating one.

Chapter III discusses the characterization evaluation of PMU. This chapter presents the dynamic logic model of the PMU. Likewise, the reliability indices calculation is performed. The Markov dynamic model is then described, and sensitivity evaluation follows.

Chapter IV presents the risk assessment of the phasor measurement unit using Fuzzy Logic analysis. This section describes the Fuzzy Logic model and Fuzzy sensitivity to PMU. Reliability is also computed, as well as the application to PMU for risk assessment.

Chapter V presents the Uncertain Data Processing of PMU Modules Using Fuzzy Petri Net. The Petri Net Architecture and Logic are described in depth, as well as the Fuzzy Petri Net Structure. Composite Fuzzy Production Rules are fabricated. The Fuzzy Petri Net Based Sprouting Tree

Algorithm and a Flow Diagram for Sprouting Tree development are also described. Finally, the application of the Petri Net to the PMU is discussed.

Chapter VI presents the Conformation of PMU Data Transfer Security. The chapter begins with an introduction to the Blockchain, followed by a discussion of Blockchain application to PMU. This concludes with a discussion of Blockchain implementation for PMU security. Also supplied is extensive Python code.

Chapter VII summarises and highlights the main conclusions of the proposed work. The potential for more research in this field is also noted at the end of this chapter.

The list of references and appendices are provided at the conclusion of the thesis.

1.11. CONCLUSIONS

The PMU features and its characterization are presented in this chapter. The objectives and scope of the work are also discussed. Methodology to analyze the risk assessment problem has been identified. Chapter-wise dissection is also presented.

CHAPTER - II
LITERATURE REVIEW

2.1. INTRODUCTION

The objectives, motivation, and identification of the research's challenges are defined in Chapter I. A survey of the relevant literature has been done in order to obtain an appropriate comprehension of the research problems. A power system is a dynamic system that includes electricity generation, transmission, and distribution to end customers. Integration of non-conventional energy sources into the power system's main grid has increased its complexity. Monitoring, regulating, and controlling the power system grid during normal and transient states is necessary to ensure the continuity of power supply to end users. Also, according to the contract, the interchange of information and data between the operator and end-user or maintenance personnel must be protected. The phasor measurement unit is one such gadget that is able to do the aforementioned tasks by incorporating intelligent security technologies. The literature review presents the current research and methodology to identify the research problems, develop ideas and ensure that the proposed research work is not a replicating one. The references cited in this chapter are also representative rather than exhaustive. Based on the objectives outlined, a literature review of some of the significant research work done under the following areas is discussed below:

a. Mathematical Modeling and Characterisation Evaluation of PMU
b. Modeling using Fuzzy logic system
c. Petri Net model and its applications
d. Data Security Using Blockchain Technology

2.2. MATHEMATICAL MODELING AND CHARACTERISATION EVALUATION OF PMU

PMUs are gaining utility in power systems due to their capacity to deliver precise and synchronised measurements of voltage and current phases. These measures are vital for the onitoring and control of power systems in real time, which is essential for assuring system stability. These capabilities are used for multi-function.

- Enhance the precision of system condition modeling.
- To anticipate and identify grid stress and instability
- After a disruption has occurred, provide data for event analysis.
- Identification of inefficiencies
- To anticipate and control line bottlenecks.

N. Gupta, R.Garg, and P. Kumar[1] have calculated the grid-connected PV system's dependability. The authors have estimated the sensitivity of the PV system to the parameter of interest, taking into account the environmental stress. Farrokh Aminifer et.al [2] have calculated the PMU reliability model for wide-area measurement. Using fuzzy logic functions, they have assessed the uncertainty for various phase measurement components. C. Singh et al. [3] propose a systematic approach to assess the reliability of such systems, considering factors such as DER integration. The paper provides insights and methodologies to enhance the reliability analysis of distribution systems in the context of evolving energy landscapes. The research contributes to the field of sustainable energy by addressing the challenges and considerations associated with the integration of distributed energy resources into the power distribution infrastructure. C. Singh et al. [4] the paper explores strategies and methods to ensure the reliability of power systems that incorporate cyber-physical elements. It addresses the challenges and considerations arising from the integration of information technology with power systems, emphasizing the importance of reliability assurance in this context. The authors likely discuss methodologies and approaches to enhance the reliability of cyber-physical power systems, contributing valuable insights to the field. Yang Wang et al. [5] have used a fuzzy logic model, and have computed the reliability of the PMU in light of data uncertainty. They have also devised a fuzzy logic-based index to determine the various uncertainties. Peng Zhang et al. [6] have evaluated the PMU's reliability using the Monte Carlo Dynamic Fault Tree technique. In this research, GPS and CPU hardware redundancy has also been considered to improve the PMU's reliability. Pukar Mahat et al. [7] suggested a hybrid method for detecting islanding in a distribution system with several DG units operating at unity power factor. It coupled the actual power shift with the average voltage change rate. Only when the average rate of voltage change could not differentiate between grid-connected and islanding conditions was a real power shift implemented. RPS altered the actual strength of DG and distinguished islanding from other disturbances. B. S Dhillon et al. [8] this book covers a wide range of topics related to engineering dependability, including as methodological and real-world applications. It covers methods like failure analysis, maintenance plans, and reliability modeling that is used to evaluate and enhance the dependability of engineering systems. M.S Ding et al. [9] have done computation of reliability of digital relay without considering its repairing. L. R Castro et al. [10] have discussed the computation of the reliability of substation control system. The work mainly focuses on the dependability assessment of substation control systems in relation to power generation, transmission, and distribution. Analyzing the parts, redundancy, fault tolerance, and other elements that affect the substation control systems' overall reliability may be part of this. Y, Ren et al. [11] have explored a method for optimizing the reliability using static and dynamic fault trees models. The authors address the benefits and drawbacks of both static and dynamic fault tree techniques when it comes to building dependable systems. This helps to explain how these techniques are used to evaluate and improve the dependability of intricate engineering systems. J Yuan et al. [12] have developed the mathematical model of reliability using AND, OR and voting gates. The work also presents the simulation study for double buses tolerated fault control system modules. W Wang et al. [13] in this the importance of reliability indices in system design is explained and also have computed the various operational reliability indices. Debomita Ghosh et al. [14] have evaluated the reliability for different system such as smart grid communication system, and power system network.Chen, Y. Qi, and M. Wang are the authors (2017) [15] this work describes a method for assessing the dependability of PMUs in wide-area measuring systems. The suggested methodology models the dependability of PMUs using a combination of fault tree analysis and Bayesian networks. S. Singh, G. Singh, and A. Sharma (2017) [16] this article evaluates the performance of PMU-based fault location Algorithm. Using real-time data from a power system, the authors assess the accuracy and resilience of the methodologies. R. Billinton et al.[17] The reliability computations which include the failure rate λ and repair time r and switching probability is explained but redundancy of the module is not considered.C. Wang, X. Yan, and L. Cheng. (2019)[18] this article proposes a probabilistic approach for evaluating the reliability of PMUs. The proposed model uses a Bayesian network to analyse the dependencies among PMU components and model their interdependencies. Nemer et al. [19] The reliability aspect on integrated micro grid with wind and solar energy resources and the impact of restoration on the system is studied. Also evaluated the effect of uncertainty in wind and solar generating plant using Auto Regressive Moving Average model. Behahzad Karimi et al. [20] Bi-objective mathematical model to optimize reliability and cost in flexible manufacturing system is developed. And computed the reliability of a tool availability by increasing the failure rate. Phade [21] this book has presented the structure of PMU. Also gives a complete detailed explanation about the architecture of Phasor measurement unit. P. Mahajan et al. [22] the authors in this paper have developed the sensitivity functions of series impedance and shunt admittance matrices. Ch. Murthy et al. [23] the work in this research have computed reliability considering perfect switching . P. Hiberetal[24] in this a method for extracting reliability importance indices from reliability simulations of electrical networks is explored. The author has examined the communication network's reliability in wide area protection, as published by Z.H. Dai et al. [25]. In this article James Li [26] uses Markov modeling to calculate the dependability of a parallel redundant system with varying failure and repair rates. S. Gupta et al. [27] performs a sensitivity analysis in addition to dealing with the factors that affect electrical energy usage. Peng Li et al. [28] describe how to use phasor measurement units (PMUs) in distribution networks and offer new choices for voltage management and calculation of voltage-to-power sensitivity.

Y. Fu, M. Kezunovic, and X. Sun (2012[29]) this research gives a reliability assessment of PMUs in power systems based on an investigation of PMU failure rates and its repercussions. Singh, Pankaj et al. [30] the study demonstrates that PMUs are generally dependable, but can fail for a variety of reasons, including ageing, environmental conditions, and communication problems. In addition, a strategy for selecting PMUs based on their reliability performance is proposed

Overall, the literature review indicates that PMUs are gaining significance in power systems due to their capacity to offer synchronised and accurate voltage and current phasor measurements. To ensure the accuracy of real-time monitoring and control of power systems, PMU dependability is crucial. Many studies have been undertaken to assess the dependability of PMUs and to suggest methods for improving their dependability.

2.3. MODELING USING FUZZY LOGIC SYSTEM

In this review of the relevant literature, several recent studies that propose fuzzy logic controls for power systems are analysed. The papers centre on strengthening the performance of power systems, reducing the impact of uncertainties, and improving the system's overall stability. PMU data is included in the development of the suggested controllers, which make use of type-2 fuzzy logic, adaptive fuzzy logic, and hybrid neural network-fuzzy logic. The purpose of this research is to address the issues associated with integrating renewable energy sources into power systems and micro grids, as well as to improve the control of active and reactive power. The controllers that have been proposed could have repercussions for the architecture of future power systems as well as the shift towards the use of renewable energy sources. R. Xiao and H. Wang (2022)[31]have presented a study, in which, the authors suggest a wide-area adaptive fuzzy control strategy for power systems that makes use of PMU data. The purpose of the controller was to enhance the system's stability and lessen the detrimental effects of disruptions. F. Zhang and Q. Wang (2021)[32]. The purpose of this research is to present an improved type-2 fuzzy logic control for renewable energy generation in micro grids. The performance of renewable energy sources can be improved using the controller thanks to its design, which also allows it to manage the system's inherent uncertainty. M. El Haddad et al. (2020)[33] the purpose of this study is to propose a hybrid neural network-fuzzy logic type 2 controller for power system frequency management. The controller was developed to deal with the uncertainties that were present in the system and to make the system more stable. M. Abedi et al. (2020)[34] the purpose of this work is to present a PMU-based adaptive fuzzy logic controller for the integration of renewable energy in distribution systems. The controller was developed to manage the inherent unpredictability of the system while also enhancing the efficiency of the various renewable energy sources. J. Ghaderi and M. Moeini (2020)[35] in this study, the authors present a fuzzy type-2 controller for DC micro grids that are powered by renewable energy sources. The performance of renewable energy sources can be improved using the controller thanks to its design, which also allows it to manage the system's inherent uncertainty. R. Su et al. (2021)[36] this study offers an adaptive fuzzy type-2 power system stabiliser design utilising a hybrid GA and PSO method. Adaptive fuzzy type-2 power system stabiliser design. The controller was developed to increase the stability of the system as well as to manage the uncertainties that are present in the system. R. Das et.al (2020)[37] the purpose of this work is to present a fuzzy type-

2 controller for active and reactive power control of renewable energy systems. The performance of renewable energy sources can be improved using the controller thanks to its design, which also allows it to manage the system's inherent uncertainty. A. J. Akin et al. (2020)[38]the purpose of this paper is to propose a PMU-based fuzzy logic controller for the voltage control of distribution systems that make use of renewable energy sources. The performance of renewable energy sources can be improved using the controller thanks to its design, which also allows it to manage the system's inherent uncertainty. F. Zhao et al. (2020)[39] the purpose of this study is to present a novel design for an adaptive fuzzy type-2 power system stabiliser that makes use of an enhanced particle swarm optimization technique. The controller was developed to increase the stability of the system as well as to manage the uncertainties that are present in the system. M. H. Gheisari et al. (2021)[40]the purpose of this paper is to present a hybrid fuzzy type-2-deep neural network for wind power forecasting. The controller was developed to improve the accuracy of wind power predictions as well as to manage the uncertainties present in the system. M. Shamsi et al. (2019) [41] the purpose of this work is to propose a new fuzzy inference system for PMU-based fault detection of power system. With the assistance of PMUs, the system is intended to locate and categorise defects that may occur within the system. W. Lu et al. (2019) [42] the purpose of this work is to present a PMU with fuzzy logic control for power system frequency regulation. The performance of the frequency regulation and the controller's ability to handle uncertainties in the system are both goals of the controller's design. A. G. Abokhalil et al. (2018)[43] the authors of this research suggest a fuzzy inference system for PMU with dynamic line rating of overhead transmission lines. With the use of PMUs, the system was developed to make predictions regarding the maximum power that can be transferred by overhead transmission lines. H. Y. Khalid et.al (2018)[44] the purpose of this work is to present a fuzzy inference system for PMU-based fault locations in power systems. With the assistance of PMUs, the system is intended to identify and localise errors inside the system.

M. M. Atia et.al (2017) [45] the purpose of this article is to present a PMU with fuzzy inference system for monitoring power system oscillations. With the assistance of PMUs, the system is intended to monitor and determine the source of oscillations in the power system. M. H. Marzban et.al (2017) [46] the purpose of this study is to present a fuzzy logic-based adaptive PMU measurement error correction for power system stability analysis. The purpose of the system is to increase the accuracy of power system stability analysis as well as correct the inaccuracies that are present in the measurements taken by the PMU . S. S. S. M. Alahmadi et al. (2017)[47] the purpose of this article is to present a fuzzy inference system for PMU-based detection of false data injection attacks in smart grids. The purpose of the system is to identify and stop cyber attacks that are launched against PMUs in smart grids. W. Lu et.al (2016)[48]the purpose of this study is to propose a fuzzy inference system for PMU-based fault detection and classification in power systems. With the assistance of PMUs, the system is intended to locate and categorise malfunctions that may occur within the system. Zadeh [49] this book explains the idea of fuzzy logic, a mathematical framework that allows degrees of truth between 0 and 1, extending the concept of classical binary logic. When dealing with ambiguity and imprecision in decision-making processes, fuzzy logic is especially helpful.. H. Y. Khalid et al. (2016)[50] this study presents a fuzzy inference system for PMU for identification of critical oscillations in power systems. With the assistance of PMUs, the system is intended to determine which oscillations in the system are considered critical. P. Singh et al. (2015)[51] in this research, the authors present a fuzzy logic-based approach for determining the dynamic state of a system by analysing its PMU readings. Using PMU, the system is intended to provide an estimation of the dynamic state of the power system. M. H. Marzban et al. (2015)[52] provides a fuzzy logic-based approach for PMU data validation and correction in power systems. Validation and correction of the PMU readings, as well as improvements to the quality of power system analysis, are all goals of the system's design. M. M. Atia et al. (2015) [53]the purpose of this work is to present a fuzzy inference system for PMU for dynamic security evaluation of power systems. Using PMUs, the system is intended to do an analysis of the dynamic safety of the power system. This study presents fuzzy logic for PMU data quality control for power system dynamic analysis. M. H. Marzban et.al(2014)[54] the purpose of the system is to increase the accuracy of power system dynamic analysis as well as control the quality of the measurements taken by the PMU. M. H. Marzban et.al (2013) [55] the purpose of this study is to offer a fuzzy logic-based technique for PMU for dynamic state estimation in power systems. Using PMUs, the system is intended to provide an estimation of the dynamic state of the power system. M. M. Atia et.al (2013)[56] presents a fuzzy inference system for PMU for the detection of voltage instability in power systems. With the assistance of PMUs, the system is intended to identify and eliminate instances of voltage instability inside the system. H. Y. Khalid et.al(2012) [57] a fuzzy inference system for PMU for the identification of sub-synchronous resonance in power systems. With the use of

PMUs, the system has been built to detect and eliminate sub-synchronous resonance that may occur within the system. H. Y. Khalid et.al (2013)[58] presents a fuzzy inference system for PMU for detection of transient instability in power systems. With the assistance of PMUs, the system is intended to both identify and eliminate transitory instability inside the system. H. Y. Khalid et al. (2011)[59] the purpose of this study is to propose a fuzzy inference system for PMU for identification of forced oscillations in power systems. With the assistance of PMUs, the system is intended to detect and eliminate oscillations that are caused by externally applied forces. M. H. Marzban et al. (2011)[60] the purpose of this article is to present a fuzzy logic-based PMU data validation and correction for power system state estimation. The PMU measurements will be validated and corrected with the help of this system, and the accuracy of the power system status estimation will be improved as a result.

In conclusion, the literature review showed a wide variety of fuzzy logic-based methodologies for the purpose of enhancing the accuracy, performance, and stability of power systems through the examination of PMU data. The systems that are proposed in the papers are designed to manage uncertainties and improve the performance of renewable energy sources; they are also intended to improve system stability; detect and correct errors in PMU measurements; estimate the dynamic state of power systems; and evaluate dynamic security. Control and monitoring of power systems can be improved with the help of methodologies based on fuzzy logic, which offer a solution that is both promising and successful. These papers, which are discussed in this survey, demonstrate the potential of fuzzy logic-based systems in the field of power systems and the importance of making use of PMU data in order to achieve efficient and reliable power system operation.

2.4. PETRI NET MODEL AND ITS APPLICATIONS

This review of the relevant literature will concentrate on the power system analysis and fault diagnostic applications of Petri Nets and Phasor Measurement Units (PMUs). It consists of thirty papers that have been published. The papers discuss a wide variety of subjects, such as microgrid modeling, transient stability analysis, fault identification, and dynamic state estimation. Petri Nets are used as a modeling tool in the methodologies that are proposed in these publications. This allows for a more accurate representation and analysis of the behaviour of power systems and PMUs, which in turn provides more accurate measurements of power system variables. The survey provides an overview of the various methodologies and techniques employed in the sector. Particular attention is paid to the potential advantages of utilising Petri Nets and PMUs in power system analysis and problem diagnostics. X. Chen et al. (2021) [61] the authors of this research present a fault diagnosis approach that is based on PMU and Petri Nets. With the use of PMUs and Petri Nets, the system is intended to determine where failures are occurring in power systems. M. Li et.al(2021)[62] the authors of this study present a Petri Net-based approach for performing power system transient stability analysis using PMU data. With the assistance of PMUs and Petri Nets, the system is intended to do an analysis of the transient stability of power systems. Y. Feng et.al(2021)[63] the authors of this research present a hybrid fault detection approach for power systems that is based on PMU and Petri Nets. With the use of PMUs and Petri Nets, the system is intended to determine where failures are occurring in power systems. S. Wang et al. (2021) [64] the purpose of this study is to make a proposal for research on power system transient stability analysis based on PMU and Petri Nets. With the assistance of PMUs and Petri Nets, the system is intended to do an analysis of the transient stability of power systems. W. Zhang et al. (2020)[65] the authors of this study propose the use of Petri Nets in the fault diagnosis of power systems that are based on PMUs. With the use of PMUs and Petri Nets, the system is intended to determine where failures are occurring in power systems. K. Duan et.al(2020)[66] the authors of this research present a Petri Net for performing transient stability analysis of power systems using PMU data. With the assistance of PMUs and Petri Nets, the system is intended to do an analysis of the transient stability of power systems. X. Du et.al(2020)[67] the purpose of this article is to offer a Petri Net for power system transient stability with PMU data. With the assistance of PMUs and Petri Nets, the system is intended to do an analysis of the transient stability of power systems. S. Xu et al. 2020[68] in this research, a fuzzy-Petri Net approach is proposed for the purpose of validating PMU data and providing fault diagnostics for power systems. With the use of fuzzy-Petri Nets, the system is intended to validate PMU readings and diagnose issues in power systems. S. Li et.al(2018)[69] the purpose of this paper is to present a formal modeling and verification approach for a wide area monitoring system using Petri Nets, with the intention of guaranteeing the system's dependability and accuracy. Y. Zhang et al (2017) [70] the authors of this study suggest a PMU-based fault diagnosis system that models and analyses its data using Petri Nets. The purpose of the system is to identify and diagnose issues that may occur in power systems. Y. Wu et al. (2016) [71] the authors of this study suggest a Petri Net method for smart grids to diagnose faults and make decisions. This method is intended to diagnose and find faults in the smart grid in order to arrive at the best conclusions about the restoration of the power system.

Z. Wu et al. (2016) [72] provides a Petri Net solution to the dynamic security evaluation of power systems. The method was developed to analyse the dynamic behaviour of power systems and evaluate their level of safety under a variety of different operating scenarios. Y. Zhang et al. (2015) [73] the purpose of this article is to present an application of Petri Nets to power system protection coordination. This method was developed to analyse and improve the effectiveness of the protective coordination techniques used in power systems. H. Lin et al. (2015)[74] the authors of this research propose a Petri Net technique to analyse the impact of wind power on power system stability. This approach was developed in order to explore the dynamic behaviour of power systems that have a large penetration of wind power. X. Li et al. (2015) [75] in this paper, the authors present a fault diagnosis approach of power systems that is based on Petri Nets and decision trees. On the basis of readings from PMUs, the approach was developed to provide a diagnosis and pinpoint the location of defects in power systems. J. Wu et al (2014)[76] in this paper, a method for power systems that have a high penetration of wind power is proposed. The method uses Petri Nets. The method was developed to more accurately assess the dynamic status of power systems in their operating environments. X. Zhang et.al(2014)[77] this study proposes a modeling and analysis approach for micro grids that is based on Petri Nets. This method is intended to simulate and analyse the dynamic behaviour of micro grids under a variety of different conditions of operation. H. Chen et al (2013)[78] the authors of this study propose applying Petri Nets to the process of assessing the dynamic security of power systems that use wind power. This method was developed to assess the dynamic safety of power networks that have a significant amount of wind power penetration. S. Li et.al(2018)[79]the purpose of this paper is to present a formal modeling and verification approach for a wide area monitoring system using Petri Nets, with the intention of ensuring the system's dependability and accuracy. Y. Zhang et al. (2017) [80] the authors of this study propose a PMU fault detection system that models and analyses its data using Petri Nets. The purpose of the system is to identify and diagnose issues that may occur in power systems. Y. Wu et al. (2016) [81] presents a Petri Net fault diagnosis and decision-making technique for smart grids. This method is intended to diagnose and find faults in the smart grid in order to arrive at the best conclusions about the restoration of the power system. Z. Wu et al. (2016) [82] presents a Petri Net method for the dynamic security evaluation of power systems. The method was developed to analyse the dynamic behaviour of power systems and evaluate their level of safety under a variety of different operating scenarios. Y. Zhang et.al(2015)[83] the purpose of this article is to present an application of Petri Nets to power system protection coordination. This method was developed to analyse and improve the effectiveness of the protective coordination techniques used in power systems. H. Lin et al. (2015) [84] the authors of this study present a Petri Net technique in order to analyse the impact of wind power on power system stability. This approach was developed in order to explore the dynamic behaviour of power systems that have a large penetration of wind power. X. Li et al. (2015) [85] the authors of this study present a method for diagnosing problems with power systems that is based on Petri Nets. On the basis of readings from PMUs, the approach is developed to provide a diagnosis and pinpoint the location of defects in power systems. J. Wu et al. (2014)[86] in this article, the authors offer a method for estimating the state of power systems using Petri Nets, and they focus on those that have a high percentage of wind power. The method was developed to more accurately assess the dynamic status of power systems in their operating environments. X. Zhang et al. (2014)[87] this article proposes a modeling and analysis method for micro grids that is based on Petri Nets. This method is intended to simulate and analyse the dynamic behaviour of micro grids under a variety of different conditions of operation. H. Chen et al. (2013)[88] the authors of this study propose applying Petri Nets to the process of assessing the dynamic security of power systems that use wind power. This method was developed to assess the dynamic safety of power networks that have a significant amount of wind power penetration. A. Yavari and H. Lesani (2018)[89] the purpose of this article is to propose a new method for the placement of PMUs in power systems that will achieve both observability and measurement redundancy. In order to find the appropriate location of PMUs for effective monitoring and control of the power system, the method takes into account the topology of the system, the characteristics of the load, as well as the constraints of the PMUs. Joana Pereira et.al (2016) [90] in this research, a hybrid evolutionary algorithm is used to offer an optimal PMU placement strategy that is applicable to power systems. The technique combines a genetic algorithm with a particle swarm optimization algorithm in order to discover the ideal sites for the placement of PMUs. These locations will allow for the fewest possible PMUs to be used while still ensuring that the power system can be observed in its whole. The suggested technique is validated on power systems that adhere to IEEE standards and compared to other methodologies already in use.

Petri Nets are a type of mathematical model that can be applied to the analysis and description of complex systems in a variety of domains. They are utilised in the modeling and analysis of the behaviour of concurrent as well as asynchronous systems. Petri Nets have been utilised to model several elements of power system operations, including fault diagnosis, transient stability analysis, dynamic security evaluation, and decision-making, in the context of power systems. Petri Nets are extremely helpful when modeling complex systems because the interactions that occur between the many components of the system may be modelled as transitions between states. In order to give an accurate and efficient analysis and diagnosis of power system faults and occurrences, Petri Nets are also used in combination with other approaches, such as PMU data, fuzzy logic, and sprouting trees. Petri Nets can also be used alone. Petri Nets offer a powerful tool for enhancing the dependability, security, and efficiency of power systems, and their use is becoming more widespread in power system research and implementation.

2.5. DATA SECURITY USING BLOCKCHAIN TECHNOLOGY

In a nutshell, the research done thus far indicates that the utilisation of PMUs in cloud computing holds significant promise for enhancing the effectiveness, precision, and dependability of power system monitoring and control. Real-time monitoring and control of power systems can be made possible with the use of cloud-based PMU data management, analytics, and processing systems. These technologies can also increase the accuracy and dependability of power system operation. Cloud-based PMU data verification and consensus algorithm have the potential to ensure the accuracy and consistency of PMU data, while cloud-based PMU data fusion methods have the potential to increase the accuracy and reliability of state estimates. In general, the study that has been done on the topic indicates that PMU in cloud computing is a fruitful area for the conduct of future research and development. A. Shukla et al.[91] a Blockchain power management system for smart grids is proposed in this study. The system makes use of PMUs to enable real-time monitoring and control of the power system. The administration of energy resources will be more safe, more open, and more effective thanks to the implementation of this system. S. Zhang et al. (2020)[92] the authors of this work present a method for performing dynamic state estimate using Blockchain technology for PMU data in smart grids. By combining past data from PMUs into the estimation process, the technique is intended to improve the accuracy and dependability of state estimates. R. Singh et al. (2019)[93] the authors of this work suggest a Blockchain-enabled power quality monitoring system that makes use of PMUs to collect real-time data on several power quality parameters. The system was developed to provide safe and tamper-proof storage for power quality data, as well as to permit real-time monitoring and control of power quality. Both of these functions can be accomplished through the use of the system. S. Chakraborty et al. (2019)[94] the authors of this study propose a data management system for smart grids that is based on Blockchain technology. PMU data may be stored, shared, and analysed in a way that is efficient, transparent, and safe with this system, all while maintaining the confidentiality and privacy of the data. M. Faruque et al. (2020)[95] the authors of this work present a method for power system state estimation that uses Blockchain technology to combine data from power monitoring units. The method is intended to improve the accuracy and reliability of state estimation by fusing data from various PMUs, all while ensuring data privacy and security through the use of Blockchain technology. This will be accomplished by combining the data A. Sarkar et al. (2019) [96] the authors of this research suggest a Blockchain-based PMU data sharing system for interconnected micro grids. The framework is intended to facilitate the sharing of PMU data between micro grids in a way that is secure, transparent, and efficient, all while guaranteeing the data's privacy and security through the utilisation of Blockchain technology. L. Fan et al (2019) [97] the authors of this research suggest a Blockchain-based PMU data verification and consensus Algorithm for use in smart grids. Using a consensus method that is founded on Blockchain technology, the algorithm has been developed to ensure that the data collected from PMUs are accurate and consistent. S. Huang et al. (2020)[98] in this paper, the authors present a method for Blockchain-enabled PMU data analytics that may be used for power system monitoring and control. With the utilisation of Blockchain technology and the analysis of data from PMUs, the method accomplishes the goal of providing real-time monitoring and control of the power system. R. Kaur et al (2017) [99]. In this article, the authors suggest a PMU-based real-time power monitoring system for cloud data centres. The purpose of the system is to enable real-time monitoring of power use as well as the quality of electricity in cloud data centres, with the end goal of increasing energy efficiency and lowering costs. X. Lin et.al (2018)[100] in this work, a PMU data management system for smart grids that is based in the cloud is proposed. PMU data can be stored in a way that is private and safe, shared in a manner that is both efficient and scalable, and analysed using the system. All of this is made possible by the design of the system. S. Kumar et.al (2016)[101] the design and implementation of a PMU-based power monitoring system for cloud computing data centres is presented in this study. In addition to providing real-time monitoring of power use and power quality, the system is intended to increase energy efficiency and cut expenses. S. Zhao et.al (2017)[102] an analytics solution for PMU data that is cloud-based is proposed in this research for use with smart grids. This approach is intended to improve the precision and dependability of power system monitoring and control by enabling effective analysis of PMU data using cloud computing. This will be made possible by the method's design. Y. Liu et.al (2017)[103] a data processing and management system for PMUs based in the cloud is proposed for use in smart grids in this article. The system was developed to enable efficient and scalable processing, analysis, and administration of PMU data through the use of cloud computing. As a result, the accuracy and reliability of power system monitoring and control were significantly improved. Y. Shen et.al (2018)[104] a data verification and consensus mechanism for PMUs based on the cloud is proposed in this study for use in smart grids. By utilising a consensus process that is founded on cloud computing, the Algorithm was developed to verify that the data collected from PMUs are accurate and consistent. Y. Li et.al (2017)[105] in this study, the authors offer a cloud computing system that is based on PMUs and is intended for real-time monitoring and control of power systems. The efficiency and dependability of power system operation will be improved as a result of the system's architecture, which makes it possible to perform monitoring and management of the power system in real time by utilising cloud computing. Z. Zhang et al (2018)[106] this article presents a method for power system state estimate that is based on PMUs and cloud computing. By combining PMU data into the estimation process and making use of cloud computing, the method aims to increase the accuracy of state estimation as well as the efficiency with which it may be performed.

M. R. Faghih and M. H. Hajivand (2021)[107] in this research, we present a Blockchain-based data management system for the power grid that makes use of PMUs that is both safe and efficient. When it comes to the transmission and storage of PMU data, the system is built to protect users' privacy, keep their data secure, and maintain its integrity. S. Zhang et al (2021)[108] the purpose of this work is to present a complete survey of Blockchain for PMU data management systems for smart grids. The survey examines many facets of these systems, including data privacy, data security, data integrity, and operational efficiency. A. R. Nazir et al (2021)[109] the authors of this study suggest a security architecture for PMUs in smart grids that is based on Blockchain technology. A tamper-proof and auditable record of data transactions is provided by the framework, which is designed to secure the confidentiality, integrity, and availability of PMU data as well as provide a record of data transactions that can be audited. Y. Guo et al (2021)[110] the authors of this work suggest a system for managing PMU data that is both secure and efficient using Blockchain technology. In addition to enhancing the efficacy of data transmission and storage, the system was developed to protect the confidentiality, security, and integrity of data collected from PMUs. S. Kumar et al. (2021)[111] The authors of this work suggest a Blockchain-based PMU data management system for the secure and efficient operation of power grids. Using Blockchain technology, the system is intended to protect users' privacy, maintain data security and integrity, and make data management more effective and scalable. Its primary goal is to ensure that data is kept in its original format.

S. S. Park et.al(2021)[112] The authors of this work suggest a Blockchain-based safe PMU data management system for smart grids. Using Blockchain technology, the system is designed to protect the privacy, integrity, and availability of the data, as well as to offer a tamper-proof and auditable record of the data transactions that have taken place. P. Joshi et al (2021)[113] The purpose of this article is to offer an AI-based technique for the optimal placement of PMUs in power systems in order to increase observability. The method identifies the best possible spots for the placement of PMUs by employing a genetic algorithms and several deep learning techniques. As a result, the method improves both the effectiveness and the precision of power system monitoring. H. Li et al (2021)[114] The authors of this study suggest a real-time power system monitoring and control system that makes use of several AI techniques, including machine learning and deep learning. PMUs are used to collect data, and then artificial intelligence algorithms are applied to perform real-time monitoring and control of the power system. This results in an increase in the effectiveness and dependability of the operation of the power system. Z. Zhang et al. (2021)[115] the purpose of this research is to propose an AI-based anomaly detection approach for PMU data in power systems in order to improve monitoring and control. The method makes use of machine learning and deep learning techniques to detect unusual behaviour in PMU data. This allows for early diagnosis and avoidance of failures in the power system. R. Shahzad et al. (2021)[116] presents an intelligent detection strategy for power system transients utilising PMUs and machine learning. In order to analyse PMU data and identify transitory occurrences in real time, the method makes use of a deep learning neural network. As a result, the method improves the effectiveness and precision of power system monitoring and control. N. Baburaj et al (2021)[117]the purpose of this article is to offer an AI-based fault location method for power distribution networks that makes use of PMUs. This method analyses PMU data and identifies problem locations in real-time by using techniques from machine learning and deep learning. As a result, the method improves both the efficiency and accuracy of fault identification and location. A. E. Kanso et al. (2021)[118] the authors of this study present an AI-based method for estimating the state of power systems by employing PMUs. The method analyses data from PMUs and makes an estimate of the state of the power system in real time by using machine learning and deep learning techniques. As a result, the method improves the effectiveness and precision of power system monitoring and control.

S. Sahoo et.al(2021)[119] a method for the intelligent identification and diagnosis of faults in power systems is proposed in this research, and it makes use of PMUs and machine learning. This technology makes use of deep learning techniques to analyse PMU data in real time in order to discover and diagnose defects. As a result, the method improves the effectiveness and precision of power system monitoring and control. J. Wang et al. (2021) [120] in this study, a thorough evaluation of PMU for power system dynamic state estimation (DSE) methodologies was presented. In this study, we will go over the fundamental principles of PMUs, as well as the many types of DSE algorithm and their respective performance evaluations. In addition to this, the authors present their predictions for the further progression of PMU-based DSE.

2.6. CONCLUSION

In conclusion, the papers that were examined place an emphasis on the significance of PMU data in the monitoring and control of power systems. It has been suggested that modern technologies, such as Blockchain and cloud computing, be utilised to assure the safekeeping of PMU data as well as its sharing and analysis in a manner that is both efficient and scalable. The technologies and methods that have been proposed have the potential to cut down on energy consumption and expenses, in addition to improving the precision and dependability of the monitoring and control of power systems. Cloud data centres have also been suggested to incorporate real-time power monitoring systems that make use of PMUs. Such a system has the potential to significantly improve energy efficiency while simultaneously lowering costs. These papers, taken as a whole, highlight the growing interest in utilising PMUs for advanced power system monitoring and control, and they suggest that further research in this area could do significant benefits for power systems.

CHAPTER-III
RELIABILITY AND SENSITIVITY CHARACTERIZATION OF PHASOR MEASUREMENT UNIT

3.1. INTRODUCTION

Phasor measurement unit (PMU) used for real time system operation must be trustworthy. Its continuous monitoring and aging deteriorates the performance, dependability, and security of the system over a period of time. If the level of deterioration exceeds a specific threshold, the system may cease to function properly which may be considered as a system failure. Failures cannot be eliminated totally. However, they can be reduced by enhancing the system design reliability. According to the Institute of Electrical and Electronic Engineers (IEEE), "Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time". Reliability can also be defined as the probability of system's availability and is concerned with principles such as dependability, successful operation or performance [8]. Dependability is a feature of design uncertainty that depicts the probabilistic condition of a system or component. The probability that a system will operate as intended for a predetermined period of time and fulfil its intended function without experiencing any problems is known as reliability. For repairable systems, availability is a performance criterion that considers the dependability and maintainability of the system. Further, availability is expressed numerically as a probability between 0 and 1.

Phasor measurement unit is an intelligent device that acquires online real-time data in reference to synchronous frames uninterruptedly. It can be considered as a series connected device of modules as the failure of any one module will lead to the failure of the whole unit. The parameters of the module may vary due to different stress levels caused by temperature, environmental, and operational conditions during the continuous operation of PMU. Thus, there may be variations of module parameters from design values. The variation in parameters can be best studied with the help of sensitivity analysis techniques. Sensitivity studies are performance evaluations of PMU when one or more parameters vary due to any reason [2], whereas reliability predicts risk management. These studies help the design engineers and system operators in improving the design and operational efficiency. This chapter mainly focuses on (i) development of the Markov model of each module considering each sub-module as a redundant system, (ii) evaluation of reliability and sensitivity of PMU, (iii) Monte Carlo Simulation study related to reliability of GPS and PMU considering repair rate and failure rate, (iv) computation of sensitivity, w.r.t, failure rate, and repair rate for different modules and of PMU.

3.2. RELIABILITY ANALYSIS

Reliability analysis depends upon the system structure, which is the graphical depiction of components ordered according to a given design to fulfil desired functionality. The system may be (i) Series structure (ii) Parallel structure. The concept of reliability block diagrams (RBDs) is another essential concept in reliability. RBDs are graphical representations of the system that depict the various components and their reliability in a series or parallel arrangement [3]-[7]. RBDs help to analyse the dependability of complex systems and identify weak links and improvement opportunities.

3.2.1. Series Structure

A structure where the placement of the components ensures that the proper operation of each component or subsystem is necessary for the system to function sequentially. That is, the system collapses as a whole if any one of its parts fails. The reliability of a series system, as shown in Fig.3.1, is determined by the failure probability of each component in the series and can be given by eqn.(3.1)

$R_{\text{total}} = R_1 \text{ x } R_2 \text{ x } R_3 \dots \text{ x } R_n$ [8] (3.1)

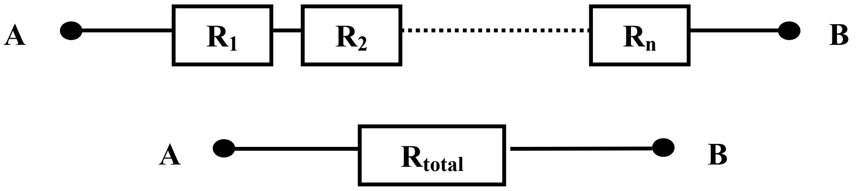


Fig. 3.1.Series Structure

Where R total is the system's overall reliability, R_1, R_2, R_3,... R_n is the reliability of the series' constituent components.

3.2.2. Parallel Structure

A structure whose components/ sub-systems are placed in such a manner that the operation of the system depends on the successful operation of any one of them or a system that fails if all of its components/sub-systems fail. Units operating in parallel are sometimes known as redundant units. Redundancy is a crucial component of system design and dependability since increasing redundancy is one of the various ways to enhance system reliability. The probability that one or more of the units fails defines the likelihood of failure or unreliability of a system with statistically independent parallel components. Therefore, for a parallel system as shown in Fig. 3.2 to fail, each unit must fail. If unit 1, unit 2 or any of the other units succeeds, then the system succeeds [8]-[12]. The reliability of a parallel system is computed based on the failure probability of each parallel component. This can be mathematically represented by the following formula as shown in eq. (3.2):

$$R_{total} = 1 - (1 - R_1) \text{ x } (1 - R_2) \text{ x } (1 - R_3) \ldots \text{ x } (1 - R_n)[8] \qquad (3.2)$$

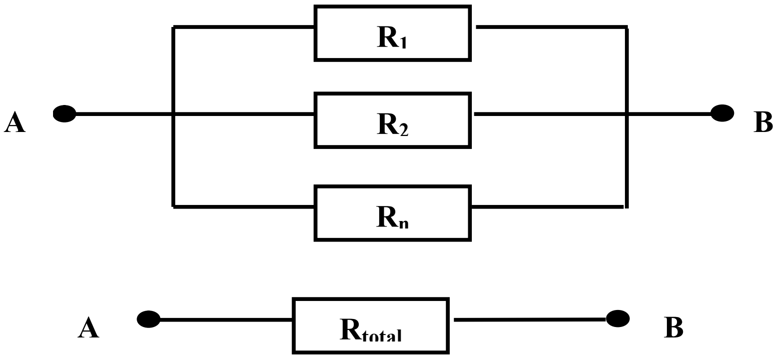


Fig. 3.2. Parallel Structure

where R_{total} is the system's overall reliability, R_1, R_2, R_3,... R_n are the reliabilities of the parallel configuration's distinct components.

Using methods such as statistical analysis, testing, and historical data analysis, it is possible to determine the dependability of each component in the parallel configuration. Once the reliability of each component is known, the above formula can be used to calculate the system's overall reliability.

3.2.2.1. Redundant Standby Structure

Redundant Standby (RS) is a system that ensures high availability and dependability. RS is implemented in a PMU system by operating two or more identical PMUs in parallel, one of which is designated as the master and the others as slaves[9]. The master PMU is responsible for processing the measured data and generating the output, while the slaves continuously monitor the master and assume control in the event of a malfunction.

The high availability and dependability of data is one of the main advantages of redundant standby in PMU systems. As PMUs are essential for the control and safeguarding of the power grid in real-time, any disruption in the measurement of data can have severe consequences. Even in the event of a failure, the RS architecture guarantees that the PMU data is always accessible and accurate. Additionally, It facilitates maintenance and repair. Due to the parallel operation of redundant modules of PMUs, the system can continue to function even when one of PMU module is unavailable for maintenance or repair. This reduces the system's outage and maintenance costs and may be utilized in several ways. Further there is a clear distiction between parallel and standby redundancy. In parallel redundancy, redundant units are integral components of the system from the beginning. Redundant Standby architecture can be implemented in the hardware, software, and network layers of the PMU system. On the hardware level, redundant power supplies and redundant communication interfaces can be implemented to ensure that the PMUs continue to function even in the event of a failure[10]-[15]. At the software level, fault-tolerant algorithm can be used to detect and recover from software errors, while redundant communication links and protocols can be used at the network layer to ensure transmission in the event of a network failure.The standby unit can be classified in following manner:

➢ Cold Standby Unit: A Cold Standby unit is a backup system that is maintained in a non-operational or "cold" state until the primary system fails and is required to take over[16]-[18]. This procedure may take some time to complete because the standby system must be powered on, initialized, and activated. During this period, there may be a transient interruption of service, which can be minimized by expediting the activation procedure.

One of the primary benefits of a Cold Standby Unit is that it is less expensive than a hot standby system. Since the standby device is inactive for the majority of the time. This makes the Cold Standby Unit an economic backup and recovery solution for applications where delay is not critical. The time required to activate the standby system is a major concern. This can result in a transient interruption of service, which in some cases may not be acceptable. In addition, the Cold Standby Unit must be routinely tested and maintained to ensure that it is functional when required.

➢ Hot Standby unit: A Hot Standby, also known as hot backup or active standby, is a form of standby system that is always fully operational and prepared to assume control of the primary system in the event of a failure[19]-[22]. This form of standby system is typically employed in situations where high availability and zero downtime are essential. In a Hot Standby configuration, both the primary and standby units are completely operational and processing data concurrently. The primary system handles the normal workload, while the standby system continuously monitors the primary system for any signs of failure or degradation. In the event that the primary system fails, the standby system takes over the burden immediately and seamlessly.

High availability and quick recovery time are two of the primary benefits of a Hot Standby configuration. Since the standby system is always completely operational and processing data in real time, there is no need for an initialization or activation procedure during a failover. There are, however, some drawbacks to a hot standby configuration. The expense of redundant hardware and software components required to maintain the continuous operation of both systems is one of the primary concerns. This may be costly, particularly for large-scale systems. Another concern is the possibility of data loss or corruption if the primary system fails before data replication to the standby system is complete [23]-[26]. It necessitates redundant hardware and software components and can be costly to implement and maintain.

3.3. RELIABILITY INDICES

Quantitative measures that can be applied to the evaluation of a system's or component's degree of dependability are known as reliability indices. There are several reliability indices that can be computed in order to assess the performance of a system [30] some of these indices are as follows:

- Failure Rate (Failure Rate): The failure rate is the rate at which it is anticipated that a component or system will fail over a given period of time. The standard units of its measurement are failures per hour, failures per million hours, or failures per billion hours. Eqn.(3.3)[8] can be used to calculate the percentage of attempts that were unsuccessful.

$$\text{Failure Rate} = \frac{\text{No.of Malfunction}}{\text{Total operating time}} \tag{3.3}$$

- Mean Time Between Failures (MTBF): It refers to the amount of time, on average, that passes between two failures of a system or component in quick succession. Typically, it is measured in hours, and the following formula shown in eqn. (3.4) [8]can be used to determine how much time has passed.

$$\text{MTBF} = \frac{\text{Total operating time}}{\text{No.of breakdowns}} \tag{3.4}$$

- Availability (A): Availability is the percentage of time that a system or component is operational and available for usage. Availability measures the amount of time when a system or component is available. Eqn.(3.5) [8]can be used to calculate the availability

$$\text{A} = \frac{[(\text{Total operating time} - \text{Total downtime}) \text{ x } 100]}{\text{Total Operating Time}} \tag{3.5}$$

- Mean Time To Repair: It is abbreviated as MTTR. This is defined as the amount of time it takes, on an average, to fix a malfunctioning component or system. Typically, it is measured in hours. The formula is shown in eqn. (3.6)[8].

$$\text{MTTR} = \frac{\text{Total downtime}}{\text{Number of breakdowns}} \tag{3.6}$$

- Probability of Failure on Demand (PFD): It is the probability that a component or system will fail when it is called upon to perform the function for which it was designed. It is most commonly expressed as a decimal number between 0 and 1. PFD can be calculated by using eqn. (3.7)[8]

$$\text{PFD} = \frac{\text{No.Of Failures}}{\text{Total demand}} \tag{3.7}$$

These are just a few reliability indices that may be generated in order to assess the performance of a system or component. The values of failure rates and repair rates of CT/PT, filter, ADC, GPS receiver, CPU, and power supplies are considered as given by the manufacturer or are estimated using various methods.

The subsequent section presents the development of the reliability models of PMU for the computation of characterization indices.

3.4. RELIABILITY COMPUTATION METHODS

There are many methods for the computation of system reliability. However, in this work some important methods that are used for the simulation study of the system in reference to time/frequency are presented. In this section dynamic logic model of all the five modules of PMU is developed. Further Markov and Monte Carlo reliability models are developed for reliability analysis.

3.4.1. Dynamic Logic Model of PMU

The phasor measurement unit captures the power system data (voltage, current, circuit breaker status, etc.) continuously in a dynamic mode. These power system data are used for further operation and control of the power system as well as stability evaluation. The sub-modules of PMU are functioning continuously and are defined by their failure and repair rate, respectively. In this chapter, the Markov model is used for evaluating reliability as it can capture many important features of reliability concern to PMU modules. Therefore, in the present study, the Dynamic failure model and Markov reliability method are discussed and implemented for computing the reliability indices of PMU.

3.4.1.1 Failure model of Data Acquisition module

Module-1 is the Data Acquisition System (DAS) and its sub modules are (i) a Hall Effect transducer, which converts the voltage and current signal from PT and CT into small signals that are compatible with a PCB circuit; (ii) an Anti-aliasing filter, which gets rid off high-frequency noise (iii) an ADC converter, which changes analog signal into digital signal. Each of these three sub-modules has a stand-by mode function, and they are coupled to one another in series. The ADC sub module needs a high frequency refrences pulse in order to begin the conversion of an

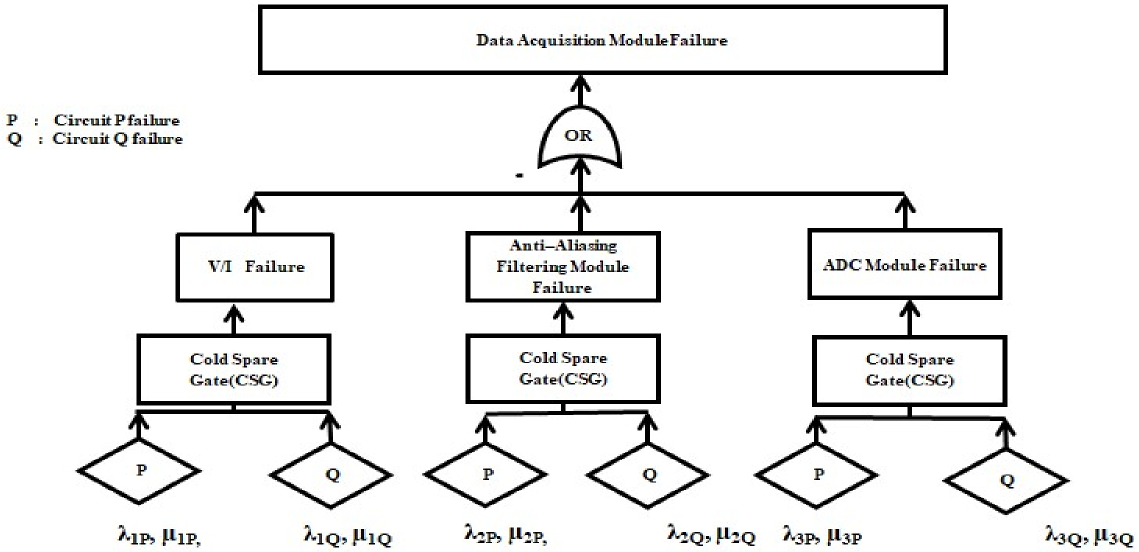


Fig. 3.3: Failure model of Data Acquisition Module (λ- Failure rate, μ- Repair rate)

analog signal to a digital one. This pulse comes from GPS. On display in Fig. 3.3 is a failure model diagram for the Data Acquisition system module that makes use of binary logic gates.

3.4.1.2.Failure model of the CPU module

Module-2 is the central processing unit (CPU), which has sub modules as (i) software and (ii) hardware. While the rate of failure for central processing units (CPUs) used in military handbook is extremely low, the rate of failure for commercial CPUs is satisfactory. It is suggested that even while utilizing a commercial CPU, a stand-by CPU is needed. In comparison to the reliability of hardware, the dependability of software is relatively good; hence, it is sufficient to address the reliability of hardware when designing a system for commercial application. The failure model diagram of the CPU module is shown in Fig. 3.4, which uses binary logic gates.

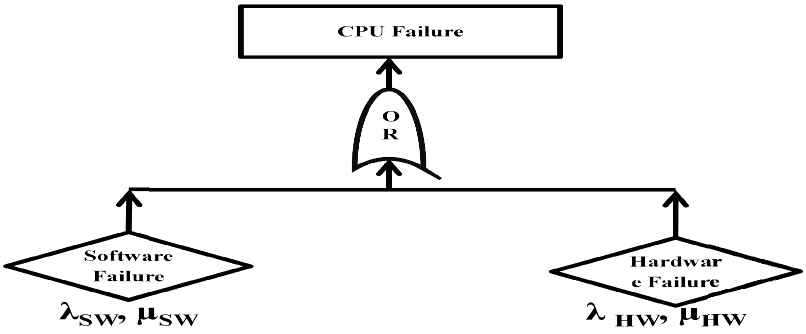


Fig.3.4: Failure Model of CPU

3.4.1.3.Failure model of MODEM and Power supply module

Phasor measurement units are essential components of today's contemporary electric power grid because of synchronized high-speed measurements of voltage and current phasors. The modem and power supply module of a PMU are used to facilitate data connection and the delivery of power to the system, respectively. Failures that may occur in the modem module of a PMU include the following:

- ➢ Connectivity problems on the network. The modem may be unable to establish a connection to the network or may drop the connection often, both of which can result in broken or poor communication.
- ➢ Errors during data transmission: It is possible for the modem to have faults while it is transmitting data, which can result in the data being garbled or lost.
- ➢ Failures in the modem's hardware: There is a possibility that the modem will become inoperable as a result of hardware problems. These failures could include a faulty antenna or a malfunctioning transmitter.

Failures that may occur in the power supply module of a PMU include the following:

- ➢ It is possible that the power supply module may develop high or low voltage, either of which could result in damage or a malfunctioning of PMU.
- ➢ The power supply module may deliver an excessive amount of current or may encounter a short-circuit, both of which could cause harm to the PMU or to the power supply module itself.
- ➢ The power supply module has a risk of overheating if there is insufficient cooling or if the ambient temperature is excessive. This may result in damage or failure of the module.

It is vital to monitor and maintain the MODEM and power supply modules in a PMU in order to guarantee that the device will function in an accurate and dependable manner. Frequent inspection and upkeep of the PMU can help to reduce the likelihood of problems occurring and ensure that it continues to perform as expected. Module-4 (MODEM) provides a communication link that can be used to interact with and upload power system data that has been captured to the cloud, the web, or any other communication channel. In order to improve the system's availability, it is necessary for this module to remain in the standby mode. Also every single module that makes up PMU makes use of the active components. In order to carry out smooth functional operation these components require stimulation. Thus, having a reliable source of power supply is an essential prerequisite for the effective operation of the PMU. In this section the dual power supply is focused while it was in standby mode. Hence, the Dynamic Models of the communication and power supply modules are comparable, as shown in Fig. 3.5 (a) and (b), respectively.

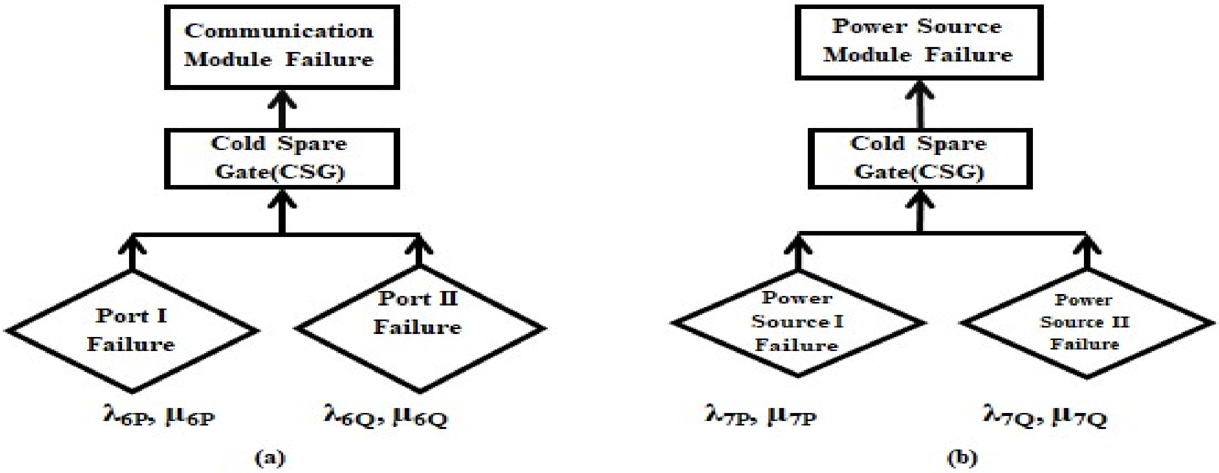


Fig.3.5: Failure models of (a) Communication Module (b) Power Supply Unit.

3.4.1.4.Failure model of GPS module

GPS is one of the critical components of PMU. It has two functions:

(i) Provide the sampling pulse to the ADC and

(ii) Generate time stamping on the acquired data.

In the event of failure of GPS, which provides a pulse of 1PPM from the satellite to the crystal oscillator, ensures the accuracy of a maximum 1% for 26 hrs [28]. If the pulse from the GPS system is not available, a dynamic intelligence switch shifts the crystal oscillator into stand-by mode. Fig. 3.6 shows the failure model diagram using binary logic gates of GPS module- 2.

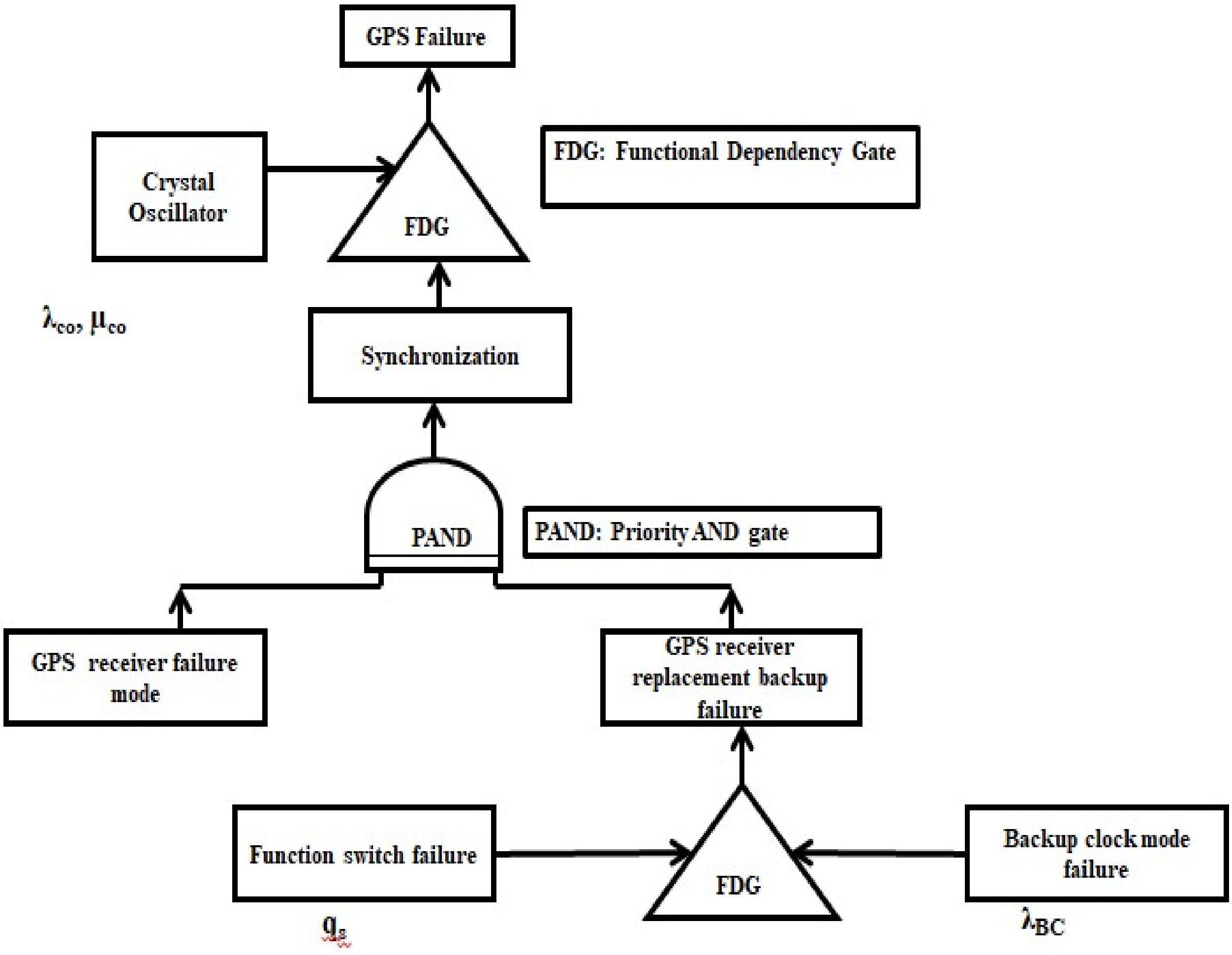

GPS Failure
Crystal Oscillator
FDG
FDG: Functional Dependency Gate
λ_{co}, μ_{co}
Synchronization
PAND
PAND: Priority AND gate
GPS receiver failure mode
GPS receiver replacement backup failure
Function switch failure
FDG
Backup clock mode failure
q_s
λ_{BC}

Fig.3.6: Failure model of GPS

3.4.1.5 Failure model of Complete PMU

The failure of any of the five modules of PMU causes its complete shuts down. Thus, each module set forms a series circuit. Fig. 3.7 shows the failure model diagram using binary logic OR gates of complete PMU.

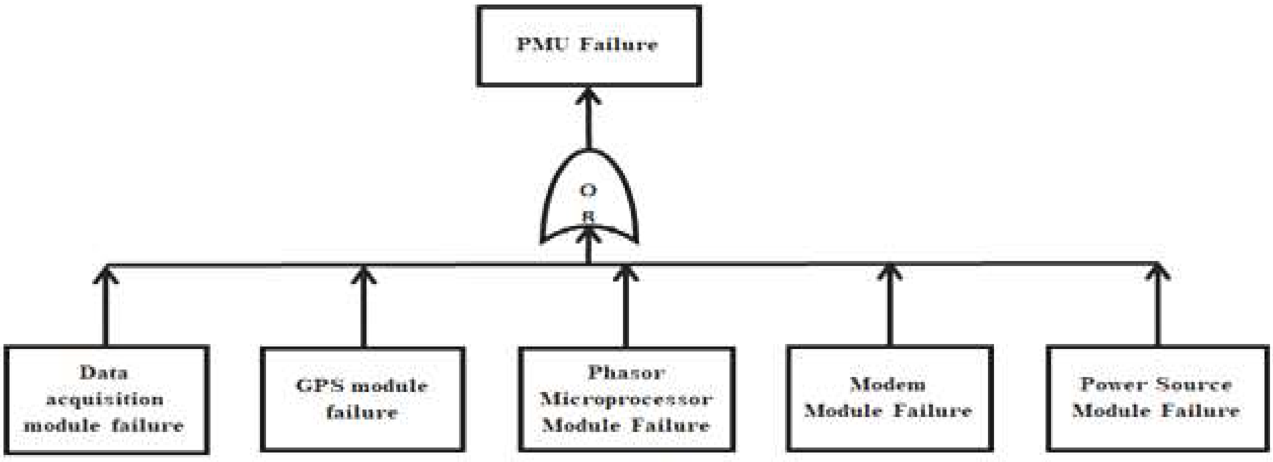

PMU Failure
O
R
Data acquisition module failure
GPS module failure
Phasor Microprocessor Module Failure
Modem Module Failure
Power Source Module Failure

Fig.3.7: Failure model of PMU

3.4.2 **Monte Carlo model**

The Monte Carlo model is a probabilistic model used to estimate the reliability of complex systems. This model is based on the Monte Carlo simulation, which is a method for generating random numbers and using them to simulate different outcomes of a system. In the Monte Carlo model of reliability, a system is represented as a series of interconnected components or subsystems, each of which has a probability of failure. The model uses random numbers to simulate the behavior of the system over time, taking into account the probability of failure of each component and the interactions between them. One advantage of the Monte Carlo model is that it can take into account a wide range of factors that may affect the reliability of the system, such as variations in operating conditions, environmental factors, and the effects of maintenance and repair activities. This makes it a useful tool for predicting the reliability of systems in real-world applications. However, the Monte Carlo model also has some limitations. It requires a large number of simulations to obtain accurate results, which can be computationally intensive and time-consuming. In addition, the accuracy of the results depends on the quality of the input data, such as the reliability data for individual components and the assumptions about the interactions between them. Despite its limitations, the Monte Carlo model is a powerful tool for predicting the reliability of complex systems.

The Monte Carlo model for PMUs simulates the efficiency of PMUs under various operating conditions and input parameters. This permits the evaluation of the PMU's dependability and the identification of potential failure modes.

Simulation is the process to estimate the reliability of the PMU by simulating the failure and repair rate of random behaviour of the system.Thus, it is similar to series of real time experiments performed in simulated time[28]. When the PMU is simulated, the occurrence of events depends upon their failure and repair rates and probability distribution function. This is achieved using random numbers and converting these into density functions. The various steps involved are:

(i) Generate Random numbers.

(ii) Using the Algorithm X_{i+1} = (AX_i +C) (modB) where A, B, and C are non negative intergers where A is a multiplier, B is the modulus and C is the incremental.modulus(B) is the maximum permissible value and the calculated random number should not exceed it.

(iii) After generating the sequences of random numbers X_i ,uniform random number(U_i) in range(0,1) can be given by $U_i = \frac{X_i}{B}$.

(iv) Convert this random number into mission time (T) using eqn. $T= -\frac{1}{\lambda}$ lnU; where λ is the failure rate.If this time is more than or equal to calculated mission time (depending on the value of λ) then events is success otherwise failure.

(v) Repeat step 1 to 3 for the desired number of simulations.

(vi) Simulation study depends on the random number generator and the number of simulations.

The simulated results of reliability for GPS and PMU systems are presented in Fig. 3.8 and 3.9, respectively. From these graphs it is noted that the reliability of GPS is 0.9999 and that of PMU is 0.8875. It may be noted that initially at t= 0 the reliability graph starts from unity (as per eqn.3.28) and it oscillates according to random number generated as the mission time (in days) increases.

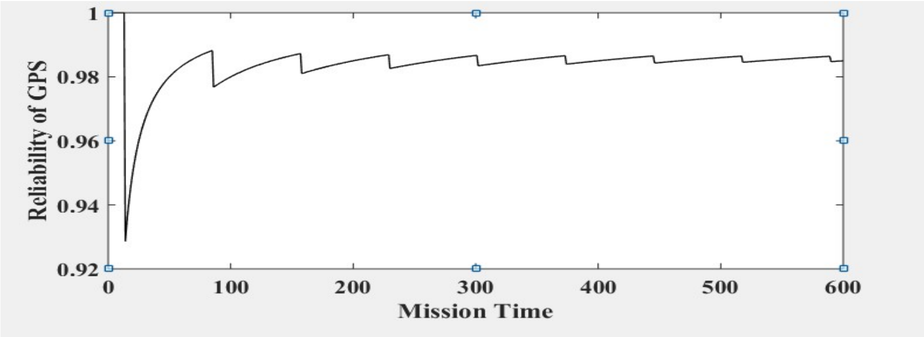


Fig.3.8: Simulation result for Reliability of GPS

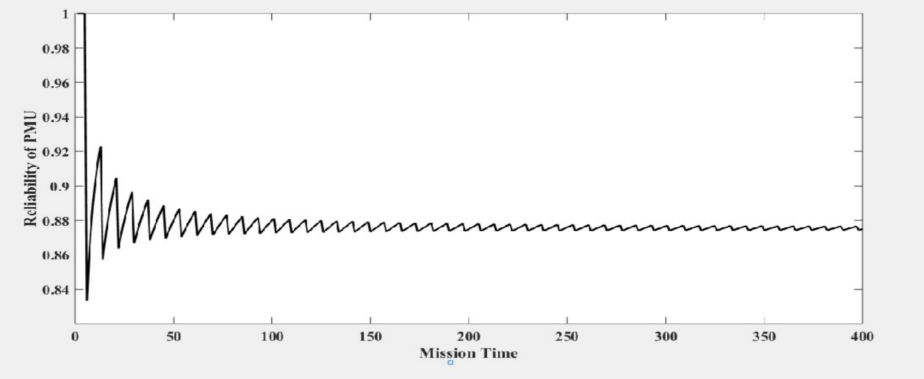


Fig.3.9: Simulation result for Reliability of PMU

3.4.3 Markov Reliability Model

The Markov reliability model is a mathematical model based on the Markov process, which is a mathematical framework used to model systems that change with time.

It represents a set of states, and the probability of transitioning from one state to another. The states represent the different possible conditions of the system, such as operating normally, experiencing a failure, or being repaired. The transition probabilities represent the likelihood of the system moving from one state to another and are often determined by historical data or by expert opinion. Markov's model for PMUs includes a collection of states, transition probabilities, and assumptions. The states represent the various operational phases of the PMU, including normal operation, partial failure, and total failure. The Markov model for PMUs is based on the assumptions of stationary and independent transitions [30]. This indicates that the probability of transitioning from one state to another remains constant and is unaffected by preceding transitions. By simulating the behavior of the PMU over time, the Markov model can identify potential failure modes and contribute to improve the system's reliability. One limitation of the Markov reliability model is that it assumes that the system is in a steady state, meaning that the probabilities of transitioning from one state to another are constant over time. This may not always be the case in real-world systems, where the probabilities may change due to external factors such as changes in the environment or changes in usage patterns. Despite its limitations, the Markov reliability model is a useful tool for analyzing and predicting the reliability of a system, and it is widely used in industries such as aerospace, defense, and telecommunications.

3.4.3.1 Markov Model of Data Acquisition System

The structure design of Data Acquisition System (DAS) with its sub modules (1), Anti-Alias filter (2) ADC (3) CT/PT is similar to two networks connected in parallel series. Each of them is connected in series and forms three phase voltage /current circuits. Data Acquisition module fails if any of the three sub module circuits fails. Thus, a two-state Markov model for sub-modules (1), (2) and (3) is combined using series parallel network theories. In a parallel stand-by system, if λ_1 and λ_2 are failure rate of main and stand- by modules, and r_1 and r_2 are their repair times ($r=1/\mu$), then

$$\lambda_{\text{parallel}} = \frac{\lambda_1\lambda_2(r_1+r_2)}{1+\lambda_1 r_1+\lambda_2 r_2};\ r_{\text{parallel}} = \frac{r_1 r_2}{r_1+r_2}\ ;\ U_{\text{parallel}} = \lambda_1\,\lambda_2\,\mu_1\mu_2 \tag{3.8}$$

$$\lambda_{\text{series}} = \sum_{i=1}^{n}\lambda_i;\ r_{\text{series}} = \frac{\sum_{i=1}^{n} r_i\lambda_i}{\sum_{i=1}^{n}\lambda_i};\ U_{\text{series}} = \sum_{i=1}^{n} r_i\lambda_i \tag{3.9}$$

3.4.3.2 Markov Model of CPU

The CPU comprises of sub-modules hardware and software. Failure of either component makes the CPU unavailable. Hardware and software can be considered as series components. If the failure rate and repair rate of hardware and software are λ_{CPU} and μ_{CPU} then,

$$\lambda_{CPU} = \lambda sw + \lambda_{Hw}\ ;\ \mu_{CPU} = \frac{\lambda sw\ \mu sw\ \mu Hw + \lambda Hw \mu sw\ \mu Hw}{\lambda sw\ \mu Hw + \lambda Hw\ \mu sw} \tag{3.10}$$

$$\text{Reliability of CPU } (R_{CPU}) = e_{CPU}^{-\lambda t} \tag{3.11}$$

$$\text{Reliability of stand-by CPU system } R_{(CPUstand\text{-}by)} = \{e^{-\lambda tcpu}\}\{1+\lambda t_{CPU}\} \tag{3.12}$$

The availability (A) and unavailability (U) of CPU is given by following equations.

$$A = \frac{\mu_{CPU}}{\lambda_{CPU}+\mu_{CPU}} \text{ and } U = \frac{\lambda_{CPU}}{\lambda_{CPU}+\mu_{CPU}} \tag{3.13}$$

3.4.3.3 Markov Model of GPS

GPS is one of the complex modules of PMU. The Markov model state space diagram of the GPS system is presented in Fig. 3.10 Here λ_T is taken as the transition rate at which the functional failure of crystal oscillator occurs. It is computed using the reciprocal of average duration required to reach the maximum cumulative time error whereas λ_{BC} is failure rate from functional failure to complete failure of the crystal oscillator. The transition rate is the repair rate (μ_{GC}) which is considered when both GPS receiver and crystal oscillator fails to when both are working and is given by eqn. (3.14).

$$\mu_{GC} = \mu_{GPS/CO} = \frac{1}{\mu_{GPS}} + \frac{1}{\mu_{CO}} \tag{3.14}$$

Fig. 3.10 represents the state space diagram for the GPS module. Here, sub-script 'f', ff and 'w' represent the failure, functional failure and working states, respectively.

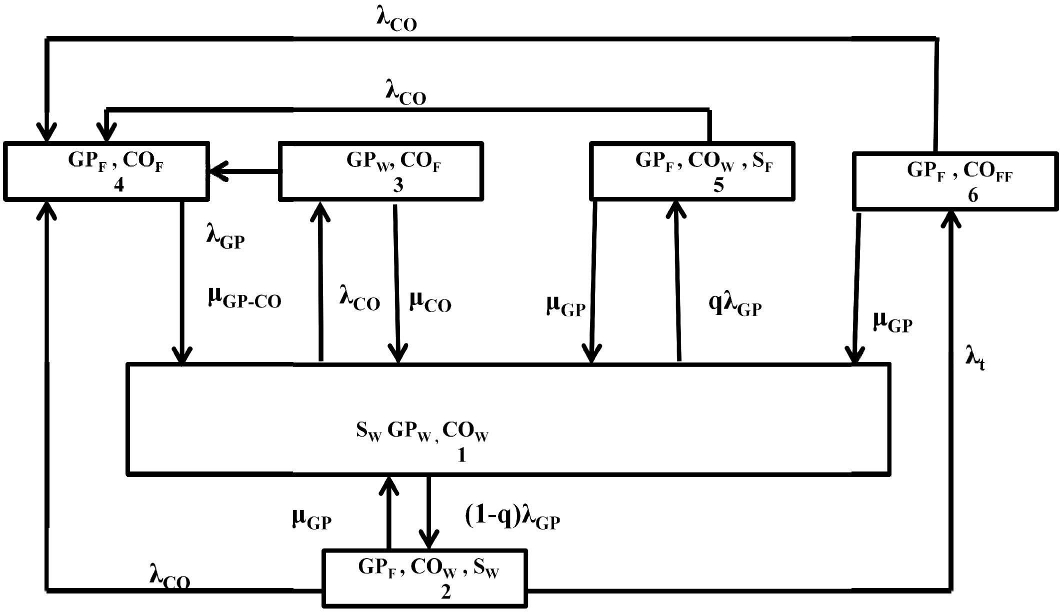


Fig.3.10: State Space Diagram for GPS Module

The state space Markov model can be written as shown in eqn.(3.31).

$$T=\begin{bmatrix} 1-(\lambda_{GP}+\lambda_{co}) & (1-q_S)\lambda_{GP} & \lambda_{CO} & 0 & q_S\lambda_{GP} & 0 \\ \mu_{GP} & 1-(\lambda_T+\lambda_{CR}+\mu_{GP}) & 0 & \lambda_{co} & 0 & \lambda_T \\ \mu_{CO} & 0 & 1-(\lambda_{GP}+\mu_{CO}) & \lambda_{GP} & 0 & 0 \\ \mu_{GC} & 0 & 0 & 1-\mu_{GP,CO} & 0 & 0 \\ \mu_{GP} & 0 & 0 & \lambda_{co} & 1-(\lambda_{co}+\mu_{GP}) & 0 \\ \mu_{GP} & 0 & 0 & \lambda_{BC} & 0 & 1-(\lambda_{BC}+\mu_{GP}) \end{bmatrix} \tag{3.15}$$

Each state limit probability can be computed by eqn. β.T = β (3.16)

Where β = [$P_1P_2P_3P_4P_5P_6$]. The matrix [T] has a rank of 5, thus an additional eqn. (3.17) used to compute P_i is

$$\sum_{i=1}^{6} \mathrm{Pi} = 1 \tag{3.17}$$

The eqns. (3.18) is used to compute the availability and unavailability of GPS module.

$$\text{Availability}_{\text{GPS}} = P_1+P_2,\ \text{Unavailability}_{\text{GPS}} = P_3+P_4+P_5+P_6 \tag{3.18}$$

The equivalent failure rate (λ_{M5}), equivalent repair time (r_{M5}) can be computed using the following equations:

$$\lambda_{M5} = [P_1(q_s\lambda_A+ \lambda_B) + P_2(\lambda_T+ \lambda_B)] / (P_1+P_2) \tag{3.19}$$

$$r_{M5} = [P_3+P_4+P_5+P_6] / [P_1(q_s\lambda_A+ \lambda_B) + P_2(\lambda_T+ \lambda_B)] \tag{3.20}$$

3.4.3.4 Markov Model of Communication and Power Supply Modules

Communication and power supply modules are considered as redundant system (failure rate and repair time of main and stand by system is consider same). Thus, the eqns. (3.21) – (3.30) are applicable for computing the reliability of the complete system. Fig. 3.11 and Fig. 3.12 represent the physical and state space of the two components stand-by system.

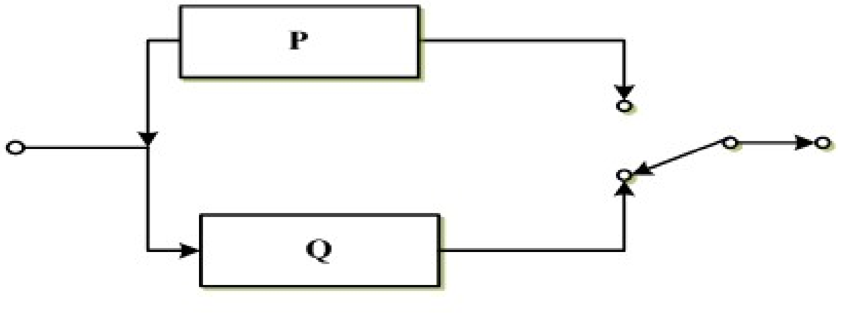


Fig.3.11: A Two Components Stand - by System

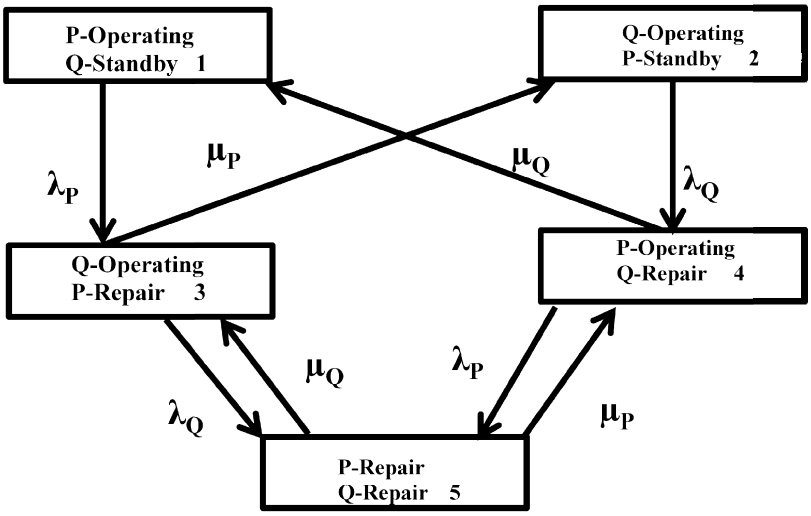


Fig.3.12: State Space for Two Components Stand - by System

3.4.3.5 Markov Model of Complete PMU

The state space model of each module of PMU can be shown by the two-state model of the Markov dynamic state model. This takes into account the probabilistic function of failure rate and repair rate for the computations of reliability indices, incorporating the formation of the Markov state space model. The state space diagram of stand- by redundant system is shown in Fig. 3.13 and its graphical model in Fig. 3.14 below. Let λ_1 and λ_2 represent the failure rate and μ_1, and μ_1 are the repair rate of the main and stand-by system, respectively. The subscript o, f, and s represent the operating mode, failure mode and stand- by mode, respectively. It is assumed that in redundant system whenever system P is operable it will replace Q as operating component. However, it depends on operating policy consideration.

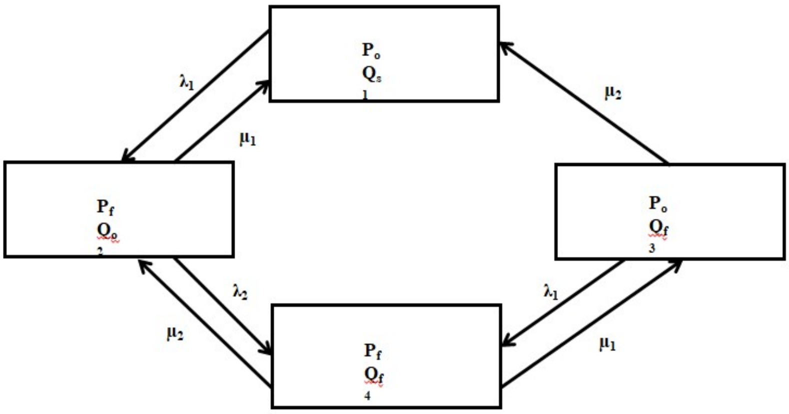


Fig.3.13: State Space Diagram for Stand-by Redundant System

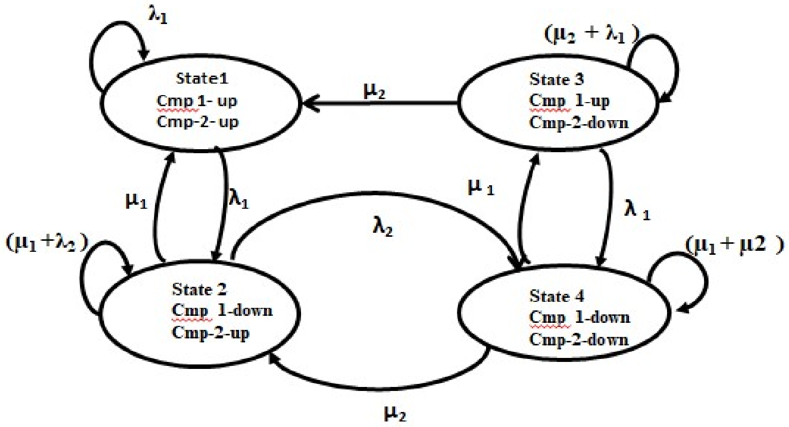


Fig.3.14: Markov Graphical model of PMU

The transitional probability matrix (P) for Markov state space model as shown in Fig. 3.14 is given by eqn.(3.21).

$$\mathbf{P} = \begin{bmatrix} 1-\lambda_1 & \lambda_1 & 0 & 0 \\ \mu_1 & 1-(\lambda_2+\mu_1) & 0 & \lambda_2 \\ \mu_2 & 0 & 1-(\lambda 1+\mu_2) & \lambda_1 \\ 0 & \mu_2 & \mu_1 & 1-(\mu_1+\mu_2) \end{bmatrix} \tag{3.21}$$

The limiting state probability vector, α, doesn't change when multiplied by the stochastic transitional probability matrix, therefore, the following eqn. (3.22) holds:

$$\alpha=\alpha P \tag{3.22}$$

Here, α is given by the vector [P_0 P_1 P_2 P_3], and P is a 4x4 matrix. As per the frequency encounter of state , frequency balance eqn. (3.23) and (3.24) can be written as below:

$$P_0\lambda_1=P_1\mu_1+P_2\mu_2;\ P_1(\lambda_2+\mu_1)=P_0\lambda_1+P_4\mu_2 \tag{3.23}$$

$$P_2(\lambda_1+\mu_2)=P_4\mu_1;P_3(\mu_1+\mu_2)=P_2\lambda_1+P_1\lambda_2 \tag{3.24}$$

The matrix [P] has a rank of 3, thus additional eqn. (3.25) used to compute state probability.

$$P_0+P_1+P_2+P_3=1 \tag{3.25}$$

Thus, the value of P_0 to P_3 is computed, and the following expressions are obtained.

$$P_0=\frac{[\{(\lambda_1+\mu_2)(\mu_1+\mu_2)-\lambda_1\mu_1)\mu_1+\mu_1\mu_2\lambda_2\ )\}/(\mu_1\lambda_1\ \lambda_2\ )]}{\mu_1\mu_2(\mu_1+\mu_2+2\lambda_1\ )+\lambda_1\ \lambda_2\ (1+\mu_2)+\lambda_1\ \mu_2(\lambda_1\ +\mu_2)} \tag{3.26}$$

$$P_1=\frac{(\mu_1+\lambda_1\ +\mu_2)\mu_2}{\mu_1\mu_2(\mu_1+\mu_2+2\lambda_1\ )+\lambda_2\ \lambda_1\ (1+\mu_2)+\lambda_1\ \mu_2(\lambda_1\ +\mu_2)} \tag{3.27}$$

$$P_2=\frac{(\lambda_1+\mu_1)\lambda_1\ \lambda_2}{(\ \mu_1\mu_2(\mu_1+\mu_2+2\lambda_1\ )+\lambda_1\ \lambda_2\ (1+\mu_2)+\lambda_1\ \mu_2(\lambda_1\ +\mu_2)} \tag{3.28}$$

$$P_3=\frac{\mu_1\lambda_2\ \lambda_1}{(\ \mu_1\mu_2(\mu_1+\mu_2+2\lambda_1\ )+\lambda_1\ \lambda_2\ (1+\mu_2)+\lambda_1\ \mu_2(\lambda_1\ +\mu_2)} \tag{3.29}$$

now, Availability A = $P_0+P_1+P_2$ and Unavailability, U=P_3 (3.30)

and Reliability of stand-by system is given by eqn.(3.31)

$$R(t)=\{e^{-(\lambda t)}\}(1+\lambda t) \tag{3.31}$$

The parallel redundant circuit module of PMU can be represented by a state space diagram as shown in Fig. 3.15 and Markov graphical models for parallel redundant systems are shown in Fig. 3.16.For cold stand- by system, let λ_1, and λ_2 represent the failure rate and μ_1, and μ_2 are the repair rate of two parallel redundant circuit modules. If P_0, P_1, P_2, and P_3 are probability of four states, then Availability (A) = P_0+P_1 +P_2, and Unavailability(U) = P_3

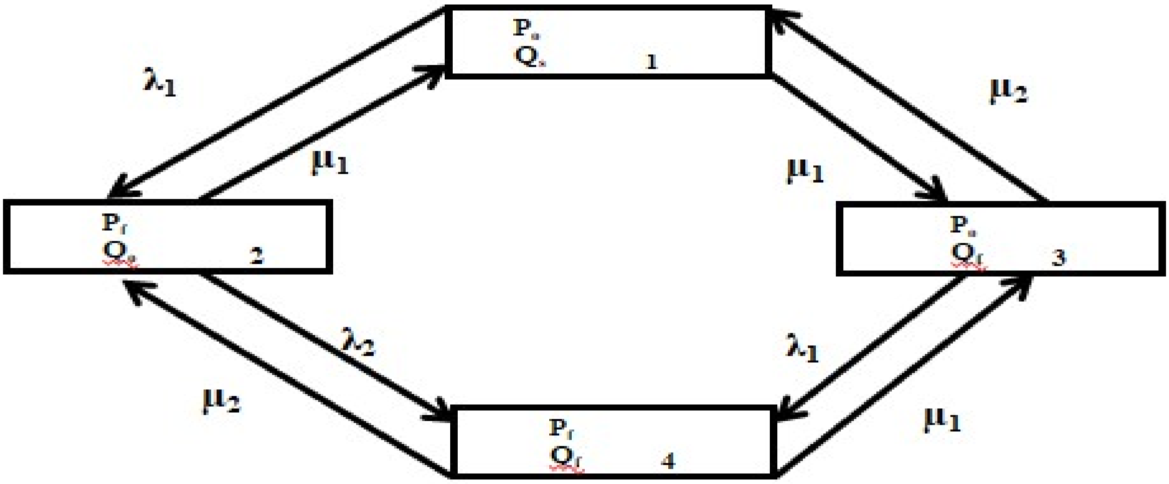


Fig.3.15: State Space for Parallel Redundant System

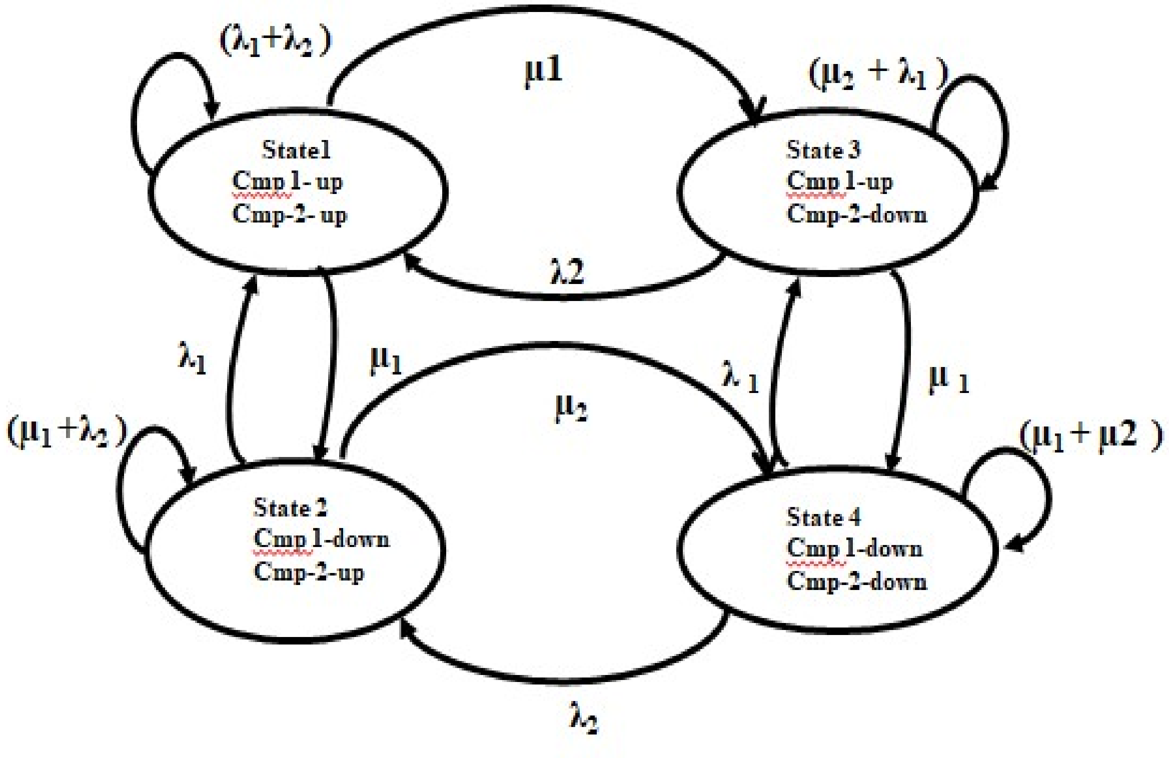


Fig.3.16: Markov model for Parallel Redundant System

The P_0, P_1, P_2, and P_3 are computed using limited state equation {α=αP}, and

$P_0+P_1+P_2+P_3 = 1$. The following probability relations are obtained.

$$P_0 = \frac{\mu_1\mu_2}{(\lambda_1+\mu_1)((\lambda_2+\mu_2)}; \qquad P_1 = \frac{\lambda 1\mu 2}{(\lambda_1+\mu_1)((\lambda_2+\mu_2)} \tag{3.32}$$

$$P_2 = \frac{\lambda_2\mu_1}{(\lambda_1+\mu_1)((\lambda_2+\mu_2)} ;P_3 = \frac{\lambda_1\lambda_2}{(\lambda_1+\mu_1)((\lambda_2+\mu_2)} \tag{3.33}$$

If $\lambda_1 = \lambda_2 = \lambda$, and $\mu_1 = \mu_2 = \mu$, then

$$P_0 = \frac{\mu^2}{(\lambda+\mu)^2} ;P_1 = \frac{\lambda\mu}{(\lambda+\mu)^2} ;P_2 = \frac{\lambda\mu}{(\lambda+\mu)^2} ; \quad P_3 = \frac{\lambda^2}{(\lambda+\mu)^2} \tag{3.34}$$

$$MTBF = \frac{3\lambda+\mu}{2\lambda}; \qquad MTTR = \frac{1}{2\mu} \tag{3.35}$$

Table 3.1: Reliability indices values usingMarkov Model

Modules	Availability	Unavailability	MTBF	MTTR	Reliability
Transducer	0.99838	$3.7912\text{x } 10^{-7}$	$1.955\text{x}10^{3}$	6.4913	0.93424
Anti-alias filter	0.99998	$1.232\text{x } 10^{-7}$	$1.4813\text{x}10^{3}$	8	0.983718
A/D convertor	1	$9.9637\text{x}10^{-8}$	$1.1476\text{x}10^{4}$	10	0.991274
CPU	0.99902	0.00097461	2.34711	27.2812	0.99245
GPS	0.999306	$6.932 \text{ x}10^{-4}$	4.22	24	0.976008
MODEM	0.99999	1.693610^{-12}	$1.6851\text{x}10^{-7}$	25	0.99974
Power supply	0.999246	$5.47206 \text{ x}10^{-7}$	$2.416 \text{ x}10^{-3}$	12	0.968433
PMU	0.998332	0.001668	1.6521	26.15	0.85388

3.4.3.6 Numerical Evaluation of Reliability Indices using Markov model for PMU

In order to show the utility of Markov model developed for PMU in Section 3.4.3, the failure rate and repair time of five modules present in Appendix –A are used. The reliability indices of modules and complete PMU are computed using the eqns. developed. The Table-3.1 shows the computed values of reliability indices.

3.5 COMPARATIVE ANALYSIS OF MONTE CARLO MODEL AND MARKOV MODEL OF RELIABILITY

The Monte Carlo model of reliability and the Markov model of reliability are two widely used methods in reliability engineering for predicting the reliability of a system. While both models use probabilistic methods to estimate the reliability of a system, they differ in several ways.

- Representation of the system: The Monte Carlo model represents a system as a series of interconnected components or subsystems, while the Markov model represents a system as a set of states.
- Calculation of reliability: In the Monte Carlo model, the reliability of a system is calculated by simulating the behavior of the system over the time, taking into account the probability of failure of each component and the interactions between them. In the Markov model, the reliability of a system is calculated by analyzing the probabilities of transitioning from one state to another over time.
- Computation time: The Monte Carlo model requires a large number of simulations to obtain accurate results, which can be intensive and time-consuming. The Markov model, on the other hand, can provide results more quickly, as it does not require simulating the behavior of the system over time.
- Accuracy of results: The accuracy of the Monte Carlo model depends on the quality of the input data, such as the reliability data for individual components and the assumptions about the interactions between them. The Markov model is based on assumptions about the behavior of the system, which may not always hold true in real-world situations.
- Applicability of complex systems: The Monte Carlo model is particularly useful for analyzing complex systems with many components or subsystems, where it may be difficult or

impossible to analyze the system using traditional analytical methods. The Markov model is more suitable for systems with a small number of states.

In summary, the Monte Carlo model is a powerful tool for predicting the reliability of complex systems, while the Markov model is more suitable for simpler systems. Both models have their advantages and limitations, and the choice of which model to use depends on the specific characteristics of the system being analyzed and the objectives of the analysis.

3.6 Timing representation of Operating Cycles of Stand-by module

In order to show the timing diagram of a redundant system, two components having ideal switch is considered .The time diagram of the system under consideration is shown in Fig. 3.17. Here, it is assumed that the redundant/ stand-by module is available in case the main module fails. Thus, the system cycle time (T) = MTTF (mean time to failure) + MTTR (mean time to repair). Practically the time to repair the module is quite small in comparison to the operating time of the system. This results in the meantime to failure = mean time between failure. The following relation can, thus, be defined as:

Time to failure (TTF) $= \frac{1}{FailureRate\ (\lambda)}$; Time to repair(TTR) $= \frac{1}{RepairRate(\mu)}$;

Time between failures (TBF) = TTF+TTR $= \frac{1}{frequencyofdutycycle(f)}$ (3.36)

The cycle time between individual states in case of two module system is given by eqn. (3.37)

$T_1 = \frac{(\lambda+\mu)^2}{2\lambda\mu^2}$; $T_2 = T3 = \frac{\lambda+\mu}{\lambda\mu}$; $T4 = \frac{(\lambda+\mu)^2}{2\mu\lambda^2}$ (3.37)

The duration indices and frequency encountering state $f(s)$ for individual states can be calculated using eqn. (3.38)

$f(s) = P(s)\ \lambda_d(s) = \overline{P}(\bar{s})\ \lambda_e(s)$ (3.38)

where P(s) = state probability; $\overline{P}(\bar{s})$ = out of state probability.

$\lambda_d(s)$ = departure rate from state; $\lambda_e(s)$ = entry rate into the state.

Thus, from mode(1 to 4) frequency of encounters of the individual state can be computed as per Table-3.2

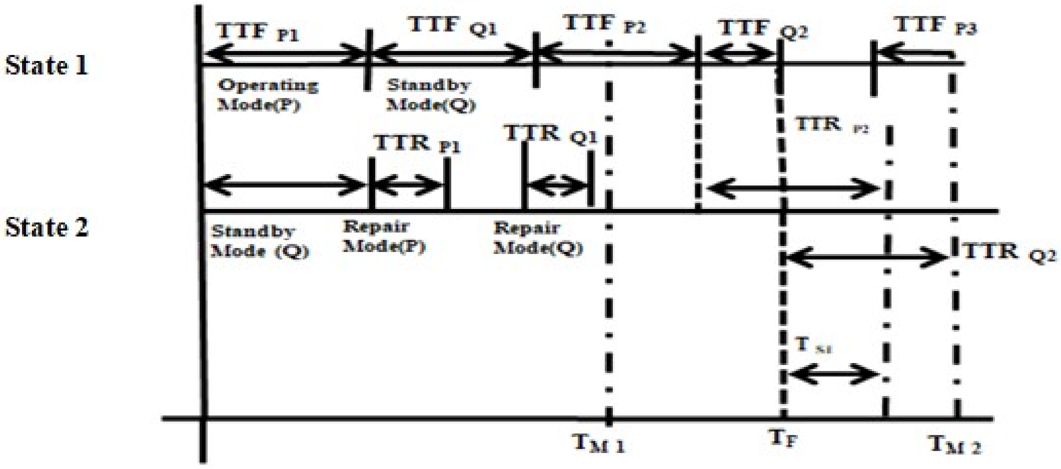


Fig.3.17: Operating Cycle of a Stand-by Systems, TTF: Time to Failure of Components, TTR: time to repair, TF: First System failure, TM: Mission Time, Ts = First system downtime

Table 3.2: Encountering frequency of states

Modes	State I	State II	Frequency of Mode (with identical failure and repair rate of stand-by system and main)
1	Up	Up	$\frac{2\lambda\mu^2}{(\lambda+\mu)^2}$
2	Down	Up	$\frac{\lambda\mu}{\lambda+\mu}$
3	Up	Down	$\frac{\lambda\mu}{\lambda+\mu}$
4	Down	Down	$\frac{2\mu\lambda^2}{(\lambda+\mu)^2}$

Table 3.3: Frequency of Modes

Module → Frequency of Modes ↓	1	2	3	4	5	6	7
1	0.82996	0.38432	0.27642	0.78978	0.00030	0.045599	0.549
2	0.41524	0.192232	0.13825	0.01880	0.236678	0.022799	0.274
3	0.41524	0.192232	0.13825	0.01880	0.236678	0.022799	0.274
4	0.00051	0.000134	8.72 x10^{-5}	8.60 x10^{-5}	5.32 x10^{-5}	5.93 x10^{-8}	0.00041

3.7. SENSITIVITY EVALUATION

In general, the sensitivity of a PMU is extremely important for its performance because it is the primary factor that defines the accuracy and dependability of the phasor readings. Sensitivity analysis is the performance evaluation technique for evaluating the change in the system's performance with respect to the change in its parameters.

It can estimate the effectiveness of a PMU with respect to change in failure rate or repair rate of a module. Mathematically, for a small parametric variation, it can be defined as the variation of the output response when there is a 1% change in any system parameter [30], i.e.

$$\text{Sensitivity (s) f(x)} = \left(\frac{\phi}{f(x)}\right)\left(\frac{\partial f(x)}{\partial \phi}\right) \text{ x } 100 \qquad (3.39)$$

However, for large variations repetitive computations are carried out considering small variations at a time. For multi parameter variation, Jacobean Matrix can be developed as shown below:

$$\mathrm{J}_{\Phi_i}^{f} = \begin{bmatrix} \frac{\partial f_1}{\partial \Phi_1} & \frac{\partial f_1}{\partial \Phi_2} \cdots & \frac{\partial f_1}{\partial \Phi_N} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_u}{\partial \Phi_1} & \frac{\partial f_1}{\partial \Phi_2} \cdots & \frac{\partial f_u}{\partial \Phi_N} \end{bmatrix} \tag{3.40}$$

Sensitivity of reliability indices w.r.t failure rate and repair rate are computed considering 1% variation in failure and repair rate values and is given in Appendix-A. The sensitivity of MTBF w.r.t repair rate is calculated from eqn. (3.41) and considering small change in repair rate.

$$\widehat{\boldsymbol{S}}_{\mu}^{MTBF} = \frac{\partial MTBF}{\partial \mu} \mathrm{X} \frac{\mu}{MTBF} \qquad \text{Hence, } \widehat{\boldsymbol{S}}_{\mu}^{MTBF} = \frac{\mu}{3\lambda+\mu} \tag{3.41}$$

Similar from eqn. (3.42), we can get

$$\widehat{\boldsymbol{S}}_{\mu}^{MTTR} = \frac{\partial MTTR}{\partial \mu} \mathrm{X} \frac{\mu}{MTTR} = \text{-1(constant)} \tag{3.42}$$

$$\text{Hence } \widehat{\boldsymbol{S}}_{\mu}^{MTTR} = \text{-1(constant)} \tag{3.43}$$

Similarly, reliability is computed from eqn.(3.31) and sensitivity w.r.t to failure rate (λ) is given by eqn. (3.44).

$$\widehat{\boldsymbol{S}}_{\lambda}^{R} = \frac{\partial R}{\partial \lambda} \mathrm{x} \frac{\lambda}{R} = \frac{\partial\{\text{expo}(-\lambda t)\}(1+\lambda t)}{\partial \lambda} . \frac{\lambda}{\{\text{expo}(-\lambda t)\}\,(1+\lambda t)\}} = \frac{-\lambda^2 t^2}{1+\lambda t} \tag{3.44}$$

Thus, sensitivity computations for availability, unavailability, MTBF, MTTR and reliability of modules w.r.t repair rate are given in Table- 3.4. However the sensitivity of MTTR w.r.t repair rate is constant.

Table 3.4: Sensitivity of PMU modules and PMU w.r.t repair rate and failure rate

Modules	$\hat{S}_{\mu}^{A}$	$\hat{S}_{\mu}^{UA}$	$\hat{S}_{\mu}^{MTBF}$	$\hat{S}_{\lambda}^{R}$
Transducer	0.99999	3.79735x 10^{-7}	0.053345	0.12196
Anti-alias filter	0.99999	1.23279x 10^{-7}	0.097747	0.031015
A/D convertor	0.99999	9.96372x10^{-8}	0.10755	0.016803
CPU	0.99999	5.4705x10^{-7}	0.99678	3.991x10^{-14}
GPS	0.995815	0.00418448	0.05202	0.7025
MODEM	0.99999	1.6935 x 10^{-12}	0.96693	0.0005082
Power supply	0.99999	5.671688 x10^{-7}	0.265909	0.05935
PMU	0.9993935	0.000606428	0.005407	0.06951

3.8. RESULT AND DISCUSSION

The Table 3.1 and 3.4 present the reliability indices and sensitivity indices w.r.t failure rate, considering 1% variation in failure rate. From the Table 3.1, it is noted that availability of the modules, increases as the failure rate decreases. However for module GPS and processor the reliability and sensitivity does not change appreciably. The overall sensitivity of PMU also increases with the change in failure rate. From the Table 3.4 it is observed that when the failure rate is reduced by 1% keeping the repair rate same, the availability of system increases. This is also evident from the fact that MTBF is inversely proportional to λ(failure rate). Further with increase or decreases in repair rate the MTBF decreases, also, when both repair and failure rate decreases by 1% the overall MTBF decreases, since the effect of reduction of repair rate dominates failure rate reduction. This statement is also applicable for availability. When the system is repairable, the availability and reliability of PMU is higher as compared to non-repairable component of the PMU module. For the completeness of PMU reliability evaluation, simulation of GPS and complete PMU is also carried out. It may be noted from the Table 3.1 that the reliability of PMU is 0.85388 and that of GPS is 0.99245 when computed analytically, whereas when the two devices are simulated, their respective values are 0.8875 and 0.9999. It can be seen that both analytically computed values and simulated values are nearly equal.

3.9. Conclusions

The reliability and sensitivity of PMU are effective characterization. They can predict the operational efficiency and utilization of PMU. Besides developing the fault tree logic diagrams of functional modules of PMU, Markov probabilistic mathematical models of all the modules of PMU are also developed. The numerical values of PMU availability, MTBF, MTTR and reliability of these modules and PMU as a whole are computed. Also, sensitivity of these modules is computed w.r.t failure rate and repair rate to study the effect of variation of failure rate and repair rate. It is observed that variation of failure rate is more dominant in reliability indices parameters of PMU to repair rate. The studies are useful for the system designer of PMU to identify the module which is more susceptible to unavailability. The sensitivity study predicts the possible variation in PMU reliability indices w.r.t failure and repair rates. The Markov Model enables to evaluate the frequency of probability in each residing state of the system. The probability of the system 'up state', 'down state' and de- rated state can be computed from the individual state probability. This frequency of encountering is very useful for understanding the behaviour of the system to evaluate the additional reliability indices that are continuously operated, repaired and maintained.

CHAPTER - IV

RISK ASSESSMENT OF PMU USING FUZZY LOGIC

4.1. INTRODUCTION

For efficient and reliable operation of power system reliability of PMU plays an important role. Markov model described in last chapter has a limitation that it assume the system in a steady state, considering the probability of transition from one state to another are constant but in real world dynamic nature of parameter needs to be considered. Manufacturers define the PMU's parametric values at intervals. These parametric values can deviate from the design value due to environmental and operational conditions. Hence, parametric values of PMU module are always within the region of uncertainty. To account for the uncertainty in the parametric set, soft computing technique such as fuzzy logic is necessary. This prompted the examination of the PMU's risk performance using an Interval Type-2 Fuzzy Logic system (IT2FS). Fuzzy logic is a soft computing technology that can take into account ambiguity and uncertainty in parametric values of PMU modules. In Type-1 fuzzy logic system, the fuzzy membership value is assured and it can extract information from data with ambiguous values. However, if the fuzzy membership value also is ambiguous and falls within an interval, the fuzzy logic system is categorised as Interval Type-2 system (IT2FS)[31]. Fuzzy set type-1 may be stated mathematically as eqn. (4.1):

$$A =\{x,\ \mu_A(x);\ x\in X\},\text{in which } 0 \leq \mu_A(x) \leq 1 \tag{4.1}$$

The value of A describes a degree of membership, $\mu_A(x)$ of x in A, whereas Type-2 can be written as [31]:

$$\tilde{A}=\{(x,u),\mu_{\tilde{A}}(x,u);\ \ x\in X;\ \ u \in U\equiv [0, 1]\} \tag{4.2}$$

in which $0 \leq \mu_{\tilde{A}}(x, u) \leq 1$. U is the universe of course for the secondary variable, u. This can also be rewritten as:

$\tilde{A}=\iint_{u\in \mathrm{U}} \mu_{\tilde{A}}(x,u)/(x,u)\ ; where \iint$ denotes union of all admissible x and u. Interval type-2 Fuzzy logic system (IT2FS) is a special case of type-2 fuzzy system (T2FS), in which the confidences level is defined in an interval i.e. data is presented in a bounded region of defined function, called foot print of uncertainty (FOU)[32]. Mathematically, it is represented as eqn. (4.3):

$$\mu_{\tilde{A}}(x, u) = 1 \text{ for } x \in X \text{ and } u \in [0,1] \text{ and } (x,u) \in FOU(\tilde{A}) \quad (4.3)$$

Fig 4.1 shows the graphical representation of FOU.Foot print of uncertainty (FOU) is another important characterization of IT2FS. It is uncertainty band between the upper membership function and the lower membership function. It is desired to reduce the FOU without compromising on the information contained in it to make classification more accurate.

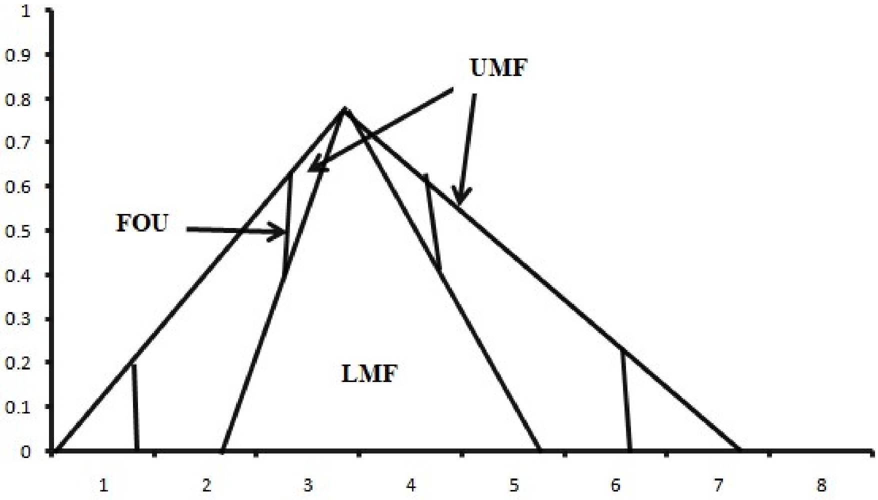


Fig.4.1: FOU of symmetrical IT2FS

Accordingly, in IT2FS, every point on universe of discourse X, has two points. If X= {1,3,5,7} and by Mendle's definition, [33] its primary membership is:

$$I = \begin{cases} [0.0, 0.25] & ; x=1 \\ [0.5, 0.75] & ; x=3 \\ [0.5, 0.75] & ; x=5 \\ [0.0,0.25] & ; x=7 \end{cases} \quad (4.4)$$

$$\text{Then, } FOU(\omega_3) = \frac{[0.0,0.25]}{1} + \frac{[0.5,0.75]}{3} + \frac{[0.5,0.75]}{5} + \frac{[0.0,0.25]}{7} \quad (4.5)$$

If the data cannot be defined by a given confidence level, a Type-2 fuzzy system must be utilised. The amount of confidence relies on the standard deviation or mean value of the test data variance. There are several approaches for evaluating data using Type-2 Fuzzy logic, including the α-cut method, Vertical Slice, and Wavy Slice representation, among others [34]. The interval type-2 fuzzy system (IT2FS) approach is one of the most effective techniques for studying type-2 fuzzy logic systems. It can effectively manage type-2 fuzzy systems. In the present study the α-cut approach has been considered for evaluating the risk assessment, reliability indices, and RAM sensitivity of PMU. Since design engineers and power system operators assess the utility and life cycle costs of PMU. Reliability, availability, and maintainability (RAM) are used to assess the performance of a PMU. RAM is a symbol of competence.

4.2 FUZZY LOGIC SYSTEM

A Fuzzy logic system is a human-centred technique that can handle ambiguity and uncertainty. It is a multi-level logic, with the ultimate objective of providing a solution for approximation reasoning using imprecise propositions based on fuzzy set theory[35]-[38], equivalent to classical reasoning using exact propositions based on classical set theory. Consider the following linguistic approximation reasoning that cannot be addressed by classical (precise) reasoning utilising two-valued logic.(i) PMU reliability is low if it is between 0.4 and 0.7, but good if it is between 0.7 and 0.9, and very high if it is between 0.9 and 0.95. (ii) PMU reliability of 0.7 falls into the low reliability group, whereas 0.71 falls into the good category. (iii) PMU reliability of 0.7 is low but not bad; PMU reliability of 0.71 is good but not exceptionally good. Of course, this is a valid logical deduction. This is an illustration of approximation reasoning. Fuzzy logic can be used to deal with such imperfect inference. In a nutshell, fuzzy logic allows for imprecise verbal words such as(a) ambiguous predicates (b) fuzzy quantifiers (c) fuzzy truth values. Fuzzy logic system can be classified in two types: (i) Static Fuzzy logic model and (ii) Dynamic Fuzzy model

(i) **Static Fuzzy Model:** The goal is to lessen the impact of random loading aggregation and disaggregation-induced natural fluctuations on the system under investigation[39]. Particularly, the filtering of measurement data collected in the field is processed using a fuzzy logic system.

(ii) **Dynamic Fuzzy Model:** The basic principle of dynamic approximation reasoning is dynamic fuzzy logic, where the truth values and the inference rules are fuzzy and are variable in nature[39].

4.2.1 Fuzzy Logic Architecture

Architecture of fuzzy logic has four components:

(i) Rule base: A fuzzy rule is a statement with conditions. On the basis of input variables, these principles are utilised to infer an output. IF THEN statements provide a form of fuzzy rules and must be used to indicate the antecedents. The mapping of variables from one fuzzy set to another is defined by a fuzzy relation. If A and B are fuzzy sets on universes X and Y, respectively, then the Cartesian product between them will produce a fuzzy relation R that is either a subset of the cartesian product of fuzzy subsets or is contained inside the whole cartesian product space. Formally, a fuzzy relation can be defined as,

$\underline{R} = \underline{A}$ x $\underline{B}$ and $\underline{R} \subset (X \text{ x } Y)$

where the relation $\underline{R}$ has a membership function,

$\mu_{\underline{R}}(x, y) = \mu\underline{A}_{x}\underline{B}(x, y) = \min(\mu\underline{A}(x), \mu\underline{B}(y))$

A binary fuzzy relation $\underline{R}(X, Y)$ is called a bipartite graph if $X \neq Y$.

A binary fuzzy relation $\underline{R}(X, Y)$ is called directed graph or digraph if $X = Y$, which is denoted as $\underline{R}(X, X) = \underline{R}(X^2)$

Let $\underline{A} = \{a_1, a_2, \ldots, a_n\}$ and $\underline{B} = \{b_1, b_2, .., b_m\}$, then the fuzzy relation between $\underline{A}$ and $\underline{B}$ is described by the fuzzy relation matrix as,

$$P= \begin{pmatrix} \mu_R(a1,b1) & \mu_R(a1,b2) & ---- & \mu_R(a1,bm) \\ \mu_R(a2,b1) & \mu_R(a2,b2) & ---- & \mu_R(a2,bm) \\ ---- & ---- & --- & ---- \\ \mu_R(an,b1) & \mu_2 & \mu_R(an,b2) & \mu_R(an,bm) \end{pmatrix}$$

(ii) Fuzzification: Fuzzification is the process of converting a crisp quantity into a fuzzy quantity utilising membership values. As seen in Fig.4.1, the vertex p, upper limit 't', and lower limit 's' together create the triangle function seen in Fig.4.1. As a result, the function A(x) may be expressed as follows:

A(x) = 0; $x \leq s$
=(x-s)/ (p-s); $s < x \leq p$
= (t-x) / (t-p); $p < x < t$
= 0 $x \geq t$

Fuzzification is carried out using membership functions like trapezoidal, triangular, Gaussian, etc., while inferencing is handled using a rules basis. The centroid approach, the centre of gravity method, the mean maximum membership method and the centre of biggest area method, etc. may all be used to defuzzify the inference engine's fuzzy output set.

(iii) Inference Engine: The input field, determines which rules should be fired and the degree to which the current fuzzy input matches each rule. Control actions are then created by combining the fired rules.

(iv) Defuzzification: The inference engine's fuzzy sets are transformed into crisp values using it. Numerous defuzzification techniques exist, and the most effective one is combined with a particular expert system to minimise the errors.

The architectural block diagrams for type-1 and type-2 fuzzy logic systems are shown in Fig.4.2(a) and (b).

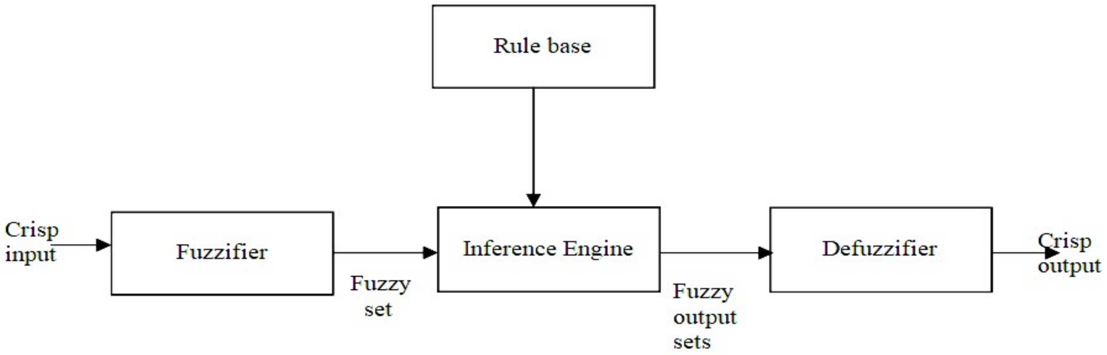


Fig.4.2a: Architecture of Type-1 Fuzzy logic system

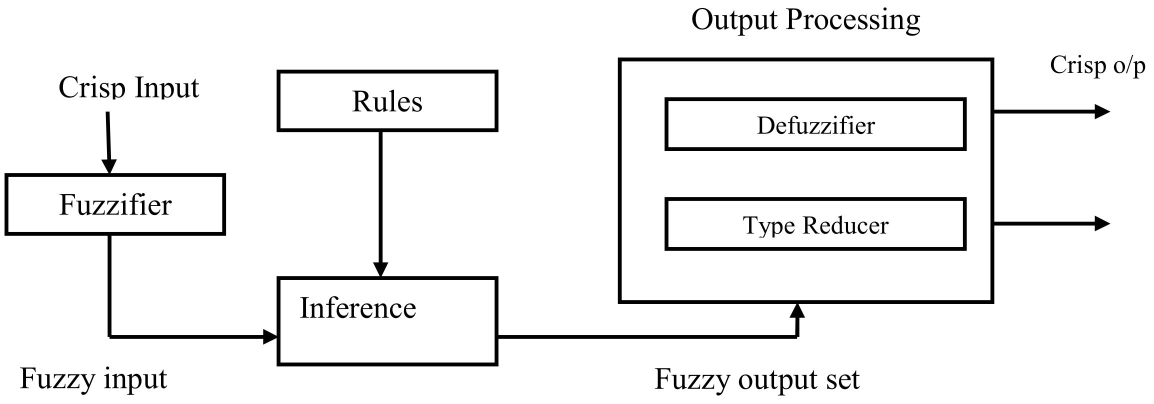


Fig.4.2b: Architecture of Type-II Fuzzy logic system

4.2.2 Interval Type-2 Fuzzy Logic Model

Jerry Mendel introduced Type-2 fuzzy logic in 2001 as an extension to traditional (Type-1) fuzzy logic[48]. The motivation behind the development of type-2 fuzzy logic was to overcome some of the limitations of type-1 fuzzy logic when dealing with uncertain and vague data. Type 1 fuzzy logic is concerned with assigning distinct membership values to fuzzy collections. Membership values indicate the extent to which an element is a member of an ambiguous set. Type 1 fuzzy logic is effective at dealing with uncertain data, but it is not suited for managing greater degrees of uncertainty and ambiguity.

Type-2 fuzzy logic extends the concept of fuzzy sets to incorporate ambiguity regarding the membership function. In other words, rather than assigning a crisp membership value to a fuzzy set, a type-2 fuzzy set assigns a set of membership functions, each of which represents a varying level of uncertainty regarding the degree of membership. When fuzzy values are presented in range of intervals, IT2FLS can be used to enhance the accuracy and reliability index computation.

IT2FLS includes a collection of inputs, fuzzy rules, and outputs. The voltage and current measurements acquired by the PMU are the inputs to the IT2FS model. Using an IT2FLS model to estimate power system variables using PMU has several advantages as stated below:

- IT2FLS can account for ambiguity and imprecision in the measurement process and generate more precise estimates of the power system variables.
- IT2FLS models are robust and can accommodate chaotic data, outliers, and missing data.
- IT2FLS models are readily modifiable and adaptable to various applications and scenarios.

4.3. FUZZY LOGIC MODEL OF PMU

The data collected by PMUs is used to analyse the behaviour of the power system. The use of estimating the reliability of PMU using Interval type-2 Fuzzy logic system (IT2FS) can increase the precision and accuracy in calculated values. The fundamental concept is to use fuzzy sets to characterise the uncertainty in the PMU measurements. The fuzzy sets can be used to represent both the degree of uncertainty and degree of membership.

When dealing with uncertainty in data, system specification representing data is often presented in a confined zone. Such issues are analysed using an Interval type-2 fuzzy System (IT2FS) model coupled with probability theory. This requires a probability density function that accounts for random uncertainty. If the probability distribution function is Gaussian, then just the mean and variance are required to fully characterise it [43]-[47]. In addition, the degree of accuracy variation in Gaussian functions is minimal. Fig. 4.3 depicts the Gaussian function with a fixed mean and an undetermined standard deviation for a type-1 fuzzy system.

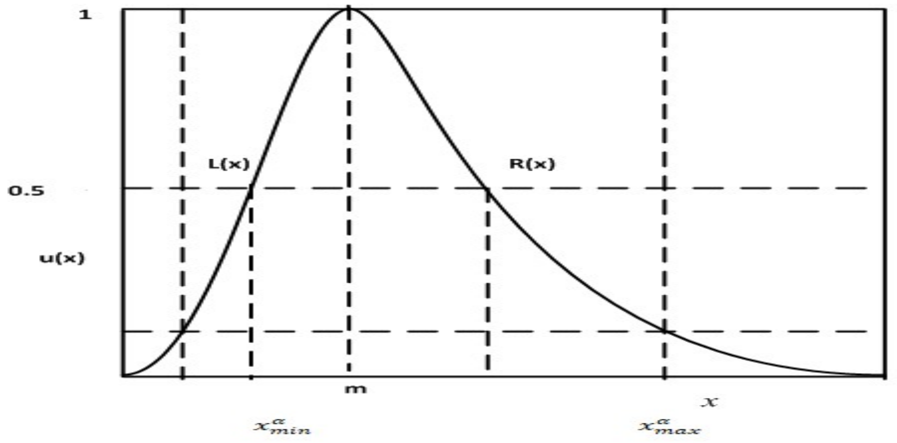


Fig.4.3: Asymmetrical Fuzzy Gaussian function with α - cut

4.3.1 The Alpha - Cut Computations

L.A. Zadeh[49] introduced the concept of alpha-cut to the field of fuzzy sets in 1965. The original chapter by Zadeh proposed alpha-cut as a method for transforming an ambiguous set into a set suitable for mathematical operations. Since then, the concept of alpha-cut has been extensively adopted in the field of fuzzy logic, particularly for applications that require a more nuanced representation of uncertainty. In the context of PMUs, alpha-cut fuzzy logic has been utilized to enhance the precision and dependability of the PMUs' measurements.

Several extensions and variations of alpha-cut fuzzy logic, such as interval type-2 fuzzy logic and generalized type-2 fuzzy logic, have been proposed over the years. These enhancements have expanded the capacity of fuzzy logic to deal with uncertainty and imprecision. In fuzzy logic, an alpha-cut is a set acquired by removing all fuzzy elements whose membership values are less than a specified alpha threshold [50]. In other words, an alpha-cut of a fuzzy set is the subset of the set containing all elements with a membership degree greater than or equal to alpha. α –plane may be produced directly from α –cut of the secondary membership functions in a similar way as in type-1 fuzzy system can be acquired (T1FS). In the context of PMUs, alpha-cut fuzzy logic is used to analyse the behavior of the power system by approximating the membership function of a fuzzy set with a set of alpha-cuts.

Several steps are necessary to implement alpha-cut fuzzy logic in PMU. First, the range of potential values for each variable in the power system must be established. This can be accomplished using either historical data or mathematical models to predict expected values. After defining the ranges, the intervals can be subdivided into a series of cuts, with each cut being designated a degree of membership based on the level of uncertainty or imprecision associated with the measurement. The alpha-cut value must then be selected. This value determine which intervals are included and excluded from the fuzzy set. The selection of the alpha-cut value can have a substantial effect on the accuracy and dependability of the fuzzy logic system, and it may be necessary to make adjustments based on the particular application and requirements.[51]-[53]

After fuzzy sets and rules have been defined, the system can be evaluated using simulated or actual data to determine its accuracy and effectiveness. It is essential to comprehensively validate the system to ensure that it provides accurate and reliable information about the power system.

Alpha-cut fuzzy logic is particularly useful in applications where uncertainty in the data acquired from PMUs must be represented.

α– cut is a degree of Fuzzy set$\widetilde{Y}\epsilon$ [0,1], and written as[54]:

$$\widetilde{Y}^{(\alpha)} = \{x \, \epsilon \, X \mid \mu_{\widetilde{Y}}(x) \geq \alpha\}, \tag{4.10}$$

Where α is a parameter in the range $0 \leq x \leq 1$.

To account for parameter uncertainty, a range of a parameter rather than a single value should be employed in PMU reliability evaluation. The cut-set in a fuzzy variable membership function is consistent with the idea of a range. In this part, the pseudo-Gauss (PG) function, a novel fuzzy membership model, is introduced first. The suggested model, which derives from the widely used Gaussian fuzzy member- ship function, is capable of handling both symmetric and asymmetric parameter characteristics in addition to accounting for statistical characteristics of the reliability parameters of PMU components. The general form of the membership function presented.

Consider the Gaussian Fuzzy function, Fig. 4.6 The presented membership function has the general form presented in eqn.(4.11)

$$U(x)=\begin{cases} L(x) = exp\left[\frac{(x-m)^2}{\sigma_L^2}\right] x < m \\ R(x) = exp\left[\frac{(x-m)^2}{\sigma_L^2}\right] x \geq m \end{cases} \tag{4.11}$$

where *x* represents a reliability parameter of a component in PMU, m is the mean estimate of *x*, *L(x)* and *R(x)* are the left and right parts of U(x) . The shapes of *L(x)* and *R(x)* are mainly dependant on the scale parameters σ_L and σ_R.

σ_L and σ_R are standard deviation of left and right sides and is given by eqn. (4.12)

$$\sigma_L=\frac{(x^{\alpha}-m)}{\sqrt{-ln}};\sigma_R=\frac{(x^{\alpha}-m)}{\sqrt{-ln}} \tag{4.12}$$

For a specified a α_i the α_i-cut interval $\{x_{min}^{\alpha}, \; x_{max}^{\alpha}\}$ of the PG membership function can be obtained using eqn. (4.13).

$$x_{min}^{\alpha}= m - \sigma_L\sqrt{-\ln{(\alpha i)}}, \tag{4.13}$$

$$x_{max}^{\alpha}= m + \sigma_R\sqrt{-\ln(\alpha i)} \tag{4.14}$$

4.4. APPLICATION OF IT2FS FOR RISK ASSESSMENT OF PMU

The membership functions of reliability parameters of its components are inputs for each module of the PMU. Fuzzy interval computations and the equivalent Markov models of all modules can be used to assess the reliability indices of the PMU as a whole. Fuzzy models of the modules differ fundamentally from crisp models, in that all of the variables are expressed as the fuzzy values. They necessitate interval calculations at fuzzy grades (cut-sets) and use their membership functions. The interval of failure rate and repair rate (lower limit, upper limit) of seven modules of PMU are presented in Appendix-B and mean value for the mission time (t) of 8760 hr. These values are used to generate the Fuzzy Gaussian function (y_1, y_2, y_3), corresponds to lower value, mean value, and upper value of data at 0, 1and 0.1 fuzzy membership values. The following assumption are considered while applying the proposed method [57]:

(i) The PMU device is in its prime life.

(ii) The device is made of electronic components and modules.

(iii) The modules of PMU have different failure rates.

(iv) The data supplied by the manufacturer is limited and mathematical computations are not very accurate and sometimes not even feasible.

Based on these assumptions, the following restrictions are presented in the proposed method:

(a) The ratio of repair time (r) to the mission time is small (≤ 0.1).

(b) The failure rates (λ) are very small ($\leq 10^{-3}$/h).

(c) The product of failure rate and mission time is small (≤ 0.1).

(d) The failure rate and repair time are constant and failures are independent.

Power Supply and MODEM are assumed to have two units in parallel-connection for redundancy. Therefore, using the parallel network concept [58]-[60], the equations used are (4.15)-(4.17):

$$\lambda_{M6/7}^{\alpha}=[\lambda_{1min}^{\alpha}\lambda_{2min}^{\alpha}(r_{1min}^{\alpha}+r_{2min}^{\alpha}),\quad \lambda_{1max}^{\alpha}\lambda_{2max}^{\alpha}(r_{1max}^{\alpha}+r_{2max}^{\alpha})] \tag{4.15}$$

$$r_{M6/7}^{\alpha}=[1/(1/r_{1min}^{\alpha}+1/r_{2min}^{\alpha}),$$

$$1/(1/r_{1max}^{\alpha}+1/r_{2max}^{\alpha})] \tag{4.16}$$

$$U_{M6/7}^{\alpha}=[\lambda_{1min}^{\alpha}r_{1min}^{\alpha}\lambda_{2mi}^{\alpha}\ r_{2min}^{\alpha},\ \lambda_{1ma}^{\alpha}\ r_{1max}^{\alpha}\lambda_{2max}^{\alpha}r_{2max}^{\alpha}] \tag{4.17}$$

where λ_{1min}^{α}, r_{1min}^{α}, $\lambda_{2min,}^{\alpha} r_{2min}^{\alpha}$,and λ_{1max}^{α}, r_{1max}^{α}, λ_{2max}^{α}, $r_{2max}^{\alpha}$are the lower and upper bound of α – cut interval for failure and repair rate.

Two circuit boards (C1 and C2) are in parallel, and each of them consists of three single-phase voltage circuits and three single-phase current circuits in series. From a reliability standpoint, this is advantageous because a board fails if any voltage or current circuit fails. This structure is shared by the CT/PT (M1), low-pass/band-pass filter module (M2), and analog/digital sampling module (M3).

Since the entire board will be replaced regardless of which circuit fails, it is assumed that each voltage (or current) circuit has an identifiable failure rate and that each circuit board has a total repair (replacement) rate.

For modules M1, M2, M3 eqn.(4.18)-(4.20) are considered.

$$\lambda_{M1,2,3}^{\alpha}=[\lambda_{C1min}^{\alpha}\lambda_{C2min}^{\alpha}(r_{C1min}^{\alpha}+r_{C2min}^{\alpha}),\ \lambda_{C1ma}^{\alpha}\ \lambda_{C2max}^{\alpha}(r_{C1max}^{\alpha}+r_{C2max}^{\alpha})] \tag{4.18}$$

$$r^{\alpha}=[1/(1/r_{C1min}^{\alpha}+1/r_{C2min}^{\alpha}),1/(1/r_{C1max}^{\alpha}+1/r_{C2max}^{\alpha})] \tag{4.19}$$

$$U^{\alpha}=[\lambda_{C1min}^{\alpha}r_{C1min}^{\alpha}\lambda_{C2min}^{\alpha}r_{C2m}^{\alpha}\quad ,\qquad \lambda_{C1Smax}^{\alpha}r_{C1max}^{\alpha}\lambda_{C2max}^{\alpha}r_{C2max}^{\alpha}] \tag{4.20}$$

Where

$$\lambda_{C1}^{\alpha}=[3(\lambda_{C1}^{U(\alpha)})_{\text{min}}+3(\lambda_{C1}^{I(\alpha)})_{\text{min}},3(\lambda_{C1}^{U(\alpha)})_{\text{max}}+3(\lambda_{C1}^{I(\alpha)})_{\text{max}}] \tag{4.21}$$

$$\lambda_{C2}^{\alpha}=[3(\lambda_{C2}^{U(\alpha)})_{\text{min}}+3(\lambda_{C2}^{I(\alpha)})_{\text{min}},3(\lambda_{C2}^{U(\alpha)})_{\text{max}}+3(\lambda_{C2}^{I(\alpha)})_{\text{max}} \tag{4.22}$$

Here, $\lambda_{C1}^{U(\alpha)}$,$\lambda_{C1}^{I(\alpha)}$,$\lambda_{C2}^{U(\alpha)}$,$\lambda_{C2}^{I(\alpha)}$are the failure rate of voltage and current for circuits C_1 and C_2.

CPU comprises of hardware and software. The failure of either circuit makes the CPU unavailable. Now, if 'λ' and 'r' represent failure rate, and repair rate and U are the unavailability of CPU, then following eqns.(4.23) – (4.25) holds[59].

$$\lambda = \lambda_{sw} + \lambda_{Hwn} \tag{4.23}$$

$$r=(\lambda_{sw}.r_{sw} + \lambda_{Hw}.r_{HW}) / (\lambda_{sw} + \lambda_{Hw}) \tag{4.24}$$

$$U =\lambda_{sw}.r_{sw} + \lambda_{Hw}.r_{HW} \tag{4.25}$$

By using fuzzy algebra, interval calculations of alpha cut (α-cut) grade for failure rate, and unavailability can be written as eqns. (4.26) to (4.28).

$\lambda^{\alpha i} = \{\lambda^{\alpha i}{}_{Swmin} + \lambda^{\alpha i}{}_{HWmin}, \lambda^{\alpha i}{}_{Swmax} + \lambda^{\alpha i}{}_{HWmax}\}$ (4.26)

$U^{\alpha} = \{\lambda^{\alpha}{}_{swmin}.r^{\alpha}{}_{swmin} + \lambda^{\alpha}{}_{Hw.min}r^{\alpha}{}_{HWmin}, \lambda^{\alpha}{}_{swmax}.r^{\alpha}{}_{swmax} + \lambda^{\alpha}{}_{Hw.max}r^{\alpha}{}_{HWmax}\}$ (4.27)

However, conventional arithmetic operation cannot be applied to repair time computations when α-cut operation is applied, since numeration and denominator both contain λ_{Hw} and λsw in eqn.(4.24). The following alternative is applied accordingly.

$r = (\lambda_{sw}.r_{sw} + \lambda_{Hw}.r_{HW}) / (\lambda_{sw} + \lambda_{Hw})$

$= [(r_{sw}.\lambda_{sw}/\lambda_{Hw}). + r_{HW})] / \{\lambda_{sw}/\lambda_{Hw} + 1\}$

$= [(r_{sw}Z + r_{HW})] / \{Z + 1\}$ (4.28)

Here, $Z = \lambda_{sw} / \lambda_{Hw}$

Therefore, α-cut operation on repair time is given by eqn. (4.29).

$r^{\alpha} = [\min\{f(r^{\alpha}{}_{swmin}, r^{\alpha}{}_{HWmin}, Z^{\alpha}{}_{min}), f(r^{\alpha}{}_{swmin}, r^{\alpha}{}_{HW\ min}, Z^{\alpha}{}_{max})\}, \max\{f(r^{\alpha}{}_{sw\ max}, r^{\alpha}{}_{HW\ max}, Z^{\alpha}{}_{min}), f(r^{\alpha}{}_{swmax}, r^{\alpha}{}_{HWmax}, Z^{\alpha}{}_{max})\}]$ (4.29)

where $Z^{\alpha} = (\lambda^{\alpha}{}_{swmin}/\lambda^{\alpha}{}_{Hwmin}, \lambda^{\alpha}{}_{swmax}/\lambda^{\alpha}{}_{Hwmax})$ (4.30)

For module GPS the equivalent failure rate, repair rate and unavailability is given by following equations (4.31) to (4.33).

$\boldsymbol{\lambda}_{M5} = [P_1(q_s\boldsymbol{\lambda}_A + \boldsymbol{\lambda}_B) + P_2(\boldsymbol{\lambda}_T + \boldsymbol{\lambda}_B)] / (P_1 + P_2)$ (4.31)

$r_{M5} = [P_3 + P_4 + P_5 + P_6] / [P_1(q_s\boldsymbol{\lambda}_A + \boldsymbol{\lambda}_B) + P_2(\boldsymbol{\lambda}_T + \boldsymbol{\lambda}_B)]$ (4.32)

$U_{M5} = P_3 + P_4 + P_5 + P_6$ (4.33)

Now, using the above equations, Reliability importance (RI) index is computed using eqn. (4.34) at different alpha cut

$\partial R_{System} / \partial R_{Sub\text{-}system} = RI$ (4.34)

The overall availability(A), unavailability(U), reliability(R), unreliability of PMU and maintainability can be calculated by considering the individual modules parameters as given by eqn.(4.35)-(4.39) and also graphs are plotted shown in Fig. 4.4(a-e)

$A_{PMU} = A_{M0} * A_{M1} * A_{M2} * A_{M345} * A_{M6}$ (4.35)

$U_{PMU} = 1 - A_{PMU}$ (4.36)

$\lambda_{PMU} = \lambda_{M0} + \lambda_{M1} + \lambda_{M2} + \lambda_{M345} + \lambda_{M6}$ (4.37)

$\mu_{PMU} = (A_{PMU} * \lambda_{PMU}) / U_{PMU}$ (4.38)

$$R_{PMU} = \frac{S_{1e}{}^{-s_2 t} - S_{2e}{}^{-s_1 t}}{S_{1} - S_{2}} \tag{4.39}$$

where S_1 and S_2 are

$S_1 = \frac{1}{2}(3\lambda+\mu+\sqrt{(\lambda^2+6\lambda\mu+\mu^2)})$

$S_2 = \frac{1}{2}(3\lambda+\mu-\sqrt{(\lambda^2+6\lambda\mu+\mu^2)})$

$$\text{Maintainability} = (1-e^{\mu t}) \tag{4.40}$$

RAM=w_1*Reliability+w_2*Availability+w_3*Maintainability

here w_1= 0.36, w_2= 0.30, w_3= 0.34 are weights as suggested by system experts.

$$\text{RAM} = 0.36{*}R+0.30{*}A+0.34{*}M \tag{4.41}$$

Unavailability and RAM are computed at different α-cuts using eqns. (4.15) – (4.41). All the computed values are shown at Appendix B. Fig. 4.4(a) to (e) represent the variation of reliability, failure rate, MTBF, repair rate and unreliability w.r.t Alpha(α)

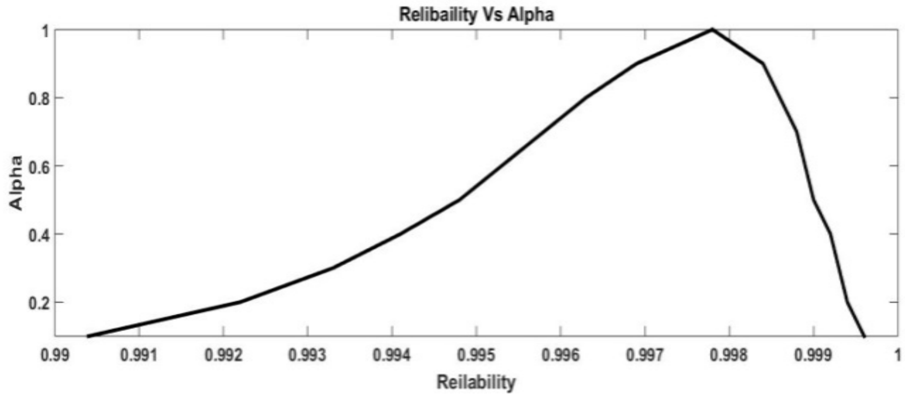


Fig.4.4a: Reliability Vs Alpha

This graph(Fig. 4.4a) may illustrate how the overall reliability of PMUs changes with different alpha. Higher reliability values are typically desirable.

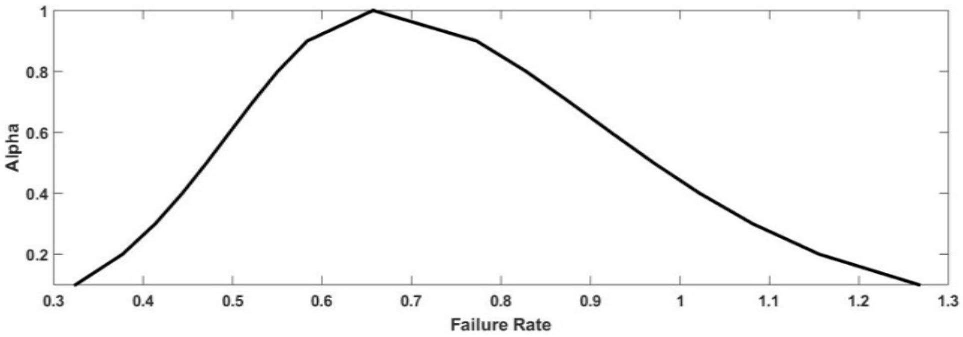


Fig.4.4b: Failure Rate Vs Alpha

Failure Rate vs. Alpha (Fig. 4.4b): Illustrating how the rate of failures changes with different Alpha.

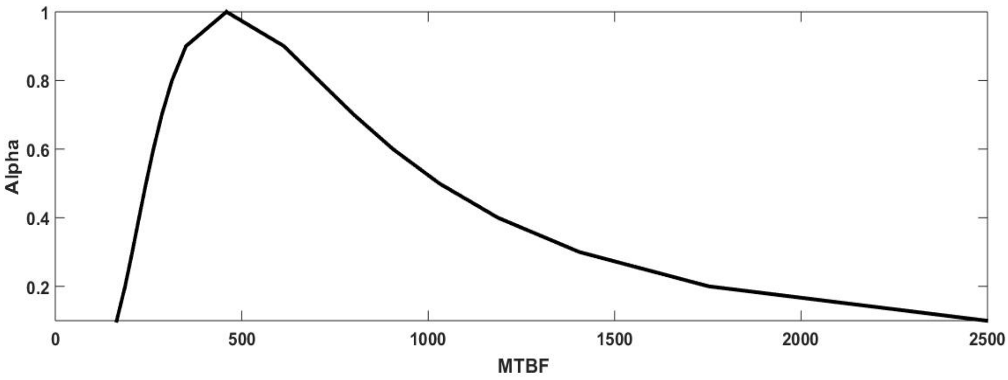


Fig.4.4c: MTBF Vs Alpha

This figure likely depicts how the Mean Time Between Failures (a measure of reliability) varies with the alpha in a particular set or category. A higher MTBF generally indicates better reliability.

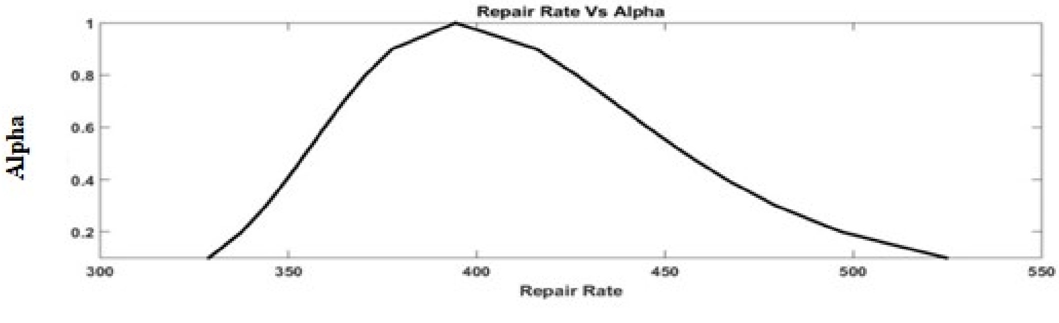


Fig.4.4d: Repair rate Vs Alpha

This (Fig.4.4d) how quickly PMUs can be repaired or restored to operational status.

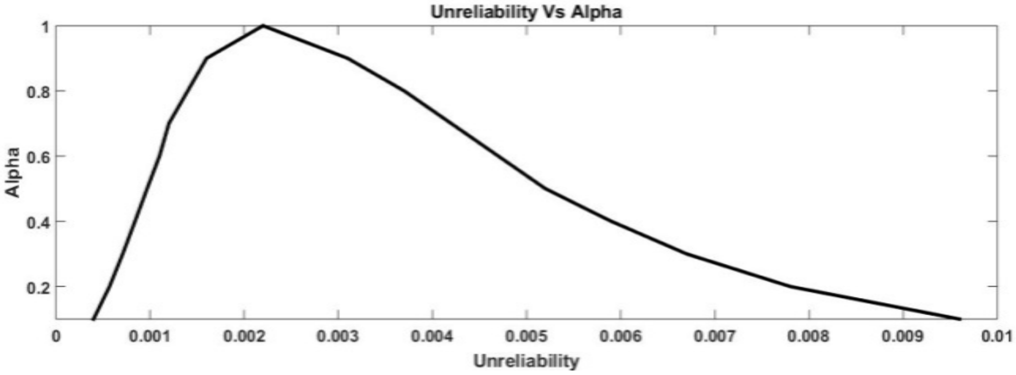


Fig.4.4e: Unreliability Vs Alpha

Fig. 4.4 e demonstrates the degree to which the PMUs are not meeting reliability expectations.

4.5. FUZZY SENSITIVITY OF PMU RELIABILITY

Fuzzy sensitivity analysis is an effective method for evaluating the dependability of Phasor Measurement Units (PMUs) and identifying the main factors that influence their performance. This method employs fuzzy logic to model the imprecision and uncertainty that are frequently present in the data and is used to evaluate the PMU's reliability, in a more precise and robust manner.

In general, fuzzy sensitivity analysis is a useful method for assessing the dependability of PMUs and enhancing their performance. Utilising fuzzy sensitivity analysis for PMU has a number of advantages. This permits the incorporation of ambiguous and uncertain data, which is frequently present in PMU applications. This can lead to more accurate and robust models of PMU reliability and aid in the identification of important factors influencing PMU performance. Another benefit is that fuzzy sensitivity analysis permits simultaneous evaluation of the influence of multiple input variables on PMU reliability. This can aid in the identification of complex relationships between input variables and PMU reliability and provide insight into how to optimise PMU performance.In conclusion, fuzzy sensitivity analysis is an effective method for assessing the dependability of PMUs and identifying the factors that have the greatest impact on its performance.

As seen from the Table- 4.1 the GPS module (M5) and phase processor–CPU module (M4) are the modules that have the greatest influence on PMU dependability. Therefore, sensitivity analysis is done just on these two modules, GPS (M5) and CPU (M4), in order to determine the effect of failure rate on PMU, which is indicated in Table- 4.2. Only one parameter(failure rate) is changed between 10% and 20% of the initial value described in Appendix B. PMU is created with several uncertainties in mind. The system designer seeks the best solution for various approximations of parameters. Thus, the sensitivity of PMU unavailability to variation in M4 and M5 failure rates, as well as the sensitivity RAM to variation in M4 and M5 failure rates, are estimated at various cuts using equations (4.42) and (4.43) and reported in Table- 4.3.

Fuzzy Sensitivity for Unavailability of M5 and M4

$$= \frac{U(M5or\ M4)at\ 90\%/110\% - U(M5or\ M4)at100\%/U(M5or\ M4)at100\%}{\lambda(M5or\ M4)at90\%/110\% - \lambda(M5or\ M4)at100\%/\lambda(M5or\ M4)at100\%} \qquad (4.42)$$

Fuzzy Sensitivity of RAM of M5 and M4

$$= \frac{U(M5or\ M4)at\ 90\%/110\% - U(M5or\ M4)at100\%/U(M5or\ M4)at100\%}{\lambda(M5or\ M4)at\ 90\%/110\% - \lambda(M5or\ M4)at100/\lambda(M5or\ M4)at100\%} \qquad (4.43)$$

4.6. RESULT AND DISCUSSION

Table- 4.1 demonstrates that the GPS module (M5) and phase processor–CPU module (M4) are the modules that have the greatest influence on PMU dependability. Table - 4.2 presents the fuzzy sensitivity of PMU at ±10% and ±20% variation of failure rate at α=0.1 and 0.5. The failure rate of λ_A, $\lambda_{B,}$ λ_T ,λ_{HW} and λ_{SW} are considered for the reason mentioned above. It may be noted from the Table - 4.2 that sensitivity of unavailability and RAM shown in Table 4.3 is higher at α= 0.5 to α=0.1. The effect of +10% failure rate variation dominates to -10% variation in case of GPS receiver. Further sensitivity of unavailability w.r.t. failure rate of GPS receiver is quite high to crystal oscillator. Also the sensitivity of unavailability w.r.t hardware is higher to that of software in case of CPU – processor.

Table-4.1: Unavailability of PMU & module

Modules	Unavailability
CT/PT(M1)	3.802x10^{-7}
Anti Alias Filter(M2)	1.233x10^{-7}
ADC(M3)	9.969x10^{-8}
CPU(M4)	6.93 x10^{-4}
GPS(M5)	9.701 x10^{-4}
MODEM(M6)	1.693 x10^{-12}
Power Supply(M7)	5.68 x10^{-7}
PMU	0.0017

Table-4.2: Calculations for Sensitivity

Parameters	$S_{\lambda}^{U(PMU)}$ (-10% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{U(PMU)}$ (+10% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{RAM(PMU)}$ (-10% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{RAM(PMU)}$ (+10% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{U(PMU)}$ (-20% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{U(PMU)}$ (+20% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{RAM(PMU)}$ (-20% $\boldsymbol{\lambda}$ variation)	$S_{\lambda}^{RAM(PMU)}$ (+20% $\boldsymbol{\lambda}$ Variation)
$\boldsymbol{\lambda}_A$ at α=0.1	(1.58,5.07)	(4.713,2.469)	(0.00806,0.017)	(0.0033,0.0031)	(1.1245,1.0403)	(1.1217,1.04498)	(0.0060,0.015)	(0.0022,0.0029)
$\boldsymbol{\lambda}_A$ at α=0.5	(2.25,10.3)	(5.309,30907)	(0.0168,0.0388)	(0.0068,0.0062)	(2.24,2.08)	(2.236,0.0889)	(0.01212,0.0242)	(0.0044,0.0048)
$\boldsymbol{\lambda}_B$ at α=0.1	(0.01,0.51)	(0.0825,1.667)	(0.0047,0.0115)	(0.0102,0.0070)	(1.1143,1.0021)	(1.1267,0.06387)	(0.00296,0.01002)	(0.0998,0.0069)
$\boldsymbol{\lambda}_B$ at α=0.5	(0.52,0.71)	(0.5886,2.228)	(0.0099,0.0268)	(0.0286,0.0142)	(2.22,2.004)	(2.245,0.1289)	(0.00492,0.01004)	(0.1889,0.0126)
$\boldsymbol{\lambda}_T$ at α=0.1	(0.83.0.64)	(0.443,3.248)	(0.0051,0.0012)	(0.0111,0.0082)	(1.1241,1.02967)	(1.1672,1.06202)	(0.00314,0.0110)	(0.01009,0.0074)

λ_T at α=0.5	(1.76,2.26)	(1.702,3.783)	(0.0109,0.0289)	(0.0256,0.0169)	(2.28,2.06)	(2.278,2.0246)	(0.00628,0.0022)	(0.02008,0.01498)
λ_{SW} at α=0.1	(0.012,0.53)	(0.0831,1.88)	(0.0041,0.0113)	(0.0108,0.0073)	(0.007,0.234)	(0.0962, 1.98)	(0.00213,0.01002)	(0.098,0.0064)
λ_{SW} at α=0.5	(0.51,0.493)	(0.56,0.278)	(0.0088,0.0226)	(0.0286,0.0146)	(0.0148,0.468)	(0.0182,2.98)	(0.00426,0.02004)	(0.0184,0.00129)
λ_{HW} at α=0.1	(1.371,5.656)	(4.108,3.8105)	0.0070,0.01414)	(0.0151,0.0218)	(1.1227,0.99158)	(1.13036,1.06006)	(0.00598,0.0126)	(0.0123,0.0129)
λ_{HW} at α=0.5	(2.144,6.595)	(4.590,3.645)	(0.0149,0.0296)	(0.0282,0.0459)	(2.244,1.82)	(2.26,2.020)	(0.0108,0.0242)	(0.0246,0.0249)

Table – 4.3 : Variation of RAM

RAM		
Alpha	Normal Min	Normal Max
0.1	0.9997	0.9954
0.2	0.9996	0.9962
0.3	0.9995	0.9967
0.4	0.9994	0.9970
0.5	0.9993	0.9973
0.6	0.9992	0.9975
0.7	0.9991	0.9978
0.8	0.9990	0.9980
0.9	0.9989	0.9983
1	0.9987	0.9987

4.7. CONCLUSION

PMU is an important device for integrated operation of grid. Its design, therefore, needs special attention so that it should be available all the time to the system operator for successful operation. Studies reveal that GPS receiver is the most critical sub-module in PMU devices. Once it fails, the crystal oscillator which was earlier in standby mode takes its place and carry out the function of synchronization with ADC and CPU. For a 50 Hz power system crystal oscillator fails when accumulated error exceeds the limit ±31 microseconds for more than one hour. These studies are useful to design and improve the availability of PMU to operate the grid more efficiently.

CHAPTER - V
UNCERTAIN DATA PROCESSING OF PMU MODULES USING FUZZY-PETRI NET

5.1. INTRODUCTION

PMU is an intelligent synchronous device that is utilized in the process of monitoring large-scale power systems. The failure rate of the PMU module is not sufficiently described by the manufacturers. There is a lack of clarity regarding the percentage failure of PMU modules during operation. The ever-changing external factors also contribute to the dynamic nature of the information processing. Fuzzy logic described in last chapter takes into account the dynamic nature of the processing but still the redundancy is not taken into account. Petri Net is a type of mathematical modeling tool that can be utilized for the purpose of describing and evaluating complicated systems. It is an ideal tool to take into account the redundancy and Fuzzy Petri Net (FPN) take into accounts both redundancy and dynamic nature. It has the ability to construct a fault tree offering the information flow from the operational state to the unavailability mode of the PMU. When it comes to coping with the inherent unpredictability of the transmission of information along the branching path of a sprouting tree, fuzzy logic reasoning is the most effective method. This chapter's study, which makes use of the sprouting method, offers design and system engineering insight into the failure flow of PMU components.

In this chapter the following flow of events is used for calculating the reliability of PMU

- ➢ Fault Tree Diagram of the Physical System using AND/OR gates is created.
- ➢ Transformation rules to transform a Fault tree into a marked Fuzzy Petri Net model (FPN) has been applied.
- ➢ Fuzzy production norms, the immediate reachable set, and reachable set has been determined.
- ➢ Sprouting tree from FPN is the method used to compute the degree to which an assertion is true has been developed.
- ➢ Ultimately, the reliability of the data obtained from the sprouting tree is validated.

5.2. FAULT TREE MODEL OF PMU

Fault tree model is a graphical and mathematical representation of system failure. It investigates the root causes of potential failure by reverse-engineering. The imprecise measurement of failure, repair rate etc of PMU modules make it difficult to assess its reliability. The individual failures or events that culminate in the apex event are the basic events in the fault tree model. The apex event is the last event in the model. The following could be some of the reasons for the failure of PMU:

- Interruption of power supply to the PMU.
- The PMU and the control system unable to establish a communication contact.
- Components of the PMU, such as the analog-to-digital converter and the GPS receiver, experience a failure in their hardware.
- A software glitch either in the PMU or in the control systems software

Fault Tree Model of the PMU is considered to examine the systems behaviour in the event of a failure. The fault tree is constructed based on following information.

a) **Events occurring in the Middle:** In the structure design paradigm, intermediate events represent those events that are triggered by one or more fundamental events. For instance, "Hardware failure of the GPS receiver" and "Loss of power supply to the GPS receiver" could be the underlying cause of the intermediate event.

b) **Logical outcomes of events:** The gates in the fault tree model are symbolic representations of the logical connections between events. AND gates, OR gates, and NOT gates are the most frequently employed types of gates. For example, an AND gate can simulate the requirement that two or more fundamental events must occur simultaneously so that an intermediate event or the top event can occur. This requirement must be met before an intermediate or final event can take place.

The following symbols are used to construct the fault tree:

- □ Top Event: A condition of a system that is undesirable due to events occurring within the system. This rectangle represents the leading event.

- ▭ Intermediate Event: A failure event that results from the combination of other events via logic gates is an intermediate event and is represented by a rectangle.
- ○ Basic Event: The circle defines a fundamental beginning fault occurrence for which no further development is required.
- ◇ Undeveloped Event: An occurrence that is not elaborated upon because it is of inadequate significance or because information is lacking.
- ∩ OR Gate: If at least one of the input faults happens, the output fault will occur.
- ∩ AND Gate: If all input faults occur, an output fault will occur.

After the fault tree model has been developed, top event or crucial event is identified by Boolean algebra, cut-set analysis. This data can be put to use to improve the overall reliability and performance of the PMU system by optimizing its design, maintenance, and operation. This can be accomplished by using the failure rate and repair rate dataset. The Phasor Measurement Unit (PMU) is made up of five modules with two sub modules as discussed in chapter I. It is necessary to specify the failure and repair rates of each module in order to conduct an analysis of the possibility of the integrated PMU being unavailable. The assumption is made that PMU will not fail if any of sub- module of DAS fails however, the quality of the input signal deteriorates. Alternately, the PMU will fail if complete DAS module will fail. In the same vein, a GPS system is deemed to be inoperable if both the GPS receiver and oscillator are unable to operate, or if the crystal oscillator/functional switch is unable to function. As a consequence of this, the PMU can be seen as a component of the 7-series modules and can be symbolised by logic failure. The fault tree diagram of PMU using AND and OR gates is represented in Fig. 5.1 [61]. The major objective of fault tree diagram is to represent system conditions symbolically with AND, OR and priority gates, which may cause the system to fail[62]-[65]. The fault tree does not depict all potential system faults or causes of system failure. Only those faults that contribute to the top event, which corresponds to a particular system failure state, are included in the fault tree.

The fault tree may be constructed by defining:

- The system (including all functional links) and its intended application.
- Undesirable occurrences within the system under discussion.

- The system fault conditions and their logical link to input fault events in terms of observable and independent faults.

Fault trees are devoid of events and redundancy. Fig.5.1 depicts the fault tree diagram of PMU . It pinpoints the systems weakness in visible form.

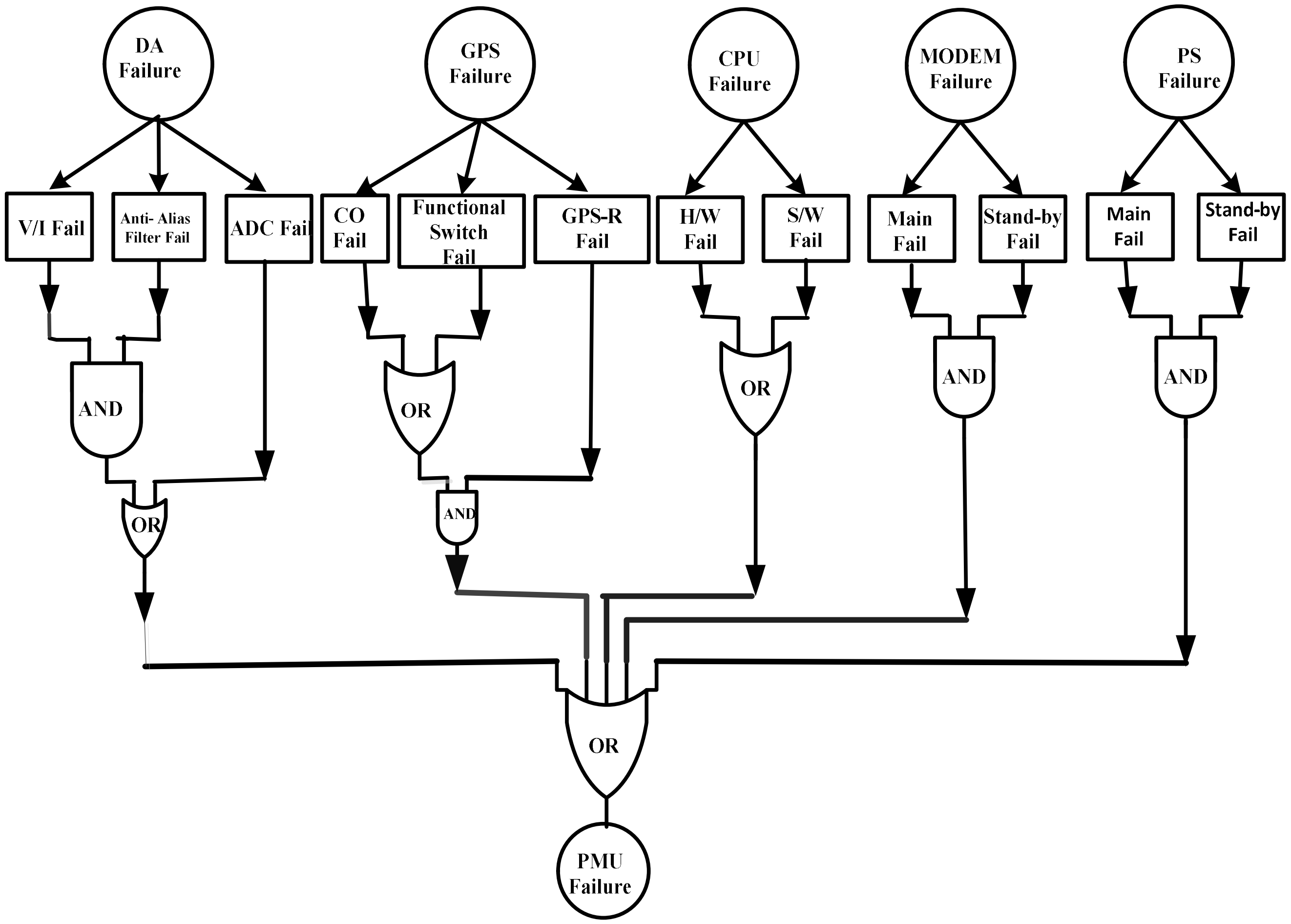


Fig.5.1: Fault Tree Diagram for PMU

5.3. PETRI- NET ARCHITECTURE

Petri-Net is a type of graphical modeling tool that is commonly used in the field of engineering to model and analyze concurrent and asynchronous behaviour in systems. Enrico Petri, an Italian mathematician and computer scientist, created Petri Nets[66]. It is especially useful for modeling systems in which events can occur in any order and at any time, and in which event interactions are complex. The Petri Net is comprised of compilation of locations, transitions, and arcs. Places represent the current state of the system, transitions represent potential future events, and arcs represent the requirements that must be fulfilled before an event can occur. A Petri Net is typically depicted in the form of a directed graph, where the circle represents place, the bar represents transition, and the arc links place and transition. These three are considered to be in a static state, whereas the token in the location is said to be in a dynamic state [67]-[72].The occurrence of an event triggers the transition and moves the token to a new location. Fig (5.2a) and (5.2b) shows the transformation of fault tree to Petri Net when AND / OR gate is used.

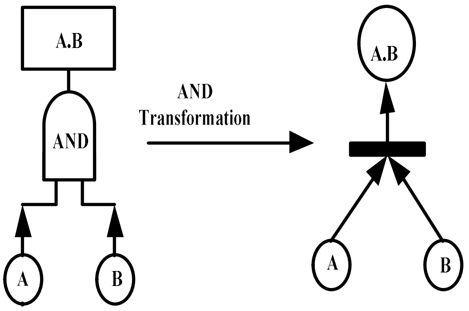


Fig.5.2a: Transformation of Fault Tree (AND) to PN

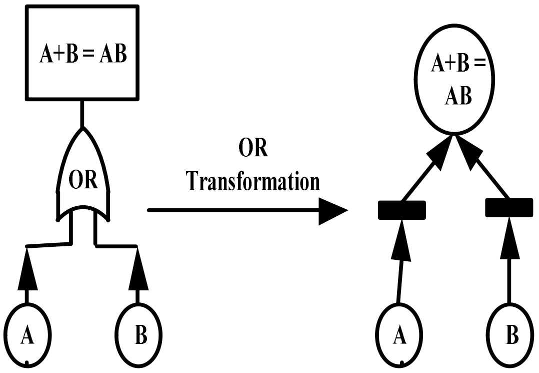


Fig.5.2b: Transformation of Fault Tree (OR) to PN

Petri Net has the potential to assess the risk and reliability of PMU failure rate and repair rate of modules are defined by the manufacturer. It can be used to assess the dependability of a PMU to cater its functions. Fig. 5.3 shows the transformed Petri Net of PMU from its fault tree model (Fig.5.1)

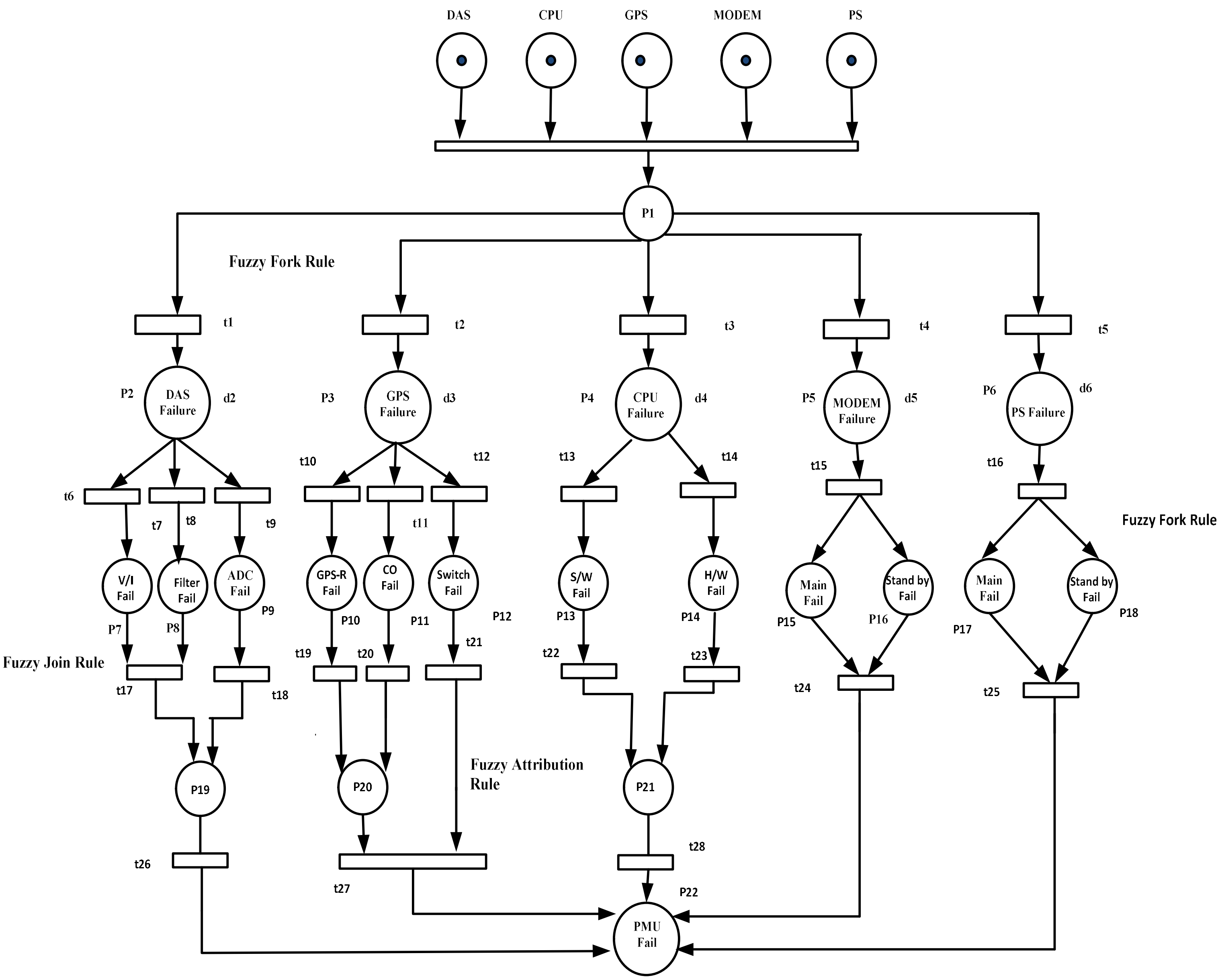


Fig.5.3: Petri Net diagram transformed from fault tree diagram of PMU

Reachability is a way of representing the states of Petri Nets. In the reachability graph of a Petri Net, nodes correspond to reachable markings and edges corresponding to the relation[73]-[75].

The mathematical property known as reachability is an essential component of Petri Nets (PN). By focusing on the behaviour of individual nodes, it examines how different sequences of events develop from the starting point to the future reachability state. Reachability analysis is beneficial because it avoids the need to examine the complete system and provides concurrency guarantee in a distributed system[76]-[78]. It is possible to build the reachability graph using an iterative process, beginning with the initial marking and adding for each reachable mark. The arcs represent the flow of information from one component to another, and the weights indicate the level of uncertainty or imprecision that is associated with the information [76].Let us assume that Q is a transition system that contains the relation T. Then, Q_0 and Q_1 for the transition (Q_0, Q_1) T; that is to say, there is a transition between Q_0 and Q_1. A state can be reached from a state Q_0 in n steps if there is a sequence of states Q_1,..., Q_n such that Q_n = Q and Q_0 Q_1... Q_n 0 steps. In other words, a state can be reached from Q_0 in n steps if and only if Qn = Q. The information that is gleaned via reachability computation also takes into account the behaviour of the system as it transit [79].

5.4. FUZZY PETRI - NET STRUCTURE

A Fuzzy-Petri Net (FPN) is an extension of the basic Petri Net that permits modeling of systems with uncertain or imperfect data. FPN can be utilized to assess the dynamic reliability/availability of a PMU when repair rate and failure rate are uncertain. Utilizing fuzzy sets, the communication that takes place between the PMU and the other components of the system can be represented by Fuzzy-Petri Net (FPN) diagram. A concept known as a fuzzy set, which also permits partial membership in a set, can be utilized to provide an accurate description of the ambiguity inherent in data. The failure rate of a GPS receiver could be represented as a fuzzy set, with values ranging from "low" to "high" and degrees of membership ranging from 0 to 1. By combining the characteristics of fuzzy sets and fuzzy rules with the structure of a Petri Net, it is possible to simulate complex systems that include input that is either uncertain or wrong. Fuzzy Petri Nets are based on probabilistic inference. The Fuzzy Petri Net (FPN) is conditional rule based system for reasoning. Transitions represent the rules and firing of transition is controlled by truthiness of rule. Each conditional rule is assigned the fuzzy membership value, called certainty factor and lie between 0 and 1.This certainty factor shows the strength in the rule. The transformation of mark from places to transitions and vice versa is represented by directed arcs. A generalized FPN structure can be defined as an 8-tuple [80]-[82]:

$$\text{FPN} = (P, T, \vartheta, I, O, \gamma, \delta, \theta) \tag{5.1}$$

where

$P = \{P_1, P_2, \ldots, P_n\}$ is a finite set of places

$T = \{t_1, t_2, \ldots, t_m\}$ is a finite set of transitions

$\vartheta = \{\vartheta_1, \vartheta_2 \ldots, \vartheta n\}$ is a finite set of propositions

$P \cap T \cap \vartheta = \emptyset; |P| = |\vartheta|$ (5.2)

I: $P \text{ x } T \rightarrow \{0, 1\}$ is the input function, a mapping from places to transitions

O: $T \text{ x } P \rightarrow \{0, 1\}$ is the output function, a mapping from transitions to places

$\gamma = T \rightarrow \{0, 1\}$ is an association function, a mapping from transitions to place [0, 1] i.e. the certainty factor

$\delta : P \rightarrow \{0, 1\}$ is an association function, a mapping from places to [0, 1] i.e. the truth degree value

$\theta : P \rightarrow$ is an association function, a mapping from places to propositions.

Transition is represented in the transformation process by each rule's corresponding membership value. The input position indicates the antecedent, while the output transition represents the response based on the degree of truthiness. As soon as a transition is triggered in FPN, the output takes on the same truthiness value as the input. In reasoning Fuzzy Petri Net, a token is the truth degree of an event or objective between zero and one and not an object. Consequently, a location cannot possess more than one token. Since there is no material object, there is no resource concept. Multiple principles may share the same proposition. The Fuzzy degree of truth propagates according to the laws of logic. The degree of veracity at the location will not diminish as propositions spread. This is the primary distinction between the Petri Net model and the Fuzzy Petri Net model. A transition is triggered if all of its inputs have a true degree that is equal to or greater than the threshold value. The structure of a Fuzzy Petri Net inference system is depicted in Fig.5.4.

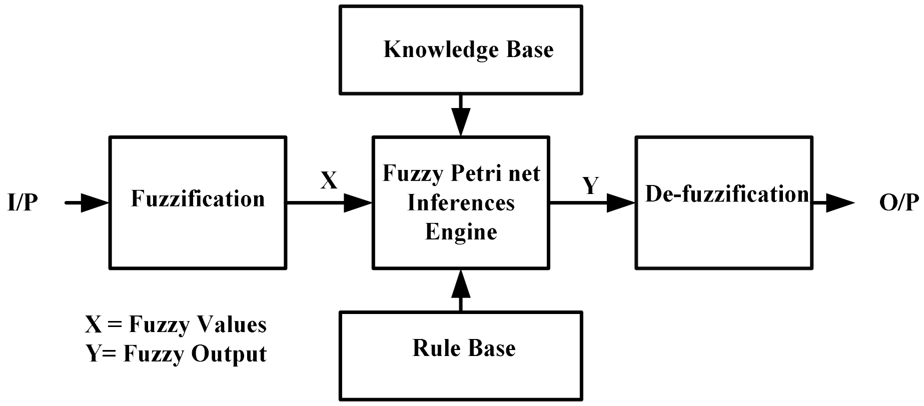


Fig.5.4: Fuzzy Petri Net Structure for PMU

5.4.1. Composite Fuzzy Production Rules

Composite fuzzy production rules (CFPRs) are a form of fuzzy logic system used in uncertain or complex environments for decision-making. Petri Nets are a graphical modelling tool for describing systems with discrete events and states. It is possible to model and control complex systems with ambiguous or imprecise inputs and outputs by combining CFPRs and Petri Nets. These can be represented as a set of principles that determine the firing of Petri Net transitions in the context of Petri Nets. Each rule is composed of an antecedent and a consequent, where the antecedent specifies a condition that must be met for the rule to be applied, and the consequent specifies the transition or transitions that should be executed if the rule is applied [83]. Both the antecedent and the consequence can be fuzzy sets, allowing for fuzzy reasoning and decision-making.

To implement CFPRs in Petri Nets, each transition in the Net must be accompanied by a set of rules. When the conditions specified in a rule are satisfied, the corresponding transition is triggered, changing the system's state. A fuzzy operator, such as the minimum or maximum operator, can be used to combine the principles associated with each transition that is used to determine the degree of certainty then the transition will be executed. CFPRs are a type of fuzzy logic system that integrates fuzzy sets and production rules to deal with imprecise or uncertain data. In lieu of the traditional binary representation of a proposition as either true or false, fuzzy sets permit the representation of degrees of membership. In contrast, production rules are a set of IF-THEN statements that specify the conditions under which certain actions should be performed [84]. By combining CFPRs and Petri Nets, a system can be generated that can reason and make decisions based on ambiguous information. Using CFPRs in Petri Nets requires the definition of fuzzy sets for the system's input variables and output variables, as well as the rules that specify how the input variables should be transferred to the output variables.

The combination of CFPRs and Petri Nets offers a potent modelling and control tool for complex systems with indeterminate or imprecise inputs and outputs. CFPRs in Petri Nets can enhance the performance and dependability of a vast array of systems and applications by facilitating more efficient and effective decision-making.

Fuzzy production rule is the inference mechanism for the transformation of input/s to output/s, once the transition fires. Firing of transition occurs if the input value [0, 1] is more than threshold value. Reachability characterization of Fuzzy Petri Net enables the input data set to the next node/ place. Rules are the expression of knowledge in Fuzzy logic. Based on the input / output and transition structure in FPN model, If – Then rule/s are applied. The following rules are used for developing the Network topology [85].

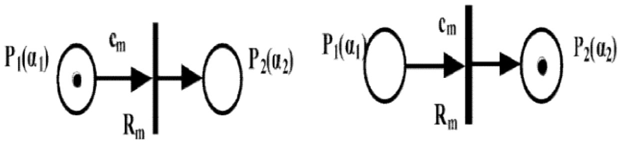
➢ The firing of transition sends the token to the next place shown in Fig.5.5

$R_m(c_m) : P_1(\alpha_1) \rightarrow P_2(\alpha_2)$; where $\alpha_2 = \alpha_1 * c_m$ (5.3)

α is the truth degree of antecedent/consequent (P_i)

c_m and is called certainty factor

R_m is Fuzzy rule.



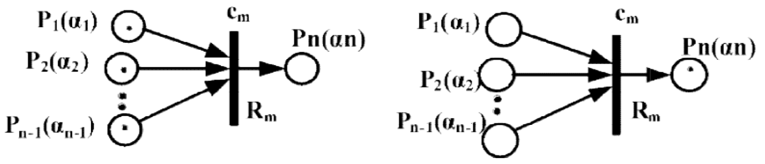
(a) Before Firing (b) After Firing

Fig.5.5: Fuzzy Production Rules (P_1, P_2)

➢ Multiple places arced to one transition (AND gate representing in fault tree model, the output value will be minimum of the inputs as shown in Fig. 5.6.

$R_m(c_m) : P_1(\alpha_1) \wedge P_2(\alpha_2) \wedge \ldots\ldots\ldots P_{n-1}(\alpha_{n-1}) \rightarrow P_n(\alpha_n)$ (5.4)

$\alpha_n = \min\{\alpha_1, \alpha_2 \ldots\ldots\ldots\ldots\ldots, \alpha_{n-1}\} * c_m$ (5.5)



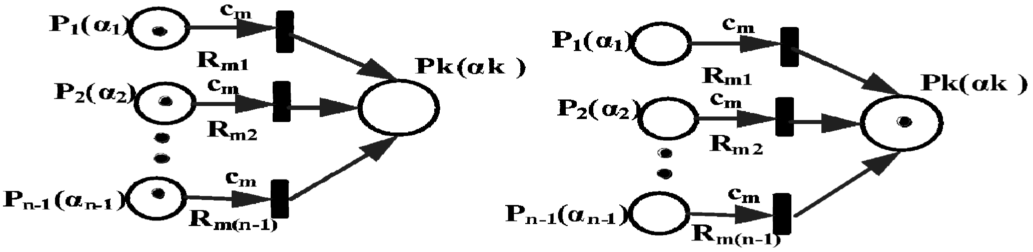
(a). Before Firing (b) After Firing

Fig.5.6: Fuzzy Join Rule (P_1, P_2 AND P_3)

➢ Multiple places arced to multiple transitions (OR gate represented in fault tree model) the output value will be maximum of the inputs as shown in Fig.5.7.

$$R_m(c_m) : P_1(\alpha_1) \vee P_2(\alpha_2)\vee\ldots\ldots\ldots\vee P_{n-1}(\alpha_{n-1})\rightarrow P_n(\alpha_n) \quad (5.6)$$

$$\alpha_n= \max\{\alpha_1, \alpha_2\ldots\ldots\ldots\ldots\ldots,\alpha_{n-1}\}* c_m \quad (5.7)$$



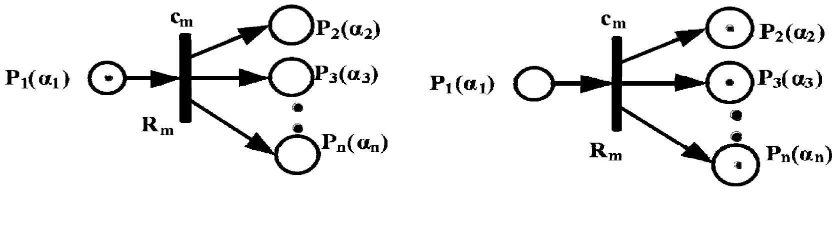
(a). Before Firing (b) After Firing

Fig.5.7: Fuzzy Attribution Rule (P_1 OR P_2 P_k)

➢ One place to multiple places through a single transition shown in Fig.5.8.

$$R_m(c_m) : P_1(\alpha_1) \rightarrow P_2(\alpha_2)=\ldots\ldots\ldots=P_{n-1}(\alpha_{n-1})=P_n(\alpha_n) \quad (5.8)$$

$$\alpha_2 =\alpha_1 * c_m ,\alpha_3=\alpha_1 * c_{m,}\ldots\ldots, \alpha_n=\alpha_1 * c_m \quad (5.9)$$



(a). Before Firing (b) After Firing

Fig.5.8: Fuzzy Fork Rule (P_1 P_2 AND P_3)

In Fuzzy logic theory, the probability of an event is specified by the degree of truthiness, whereas in the Fault Tree Model of PMU, if the degree of truthiness is high, the unit will be out of service. Truth degrees determine the probabilities of fuzzy events. A greater value indicates that the event will be rendered inoperable more quickly. During subsequent iterations, the flaw propagates upward. The mapping of a fault tree to a fuzzy reasoning Petri Net model is depicted in Fig. 5.3.

5.5 FUZZY PETRI NET (FPN) BASED SPROUTING TREE ALGORITHM(STA)

Petri Nets are mathematical models used to represent and analyse concurrent systems, and the Sprouting Tree Algorithm(STA) is a technique for analysing them. STA is used to generate a Petri Net's state space representation. The STA commences with an initial marking of the Petri Net, which represents the system's initial state. The system then employs a set of rules to generate a set of successor markings that represent the potential states the system can reach from its initial state. The STA applies these rules to each succeeding marking until no additional markings can be generated[86]-[89]. The Sprouting Tree Algorithm uses the following rules:

- Execute the transition and generate a new marking for each enabled transition in the current marking.
- If a new marking has already been created, it should not be created again.
- If a new marking is produced, it should be added to the list of successor markings.
- If a new marking is generated, its successors should be generated using the same principles.

The STA generates a tree structure, with each node representing a mark and each edge representing the transitions that were executed to reach the next mark. Fuzzy Petri Nets (FPN) are a form of Petri Net that enables the modelling and analysis of uncertain and imprecise complex systems. Commonly used to tackle optimisation problems, the Sprouting Tree Algorithm (STA) is a heuristic search Algorithm. FPN-based STA is a hybrid method that incorporates the benefits of FPN and STA to solve optimisation problems involving uncertain or imprecise data. The Sprouting Tree Algorithm is used to find the optimal solution to an optimisation problem. STA begins with an initial solution and refines it iteratively.

FPN-based STA has a number of advantages over conventional STA methods. In the first place, it permits the modelling of uncertainty and imprecision in the optimisation problem, which is typical of real-world applications. Second, it enables the use of fuzzy logic operators to evaluate the degree of suitability of candidate solutions which result in a more robust and adaptable evaluation mechanism. Lastly, it enables the incorporation of domain-specific knowledge and expert opinions into the optimisation process, which can result in improved outcomes.

The information transit path in a sprouting tree is governed by logic. The production of successive node paths is condition and threshold value dependent. FPN is a dynamic Network based on logic rules. It is the optimal method for designing and developing the sprouting tree Algorithm. The sprouting tree demonstrates the fuzzy reasoning Algorithm and the Petri Net topology. Each sprouting tree node is represented by the 3-tuple (P, Pk, IRS(Pk)), where Pk , P and IRS(Pk) is the immediate reachability set(IRS) of Pk.

> (i) Only one transition is executed at a time, corresponding to a single token at a single location. (The degree of output = confidence value of input site x certainty factor of transition).
>
> Multiple places arced to one transition (AND gate), minimum value of (P2(2), P3(2),...., Pn-1(2); where (2=3 =n-1=confidence value of input place * certainty factor of transition). If multiple places arced to multiple transitions (OR gate), then maximum value is obtained.

Using eqn. (5.10), the degrees of truth of propositions are derived from the sprouting tree.

Certainty factor (Cm) and threshold value (β) indicates the dependability and stability of each node. Greater the assurance factor, the stronger the connection between successive nodes and the root node. If the degree of reliability (P_i) of location (P_i) exceeds the threshold value (β), the transition is triggered, and the token is moved from the (P_i) node to the (P_j) node, where (P_j) = (P_i)*C_m.

If α (P_j) <β, (P_i) does not pass the token to (P_j)node. Since the route is unstable and unreliable for a brief period of time. The root node must abandon this route and search for an alternative stable route. Let Q represent the set of successful nodes.

Then

$$Q=\{[Q_j,\gamma_1,IRS(Q_j)], [Q_j,\gamma_2,IRS(Q_j)],\ldots,.[Q_j,\gamma_m,IRS(Q_j)] \tag{5.10}$$

where $\gamma_m \in [0, 1]$ and $1\leq i \leq m$.

The degree of truth of proposition, z is given by eqn.(5.11).

$$z = \text{Max }(\gamma_1, \gamma_2 \ldots\ldots\ldots.\gamma_m) \tag{5.11}$$

5.6 FLOW DIAGRAM FOR SPROUTING TREE DEVELOPMENT

Flow diagram is a formalized graphic representation of logic sequences, for quick and easy development of the Algorithm. Fig. 5.9 presents the flow chart for the development of sprouting trees. Initially the root node, (Q_s) which is also known as starting node is considered. Also, the degree of truthiness of proposition (z) is used as input value. The purpose of the computation is to get a success node which shall be terminating in nature. The immediate reachable set (IRS) helps to determine nature of node as terminating or non-terminating. The true degree determines the fuzzy possibility of the events.

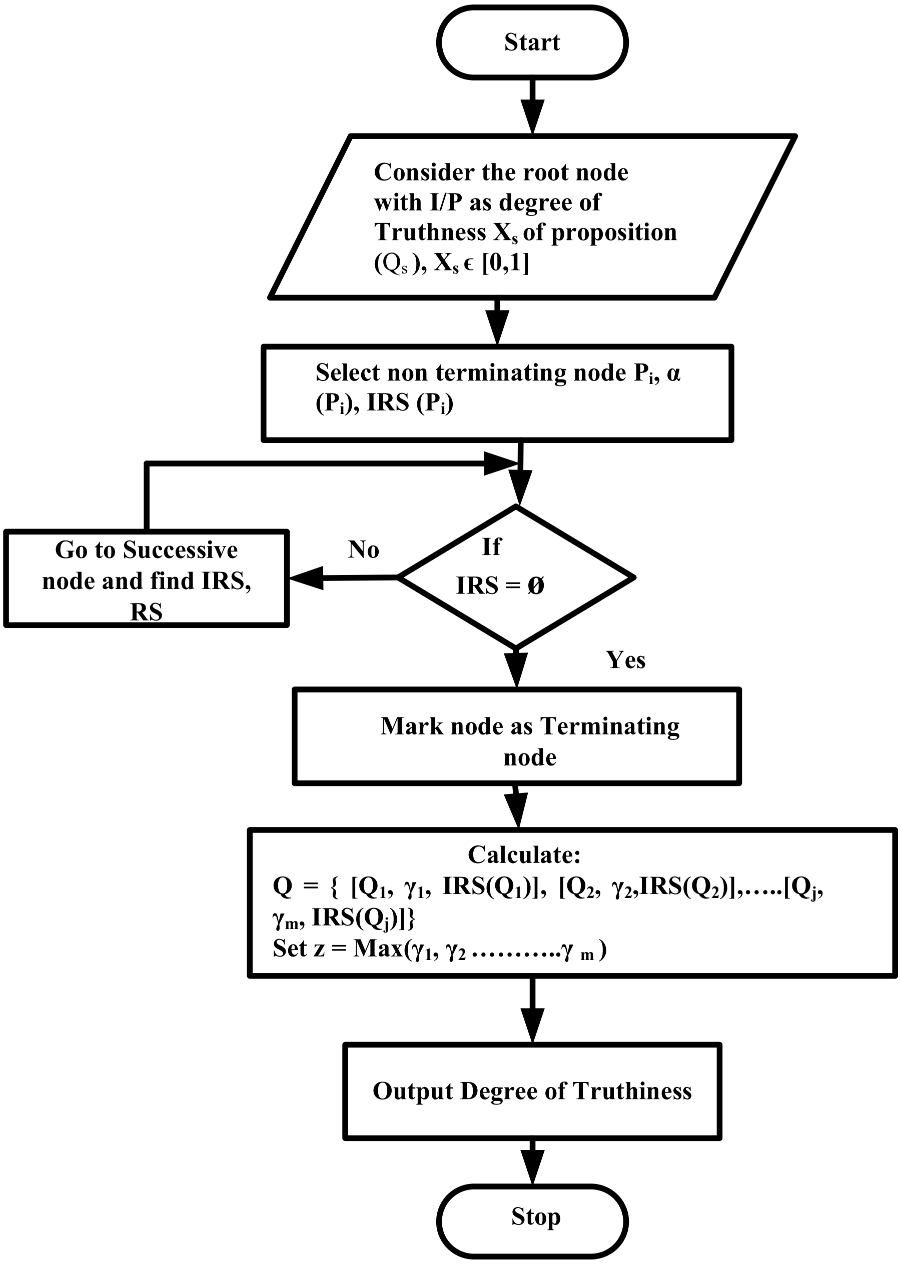

Start
Consider the root node with I/P as degree of Truthness X_s of proposition (Q_s), $X_s \in [0,1]$
Select non terminating node P_i, α (P_i), IRS (P_i)
Go to Successive node and find IRS, RS
No
If IRS = Ø
Yes
Mark node as Terminating node
Calculate:
Q = { [Q_1, γ_1, IRS(Q_1)], [Q_2, γ_2,IRS(Q_2)],.....[Q_j, γ_m, IRS(Q_j)]}
Set z = Max(γ_1, γ_2..........γ_m)
Output Degree of Truthiness
Stop

Fig.5.9: Flow chart for development of Sprouting Tree

5.7 IMPLEMENTATION OF FPN TO PMU

In this section marked FPN model of PMU has been developed and is used to evaluate the reliability of a PMU whose failure rate (Appendix. A) is known. In the present analysis, we assumed that the certainty factor (C_m between [0, 1]) is the failure rate-based availability of PMU which also satisfies the requirements for the Fuzzy Petri Net attribute. The Fault tree of PMU, depicted in Fig. 5.1, is converted to the Marked Fuzzy Petri Net diagram depicted in Fig. 5.10. Let d_1, d_2,d_3…………,d_{22} are propositions.

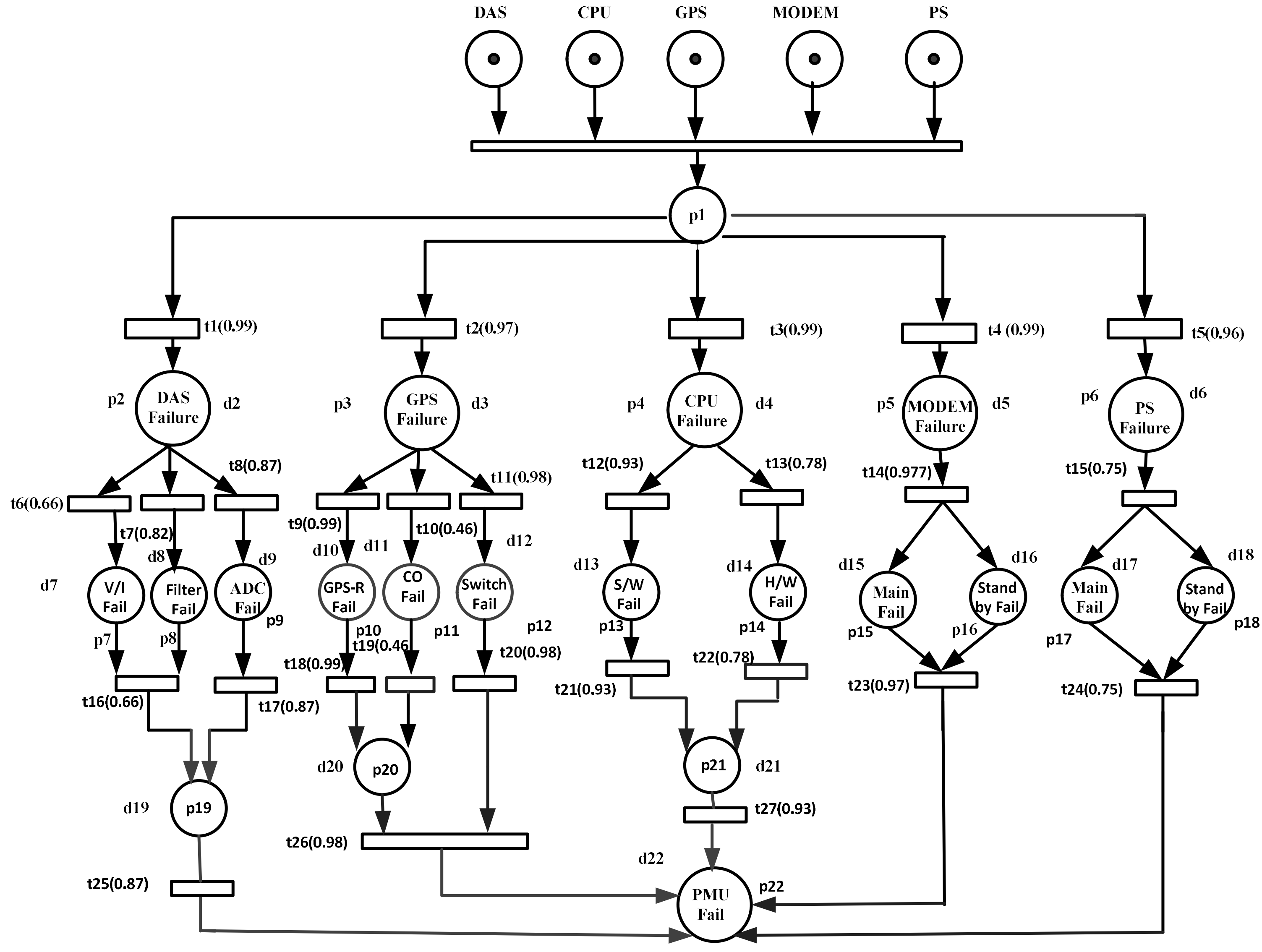


Fig.5.10: Marked Fuzzy Petri Net diagram for PMU

Using Marked FPN model is depicted in Fig. 5.10, the following fuzzy production principles are derived.

Fuzzy Production Rules:

R_1: IF d_1 Then d_2($C_m = 0.99$)

R_2: IF d_1 Then d_3(C_m = 0.97)

R_3: IF d_1 Then d_4(C_m = 0.99)

R_4: IF d_1 Then d_5(C_m = 0.99)

R_5: IF d_1 Then d_6(C_m = 0.96)

R_6: IF d_2 Then d_7(C_m = 0.66)

R_7: IF d_2 Then d_8(C_m = 0.82)

R_8: IF d_2 Then d_9(C_m = 0.87)

R_9: IF d_7 and d_8 ORd_9Then d_{19}(C_m = 0.87)

R_{10}: IF d_{19} Then d_{22}(C_m = 0.81)

R_{11}: IF d_3 Then d_{10} (C_m = 0.99)

R_{12}: IF d_3 Then d_{11} (C_m = 0.98)

R_{13}: IF d_3 Then d_{12}(C_m = 0.98)

R_{14}: IF d_4 Then d_{13} (C_m = 0.93)

R_{15}: IF d_4 Then d_{14}(C_m = 0.78)

R_{16}: IF d_5 Then d_{15} andd_{16} (C_m = 0.97)

R_{17}: IF d_6 Then d_{17} andd_{18} (C_m = 0.75)

R_{18}: IF d_{10} OR $d_{11}$and d_{12}then d_{20} (C_m = 0.98)

R_{19}: IF d_{13} OR d_{14}Then d_{21}(C_m = 0.93)

R_{20}: IF d_{21} Then d_{22}(C_m =0.93)

R_{21}: IF $d_{15}$and d_{16}Then $d_{22(}$$C_m$ = 0.97)

R_{22}: IF $d_{17}$and d_{18}ORd_9Then $d_{22(}$$C_m$ = 0.75)

The immediate Reachability set (IRS) and the successive Reachability set (RS) nodes for all places are evaluated based on the starting place (node) and also shown in Fig. 5.10 Table–5.1 presents the nodes involved in IRS and RS during progression of PMU failure information.

Table – 5.1: Immediate Reachability Set (IRS) and the successive Reachability Set (RS)

Place(P_i)	IRS(P_i)	RS (P_i)
P_1	{P_2, P_3 ,P_4 ,P_5 ,P_6}	{ P_2,…………..,P_{22}}
P_2	{ P_7, P_8, P_9}	{ P_7, P_8, P_9, P_{19} , P_{22}}
P_3	{ P_{10}, P_{11}, P_{12}}	{ P_{10}, P_{11}, P_{12}, P_{19} , P_{20} }
P_4	{ P_{13}, P_{14}}	{ P_{13}, P_{14}, P_{21} , P_{22} }
P_5	{ P_{15}, P_{16}}	{ P_{15}, P_{16}, P_{22} }
P_6	{ P_{17}, P_{18}}	{ P_{17}, P_{18}, P_{22}}
P_7	{ P_{19} }	{ P_{19} , P_{22}}
P_8	{ P_{19} }	{ P_{19} , P_{22}}
P_9	{ P_{19} }	{ P_{19} , P_{22}}
P_{10}	{ P_{20},}	{ P_{20}, P_{22}}
P_{11}	{ P_{20},}	{ P_{20}, P_{22}}
P_{12}	{ P_{20},}	{ P_{20}, P_{22}}
P_{13}	{ P_{21}}	{ P_{21},P_{20}}
P_{14}	{ P_{21}}	{ P_{21},P_{20}}
P_{15}	{ P_{22}}	{ P_{22}}
P_{16}	{ P_{22}}	{ P_{22}}

P_{17}	{ P_{22}}	{ P_{22}}
P_{18}	{ P_{22}}	{ P_{22}}
P_{19}	{ P_{22}}	{ P_{22}}
P_{20}	{ P_{22}}	{ P_{22}}
P_{21}	{ P_{22}}	{ P_{22}}
P_{22}	Ø	Ø

Based on the starting place (P_1) which is assumed with a degree of truthiness as 0.85 (given by knowledge base of the expert). Here the threshold value β = 0.25(assumed). The IRS starting place P_1 is P_2, P_3, P4, P_5 and P_6. The successive node is explored which is non-terminating. The value of γ_i (P_i) is evaluated using eqn. (5.5). For P_2 place, γ_2 = 0.85 x 0.99 is computed and similarly value of γ_3= 0.82, γ_4 = 0.84, γ_5 = 0.84, γ_6 = 0.81 are computed for P_3,P_4, P_5 and P_6 .Place P_{20} is the terminating node Thus, terminating nodes, Q and the degree of truth of proposition, z are found out using eqn. (5.9) and (5.10) as below.

$$Q=\{(P_{19},0.44,P_{22}),(P_{19},0.55,P_{22}),(P_{19},0.59,P_{22}).(P_{20},0.79,P_{22}),(P_{22},0.45,P_{22}),$$

$$(P_{20},0.80,P_{22}),(P_{13},0.78,P_{22}),(P_{14},0.65,P_{22}),(P_{15},0.81,P_{22}), (P_{16},0.81,P_{22}),$$

$$(P_{17},0.60,P_{22}), (P_{18},0.60,P_{22})\} \quad (5.12)$$

$$z = \mathrm{Max}[(0.44, 0.55, 0.59, 0.79, 0.45, 0.80, 0.78, 0.65, 0.81, 0.81, 0.60, 0.60)] \quad (5.13)$$

$$z = 0.81 \quad (5.14)$$

So the degree of truth of proposition is 0.81 for PMU module which gives the reliability of PMU.

Using Table – 5.1 and Fuzzy production rules, the sprouting tree is drawn, shown in Fig.5.11. In order to conform the results of reliability obtained using sprouting Algorithm, the reliability of PMU is also computed using Markov model [20], reproduced in Table: 5.2 below.

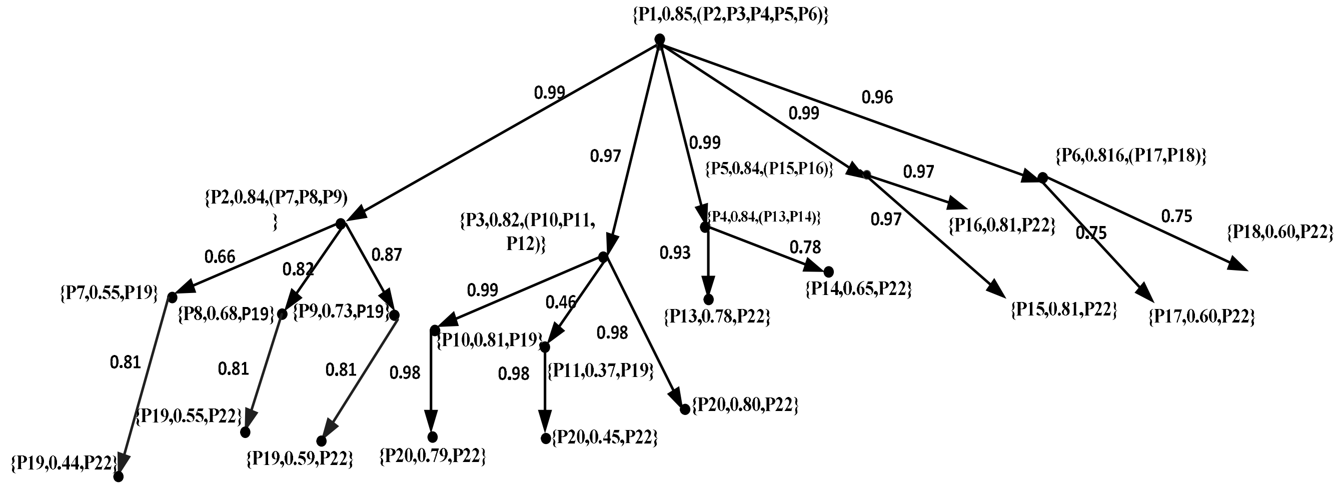


Fig.5.11: Sprouting Tree of PMU

Table 5.2: Reliability indices of PMU using Markov model

Modules	**Availability**	**Unavailability**	**Reliability**
Transducer	0.99838	3.7912x 10^{-7}	0.93424
Anti-alias filter	0.99998	1.232x 10^{-7}	0.983718
A/D convertor	0.99994	9.9637x10^{-8}	0.991274
CPU	0.99902	0.00097461	0.99245
GPS	0.999306	6.932 x10^{-4}	0.976008
MODEM	0.99999	1.693610^{-12}	0.99974
Power supply	0.999246	5.47206 x10^{-7}	0.968433
PMU	0.998332	0.001668	0.85388

It is observed that the availability of PMU by sprouting tree method and Markov model is nearly the same. However, the sprouting tree provides the information path from operating state to unavailability mode of PMU. This helps the designer to improve the design of PMU by pin pointing the module weakness. The reliability of PMU increases if the repair rates of the PMU module are also considered, since the failure rate of system decreases.

5.8 RESULTS AND DISCUSSIONS

Fuzzy reasoning associated Petri Net presents a graphical and mathematical method for risk modeling and reasoning. The possible failure causes are shown by places and firing of transitions by rules. Fuzzy logic Algorithm processes the assessment of rules. The case study of PMUs sprouting trees using Fuzzy Petri Net method is able to transform expert knowledge into rule base and has been able to trace the failure rate of different modules. The hierarchal structure has made the calculations flexible by dividing the Net into various sub Nets. The input place is the second hierarchy indicating the signs of module failures, which cannot be eliminated directly, but can be observed. Consider the diagnosis rules ($P_1 \rightarrow P_2 \rightarrow P_{9\ldots\ldots\ldots} \rightarrow P_{22)}$, the failure of ADC ($P_9$) causes Data Acquisition failure, resulting in PMU failure. The GPS receiver (P_{10}) failure doesn’t cause failure of PMU. It enables the crystal oscillator/switch to standby mode. The failure of both GPS receiver and Functional switch/ crystal oscillator (CO) causes PMU failure.

The failure of any one of the constituents (software or Hardware) in CPU causes failure of PMU. MODEM causes failure to PMU, if both Main (P_{15}) and standby (P_{16}) modules fail. Similarly, the failure of both main ($P_{17)}$and standby (P_{18}) of power cause PMU to fail. From sprouting tree shown in Fig. 5.11 the degree of truth of proposition is derived and is found to be 0.81.

5.9 CONCLUSION

The study presented in this chapter gives insight to the design and system engineer about the flow of failure mode of PMU modules. It assesses the risk of non-availability of PMU at any time which is based on the failure rate of its components. The dynamics of failure is considered as an event in the Petri Net and its uncertainty is dealt with Fuzzy logic reasoning. Sprouting tree, a logical structural path, is developed using fusion of Fuzzy reasoning and Petri Net technology. This study is important for the system designer of PMU and for smart grid implementation. The overall benefits of the methodology include: (i) Visual tool in communicating and supporting decisions based on the analysis and to determine the adequacy of PMU design, (ii) Ability to model and deal with highly complex systems, (iii) Ability to involve multiple experts and (iv) Improve handling of uncertainties and possibilities.

CHAPTER - VI
PMU DATA TRANSFER SECURITY USING BLOCKCHAIN

6.1. INTRODUCTION

Phasor Measurement Unit is a synchronous phasor device and is employed to monitor and regulate electrical parameters including active and passive power transferred over transmission lines, phase angle, etc. It is the eye and ear of power systems, since their real-time data obtained from PMU enables system operators to immediately detect and respond to disturbances and events that could result in blackouts and other interruptions. Yet, the collection and analysis of this real-time data raises a variety of data security concerns that must be addressed to maintain the data's availability, confidentiality, and integrity. The possibility of cyber assaults on PMUs data set and its associated communication network faces a significant drawback. Power system operators can maintain the dependability and resilience of their systems in the face of cyber threats and other dangers by installing proper security measures

In PMU, the measured dataset is transferred to power distribution center(PDC) / control center employing IEEE C37.118 standard protocol, however, this communication protocol lacks encryption [90], and hence it is vulnerable to cyber-attacks. The work in this chapter has addressed the issue of data security of PMU and attempted to study the integration of PMU with Blockchain technology to provide cyber security and confidentiality.

For secure movement of unique parametric values (such as power, voltage, current, frequency, money, and identification credentials) across the internet, Blockchain technology is used. Rather than storing the data on a server, each member of the distributed network (peer) can keep a copy of Blockchain on their own computer. When additional blocks are validated and linked to the chain, the chain of data records continuously grows. Cryptographic hashing algorithms checks the legitimacy of each block in the chain. Blockchain technology improves data security in PMUs by providing a decentralised and transparent platform for data storage and transfer [90]-[95].

The Blockchain is built on a peer-to-peer network. Therefore, to use Blockchain technology and to include its advantages in a synchrophasor network, it can be employed in decentralized communication architecture. Some consensus techniques allow the system to agree on changes in the ledger. The main focus of this chapter is to develop a distributed and scalable data model for the sharing of power information collected from various PMUs during the transport and distributions of power. Table- 6.1 presents the difference between Blockchain and databases [96]-[98].

Table 6.1: Main difference between Blockchain and databases.

Database	Blockchain
Centralized	Decentralized
Permission	Permission-less
Require administrator	No administrator

This chapter covers:

(i) Monitoring and simulation of tie – line power exchange between two utilities / grids.

(ii) Monitoring and simulation of power generation by photo voltaic power plant.

6.2. PROBLEM FORMATION

The phasor measurement unit (PMU) is a smart transducer that can collect data and send it to any medium in smart grids. But this process is vulnerable to data discretion and security breaches. This needs Blockchain analysis, on collected data from various sources through PMU, and hence provides a decentralized and secure system. The data so collected and transmitted to concerned needs to be secured and any discrepancy in data should be immediately highlighted. This requires a distributed, transparent system and an algorithm which can check the discrepancy of data captured and transmitted. It identifies the role of Blockchain technology in PMU and also validates its data transfer security role as a trust model to sort out the discrepancy about exchange of electrical power between two utilities or utility and consumers. The technique develops a distributed and scalable data model, based on the Blockchain which can be implemented using a heterogeneous set of Azure SQL database management systems, hosted on the AWS cloud. Fig.6.1 shows the complete architecture of the system viz. PMU embedded Blockchain technology. Data from PMU can be modulated with Blockchain to add cryptography.

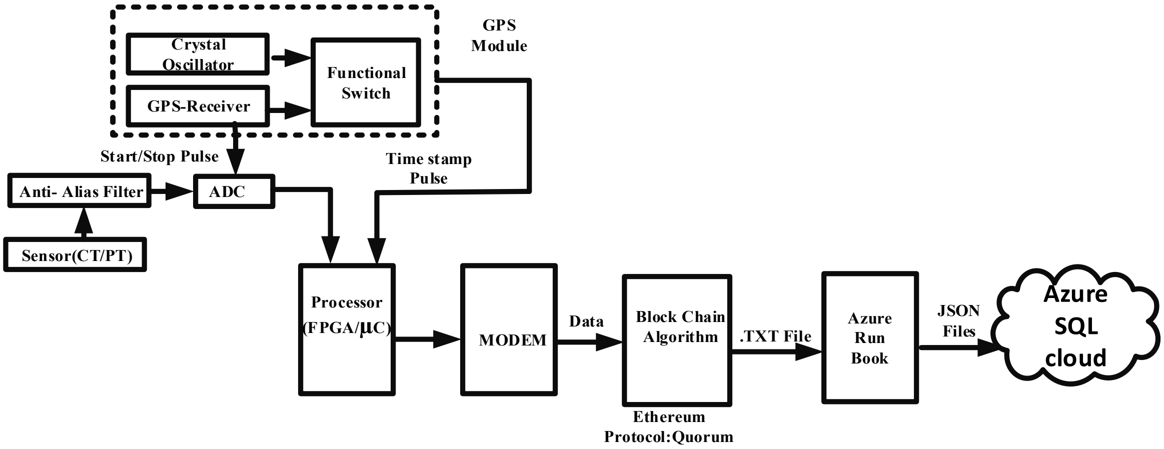


Fig.6.1: Blockchain Algorithm embedded PMU

6.3. DATA SECURITY

The process of safeguarding information against unauthorized access or use disclosure is referred to as data security. The proliferation of digital data storage in recent years, in conjunction with an increase in the incidence of cyber-attacks, has led to an increase in the significance of data security. The term "data security" refers to the collection of protocols that is put into place to prevent unauthorized access, use, disclosure, or deletion of data [99]. This involves safeguarding the data while it is being stored and transferred. The purpose of data security is to ensure that data is protected from unauthorized access, integrity is preserved, and that they are available when needed. To maintain data confidentiality only systems that have been granted permission to do so can access the information. Integrity refers to the fact that the data is correct and has not been altered in any way. When something is available, it is readily available for use whenever it is required [100]-[102].

Data is a valuable asset that can be put to a number of different uses, including research, analysis, and the formulation of decisions. Further, datasets may include sensitive or confidential information, such as personal identity information, financial information, or intellectual property. Some of the ideas and procedures that are utilized in order to ensure the safety of the data.

- The first idea is known as access control: it is the method of restricting access of data so that it can only be viewed by authorized system. Several methods, including authentication, authorization, and encryption, can be utilized to accomplish this goal. Authentication is the process of confirming the identity of the user or system that is attempting to access the data [103]. The data that a user or system is permitted to access is determined by their authorization status. The process of turning data into a format that is not readable and that can only be deciphered with the use of a key or password is referred to as encryption.
- The second idea is known as data backup and recovery: it describes the procedure of making copies of data and keeping them in a safe place [104]. This makes it possible to recover data in the case of a catastrophe, such as a hacker attack or a natural disaster. It is important to do frequent tests on your backup and recovery systems to ensure that they are in good operating order.
- The third principle is known as network security: it describes the precautions that are taken to prevent unauthorized access to, or assaults on, a network's underlying architecture. Included in this category is the utilization of intrusion detection systems, firewalls, and antivirus software. In order to prevent unauthorized users from accessing the network, firewalls are utilized. The purpose of intrusion detection systems is to monitor a network for any suspicious behaviour and take appropriate action. Malware can be located and removed with the assistance of antivirus software [105]-[107].
- The fourth idea is known as physical security: it relates to the precautions that are taken to safeguard the actual hardware that is used to store or transfer data. This includes securing servers and other equipment in locked rooms or cabinets and utilizing biometric authentication methods to prevent physical access to the devices [108]-[110].
- The fifth idea is "training and awareness": it relates to the process of educating workers and users about the most effective methods for maintaining data security. Training on how to manage passwords, avoid falling for phishing scams, and other typical security dangers are included in this. In addition to this, users should be made aware of their roles and responsibilities in the process of keeping data security [111]-[113]. Cloud computing is one of the best methods used to store big data. Thus making it an efficient technique to reliably store the data.

6.4. CLOUD COMPUTING

Cloud computing deals with hosted services by third party such as access to software, data storage, computing power, etc. without any liability for maintenance or updates of software and hardware. It provides various on-line services whereas Blockchain technology offers a structural ledger data base for storing transactional data called blocks and links them with numerous data bases called as chain. Data cannot always be tamper free on the cloud and does not assure complete integrity. It can enable Blockchain technology based projects, though it has centralized structure of data fetching. Cloud is visible or hidden but Blockchain has transparency. Some important advantage and disadvantage for cloud computing are presented in Table - 6.2 below [114].

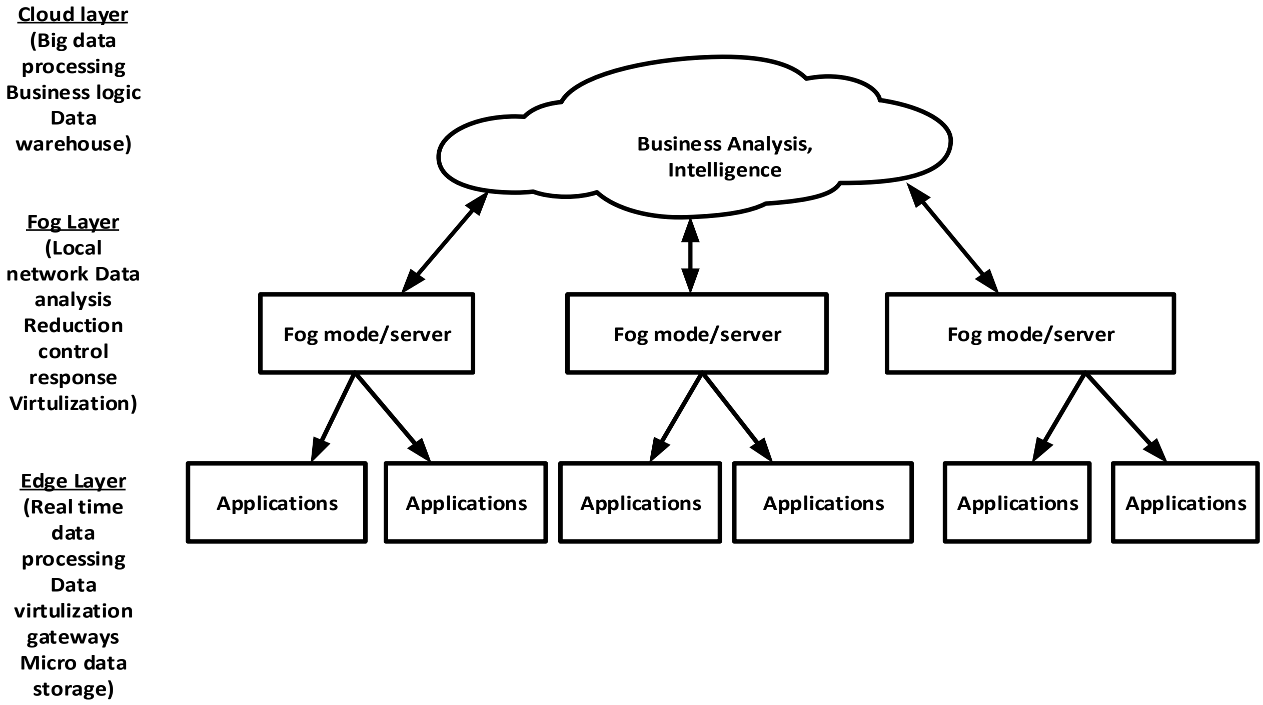

Cloud layer
(Big data processing Business logic Data warehouse)
Fog Layer
(Local network Data analysis Reduction control response Virtulization)
Edge Layer
(Real time data processing Data virtulization gateways Micro data storage)
Business Analysis, Intelligence
Fog mode/server
Fog mode/server
Fog mode/server
Applications
Applications
Applications
Applications
Applications
Applications

Fig.6.2: Line Diagram of IOT- Cloud Layer Function

Table 6.2: Cloud computing Advantages / Disadvantages

S.No.	Advantages	Disadvantages
1	Back-up and restore data	Internet connectivity
2	Improved collaboration	Vendor lock-in
3	Excellent accessibility	Limited control
4	Low maintenance costs	
5	Unlimited storage	
6	Mobility	
7	Unlimited storage capacity	

Cisco proposed Fog computing that deals with network edge and extends the facility of cloud computing. Fig. 6.2 shows the region of cloud computing, Fog computing and Edge computing [115]. Here, cloud servers are located far distant from Edge layer whereas Fog layer is near to edge layer to reduce processing time of data. Further, processing speed and response time slow down as compared to edge computing. Table - 6.3 shows the IOT-Cloud functions and Table - 6.4 presents the functional comparison of each layer in IOT – Cloud layers.

Table 6.3: IOT- Cloud layers functions

Cloud (Analysis, Processing, Warehousing)

Fog (Local analysis, processing, storage)

Edge (Real time processing, visualization,

Table 6.4: Functional comparison of IOT – Cloud layers

Parameters	Cloud	Fog	Edge
Latency	Highest	Medium	Lower
Scalability	High, easy to scale	Scalable within network	Hard to scale
Distance	Far from the edge	Close to the edge	At the edge
Data Analysis	Less time	Real-time decides to process locally or send to cloud	Real time, instant decision making
Computing Power	High	Limited	Limited
Interoperability	High	High	Low

There are four types of clouds: (i) Private cloud, (ii) Community cloud, (iii) Public cloud and (iv) Hybrid cloud. Functions of these clouds are to offer services of software's, platforms and infrastructure. Table - 6.4 shows the components of IOT and cloud computing.

6.4.1. Security of Digital Assets and Privacy

Data security deals with data protection from external and internal threats, whereas data privacy is data governance [117]. Security in digital technology for data transaction, generally is based on third party resources. However, in Blockchain technology role of third party is eliminated by designing the Blockchain with the features of decentralization, consensus and cryptography. Here, layers solution offers both privacy and security. Table - 6.5 presents the summary of some important methods of data security.

Table 6.5: Analogy of methods for data security

Data encryption	Backup and recovery optimization	Data masking	Row Level Security (RLS	Cryptography Digital Signatures	Cyber insurance
Transform to unusable format, but this format can be hacked or theft. (SMS Message, email, databases, password, user name, etc.)	Backup and recovery is the duplicating and storing of data in case of data loss due to any cause.	It hides the actual data using modified content like characters or numbers and cannot be reverse engineered.	It restricts on data row access. It also simplifies the design and coding of security in the application.	It creates a distinctive hash of message and encipher and employ the sender's private key. Creates trust between utilities, customers, business partners, and vendors.	A cyber insurance policy helps an organization pay for any financial losses they may incur in the event of a cyberattack or data breach.

Visualisation is the process of converting raw data to graphical images to get an overview of the data. Fig.6.3 shows the concept of visualization pipeline.

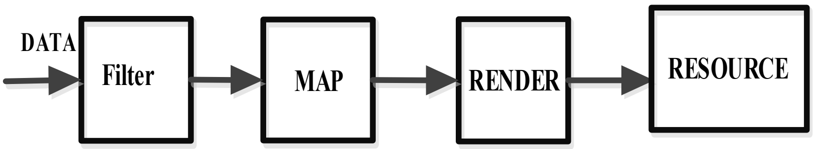


Fig.6.3: Concept of visualization pipeline.

6.5 BLOCKCHAIN

Blockchain is a layer structured technology that has the features of (i) Decentralization: Resources are owned and shared by network members; (ii) Immutability: History of transactions in ledger is unalterable; (iii) Transparency: Complete traceable and easy to maintain; (iv) Open-Source Access: A public and transparent mode to keep records. (v) Auditability: Past transaction-based judgements and (vi) Autonomy: Operate based on rules and processes in code. [118] has surveyed Blockchain applications and use in the smart grid. Also, usefulness of Blockchain as cyber-physical layer is presented. The Blockchain is a decentralised digital ledger that makes possible to conduct transactions and share data in a way that is both secure and transparent. It was at first presented as the technology that underpinned the cryptocurrency known as Bitcoin, but since then, it has achieved extensive usage in a variety of businesses outside of banking[119]. A Blockchain may be broken down into its component parts, the most fundamental of which is a distributed ledger that stores data over a network of computers known as nodes. Every node in the network has its own copy of the Blockchain, which it uses to validate transactions, add new blocks to the chain, and ensure the network's continued operation.

When a transaction is started, the legitimacy of the transaction is checked by a network of nodes through the application of intricate Algorithm and consensus mechanisms. Once the transaction has been validated, it will be recorded in a block along with other transactions that have been validated. This creates a chain of blocks, hence the name Blockchain. Because each block includes a one-of-a-kind identifier, a timestamp, and a cryptographic hash of the block that came before it, the blocks can only be connected to one another in a safe and tamper-proof manner.

The high level of confidentiality and transparency that Blockchain technology offers is one of the most significant advantages it offers. The network is more resistant to attacks and data breaches as a result of its decentralised nature, which ensures that there is no single point of failure and prevents there from being any. In addition, the utilisation of cryptographic techniques and consensus procedures ensures that the data that is kept in the Blockchain cannot be altered in any way and cannot be altered by unauthorised parties.

The following is a list of other advantages and capabilities offered by Blockchain technology:

- Decentralisation: Due to the distributed nature of Blockchain technology, there is no requirement for a centralised authority or intermediary to allow transactions or the sharing of data. This not only reduces the chances that there will be a failure at a single location, but it also gives users more freedom and control over the system.
- Because of its tamper-proof nature and its public record of transactions, Blockchain has quickly become one of the most trustworthy and transparent forms of digital ledger technology. Users can have faith that the information that is saved on the Blockchain is reliable and cannot be altered, and that all transactions can be easily audited and validated.

- Contracts that are self-executing and self-managing are referred to as smart contracts. A smart contract is a contract that is programmed to automatically execute when conditions are satisfied. They are constructed on top of the Blockchain technology and offer an automatic procedure and enforce regulations without the requirement of using intermediaries.
- Blockchain technology has the potential to make transactions both quicker and less expensive.
- Privacy: Although Blockchains that are open to the public, there are also private and permission Blockchains that can offer better privacy and control.

Blockchain technology has a wide variety of advantages as well as uses, and it has the potential to significantly disrupt and revolutionise a variety of different industries. However, it is still a relatively new technology that is still evolving, and there are challenges and limitations that need to be addressed. Some of the limitations are listed below:

- Interoperability is one of the hurdles that Blockchain technology must overcome in order to realise its full potential. Transferring data and assets from one Blockchain platform to another can be challenging since there are so many distinct Blockchain platforms and protocols. Inter-ledger Protocol and Polkadot are two examples of cross-chain interoperability.
- Scalability is an additional obstacle that must be overcome by the Blockchain technology. There is a risk that the Blockchain will become sluggish and clogged up as more users and transactions are added to the network.
- Governance: Blockchain networks need governance methods to ensure their stability, security, and evolutionary progress. Governance is also known as "stewardship." This may include decision-making mechanisms, mechanisms for the resolution of disputes, and mechanisms for the upgrade of networks[120]. There are a wide variety of governance models utilised by various Blockchain platforms and communities. These models range from decentralised autonomous organisations (DAOs) to more centralised structures.

Blockchain operation as two layers' Algorithms to improve the security and risk in association with PMU is presented in [107] - [108]. [109] suggested the Blockchain use in transaction of smart grid data between generating stations and end user.

6.5.1 Layer Structure of Blockchain

Blockchain technology is an integration of several technologies viz. cryptography, game theory, etc. This is based on trilemma of Decentralization, Security, and scalability and cannot be optimized for all three desired features simultaneously. Its architecture is designed as six layers. The content of the Blockchain is stored on the server. Hardware and Infrastructure layer generates virtual resources such as storage, networks, servers, etc. Data Layer increases scalability. Each Blockchain contains a root hash of Merkel trees and information in/ of blocks. The Merkel tree provides security, integrity and irrefutability. The Blockchain is a distributed ledger that is not centralised in any one location and records transactions that take place across a network of computers. The Blockchain is composed of multiple layers, each of which is responsible for a distinct function inside the system. The Fig.(6.4) shows the different layers of Blockchain. A comprehensive explanation of Blockchain's tiers is as follows:

- The application layer is the final layer of the Blockchain system, and it is also the layer that is at the top. This is the location where users create transactions and interact with the Blockchain. The application layer is made up of a variety of Blockchain apps, including bitcoin wallets, smart contracts, decentralised applications (also known as DApps), and more. These applications use the Blockchain as a means to carry out transactions, store data, and carry out instructions for computer programmes. In order to carry out transactions and bring the ledger up to date, the application layer of the Blockchain is in constant communication with the other layers.
- Layer of Consensus: The consensus layer is in charge of making sure that all of the nodes on the network have a copy of the ledger that is identical to one another. It is the layer that makes it possible for the Blockchain to function independently. This is accomplished by the consensus layer through the use of a consensus mechanism, which is a rule set that must be adhered to by all nodes in order for transactions to be validated and approved. Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Byzantine Fault Tolerance (BFT) are the four types of consensus

techniques that are utilised in Blockchain systems frequently. The consensus layer is also responsible for ensuring that the ledger is kept in an unchangeable and secure state.

- Network layer: The network layer is in charge of connecting nodes across the Blockchain network. Its responsibilities include these. This makes it possible for nodes to exchange information and communicate with one another. In order to accomplish this goal, the network layer makes use of peer-to-peer (P2P) networking. P2P networking is a type of decentralised network in which each node is connected to several other nodes, hence producing a web-like structure of connections. Even in the event that there are disruptions in the network or malicious attempts to disrupt it, the Blockchain will continue to function dependably and effectively because of network layer.
- Protocol layer: The protocol layer is the part of the Blockchain system that is in charge of creating the rules and standards that are used to regulate the system. This is used to detail the structure of transactions, including how data is saved and retrieved, as well as the manner in which nodes communicate with each another. The protocol layer is responsible for ensuring that all nodes on the network follow the same rules. This guarantees that the Blockchain is able to function without any disruptions.
- Data layer: The data layer is part of Blockchain that is responsible for storing all transactions. It is the most fundamental part of the Blockchain and is made up of a decentralised database that is copied to all of the nodes that are connected to the network. The data layer ensures that the Blockchain is immutable, which means that once a transaction has been recorded, it cannot be edited or deleted.

The successful operation of the Blockchain system is dependent on the contributions made by each layer. Users will be able to interact with the Blockchain through an interface that is provided by the application layer, while the consensus layer is responsible for ensuring that all nodes on the network have the same copy of the ledger. The protocol layer is responsible for defining the rules and standards that govern the system, while the network layer is responsible for connecting the network's nodes. The final layer, known as the data layer, is responsible for storing all of the transactions that take place on the Blockchain. This makes the ledger both immutable and scalable.

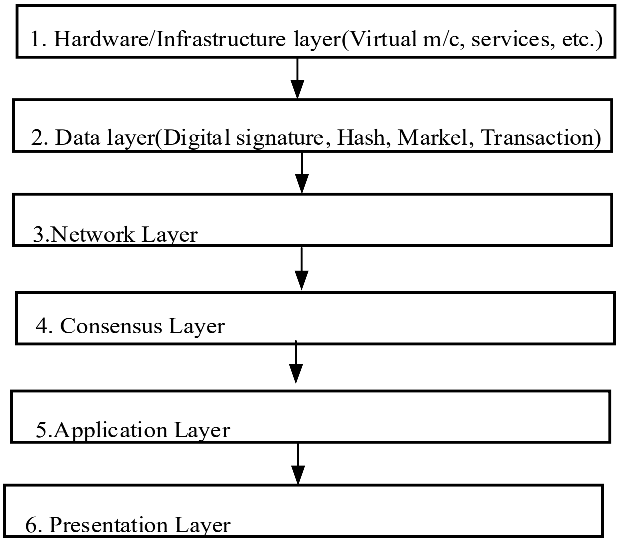

1. Hardware/Infrastructure layer(Virtual m/c, services, etc.)
2. Data layer(Digital signature, Hash, Markel, Transaction)
3.Network Layer
4. Consensus Layer
5.Application Layer
6. Presentation Layer

Fig.6.4: Blockchain Structure

Network layer (P2P layer) deals with inter-nodes communication. Consensus layer is in charge of validating the blocks, ordering them and guaranteeing that everyone agrees. Consensus layer, Application & Presentation layer contains the programs that end-users utilize to communicate with the Blockchain network.

6.6. HASH ALGORITHM

A hash Algorithms is a mathematical function that can be applied to data of any size and creates a fixed-size output, often known as a hash value or message digest. This output can be used to verify the integrity of the input data. A hash Algorithms goal is to provide a one-of-a-kind and reliable representation of the data. Hash Algorithm are an essential component of modern cryptography and find use in a wide variety of applications, including digital signatures, message authentication codes (MACs), password storage, and more. However, because of weaknesses or vulnerabilities of the Algorithms can be exploited by attackers, it is essential to use a hash Algorithms that is both powerful and secure.

Cyber security to dataset is provided by embedding Blockchain Algorithms to PMU, as shown in Fig.6.5. Blockchain embedded PMU uses hash mechanism. It is a mathematical function which transforms data chain to a fixed length numeric chain output. Generally, this output chain is quite small for the data chain. The Algorithms is based on the collision – resistance principle i.e. for different data chain same output chain should not be generated. Further, hash Algorithms generates unreadable output data chain, however, follow strictly mathematical function. Hashing is a cryptographic fingerprint. Hashes represent the binary tree of data structure. The transformed output data chain is nearly impossible to convert to its original data set. This transformed data chain is then compressed and communicated to concerns for further action and processing. Fig. 6.5 presents the Hashing process:

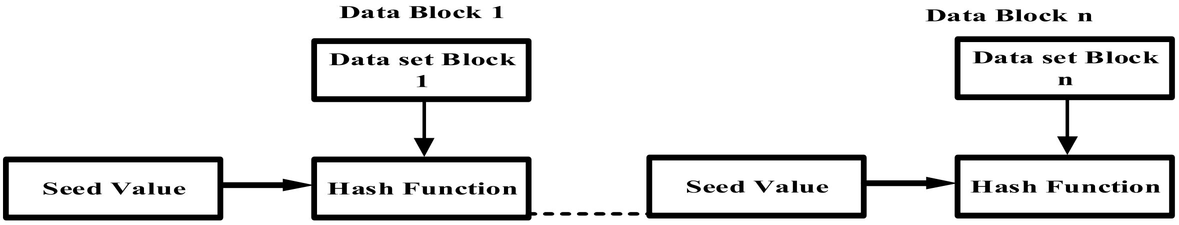


Fig.6.5: Hashing Algorithms for data / text processing

The representation of the data can then be put to use for a variety of tasks, including the verification of data integrity, the creation of digital signatures, the storage of passwords, and many more. The most common hash Algorithm are the following:

- One of the most common hash algorithm is called MD5, which stands for the Message-Digest Algorithms 5. It generates a hash value that is 128 bits long. On the other hand, it is presently thought to be unsafe, hence it must not be utilised for any cryptographic operations.
- SHA-1, also known as the Secure Hash method 1, is a hash method that generates a hash value of 160 bits and is used extensively.
- The Secure Hash algorithms 2 (SHA-2) is a family of hash algorithm that comprises SHA-224, SHA-256, SHA-384, and SHA-512. Its full name is Secure Hash algorithms 2. Within this family of algorithm, the one that generates a hash value of 256 bits is the one that is utilised most frequently.
- SHA-3, or Secure Hash algorithms 3, is a family of hash algorithm that comprises SHA3-224, SHA3-256, SHA3-384, and SHA3-512. SHA-3 is also known as the Secure Hash algorithms 3. It was developed to provide an alternative to the SHA-2 family of Algorithm that are more reliable in terms of security.
- BLAKE2 is a modern hash algorithms that is faster than SHA-2 and SHA-3 while yet retaining a high level of security.

The integration of two systems/ technologies (PMU and Blockchain) makes it useful for computation of tariffs due to tie line power exchange dataset transfer, power transfer between micro-grid and utility / main grid, etc. and also create confidence among consumers, utilities and power generating companies.

6.6.1. Addition of Block to Chain

The Mining process is adding a block to ledger. Fig. 6.6 and Fig. 6.7 show the mining process and block details, respectively. The data set creates a block and a hash is calculated w.r.t particular block using mathematical function. It is a mathematical problem which generate block of data / text message and ensure the validity of transactions. This needs a CPU and this process consumes more electric energy. The addition of a new block to a Blockchain requires the completion of a number of processes before the system can continue to function without compromising its reliability or safety. The procedure can, in general, be broken down into the following steps:

- Validity check of the block : Before a block can be added to the Blockchain, it has to be checked to make sure that it contains only legitimate transactions and that it was generated by a trusted node on the network. This is known as the validity check of the block. Checking the digital signature of the block, which is generated using the private key of the node that created the block, is the standard method for doing this operation. The signature can be validated by utilising the public key of the node, which is kept on the Blockchain for all users to see.
- Mining of the block: In certain Blockchain systems, such as Bitcoin, blocks are "mined" by nodes on the network. Mining refers to the process through which new blocks are added to the chain. The process of mining needs the resolution of a cryptographic puzzle, which takes a large amount of computing power. Once a node has successfully completed the puzzle, it will be able to generate a new block and add it to the Blockchain.
- The block must be broadcast to the other nodes in the network once it has been formed, as this is the only way for them to become aware of its existence. This makes it possible for other nodes to check the legitimacy of the block and add it to their own personal copy of the Blockchain.

- A consensus must be reached on the contents of the block before it can be added to a Blockchain. This can only happen if consensus mechanism is implemented, which requires that all nodes on the network be in agreement. Proof of Work (PoW) is the consensus method that is utilised in Blockchain systems the most frequently. This technique mandates that nodes must solve a cryptographic problem before they are allowed to add a new block to the Blockchain.
- Once a block has been verified, mined, broadcast, and validated by the consensus mechanism, it can then be added to the Blockchain. This allows the block to be added to the Blockchain after it has been mined. In order to accomplish this, the block must be added to the end of the existing chain of blocks, and the hash pointer of the block that came before it must be updated so that it points to the new block.
- Verification of Blockchain: Once a new block has been added to the Blockchain, all of the nodes on the network are required to verify the updated Blockchain to ensure that it has not been tampered with. This requires verifying the digital signatures of each block in the chain, as well as ensuring that the hash pointers are changed in the appropriate manner.

In the present study, FPGA (Xiline – Virtex) as CPU is used in PMU. Fig. 6.7 shows the mining process for some Blockchain. It is a way of adding transaction records, via blocks, onto a public ledger. Miners are nodes in the network that ensure the transactions in the block are valid. Addition of block offers utility / consumer / power generation operators to track the power transferred at any time and energy charges in lieu of it. Particularly, participants guarantee that power / electric energy utility / utilizer have not already used the funds which are sent to other participants .Upon completing the verification process, the algorithms creates a network for Blockchain. Public ledger holds transaction records in Blockchain mode. The validity of the transaction in this block is entrusted with mining. Consensus tools are explored for the purpose. Consensus among all the participants is needed on changes to the ledger. Once the block is generated, it is uploaded to cloud as shown in Fig.6.8(a).

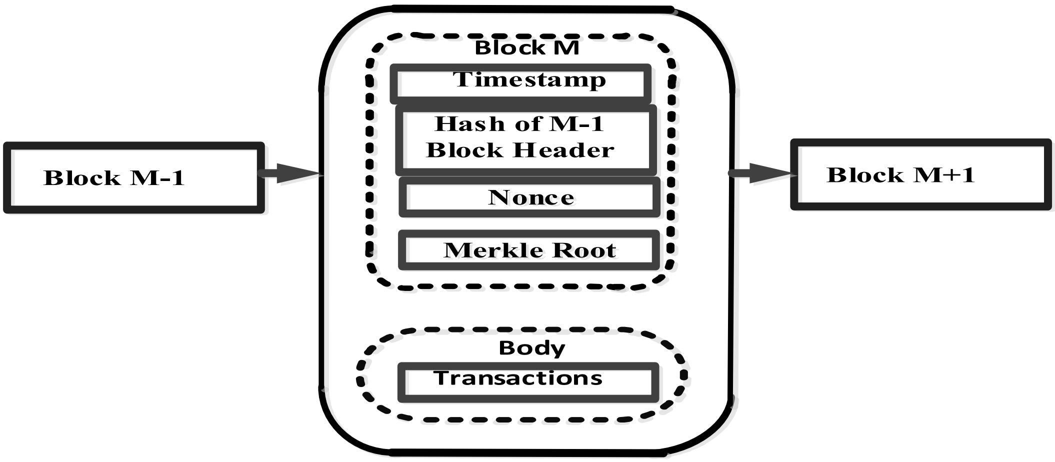


Fig.6.6: General Blockchain structure.

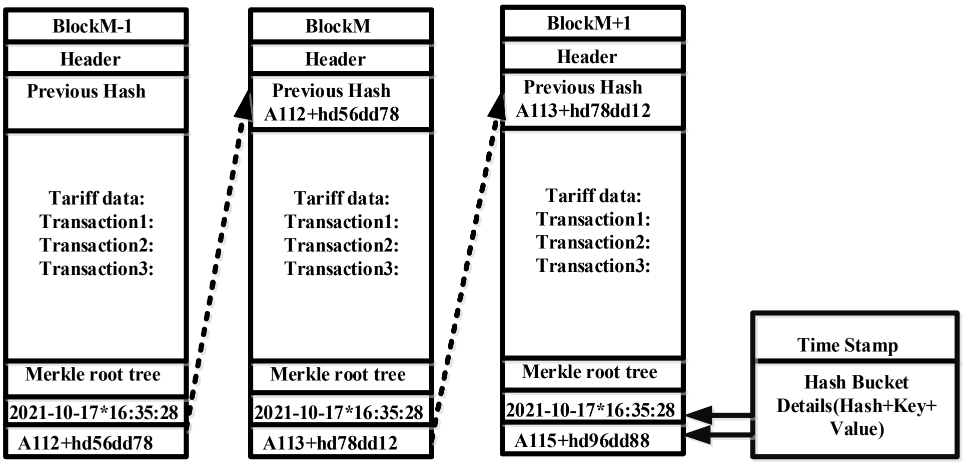


Fig.6.7: Mining Blockchain

6.7. BLOCKCHAIN APPLICATION FOR PMU

The Blockchain is value added in cryptography to PMU (Fig.6.8(a)). In order to show the utility of Blockchain technology for tie –line, the section here have simulated the problem considering one of the personal computers (PC) to uplift the data (kWH, kV, frequency, etc.) to cloud, which represent tie-line power transferred data since facility of PMUs were not available (Fig.6.8(b)). Distributed and scalable data model based on the Blockchain is implemented using a heterogeneous set of MYSQL database management system, hosted on the AWS cloud. The string of data is transformed into JSON format and stored. The fingerprinting is done by using SHA256 hashing algorithms. The mining of the new block is carried out with the proof of work.

Thus, the validity of the chain is done to prevent any kind of tampering with the Blockchain. The output from Blockchain is now available and is fed to Azure AWS cloud for further use. The following steps are followed to input the data to cloud.

STEP 1 – The data is stored in JSON format which is stored in a block and the block contains multiple data.

STEP 2 - The fingerprinting is done using hash. Standard algorithm SHA256 is employed for this function. The chance of tampering with the block is eliminated by using hash of the previous block, including its own hash. Blocks are chained together with fingerprints and connected by the previous block and the next block by hash.

```
“hash”: e2a1ec32fcf89d0388f3d0d8abcd914f941d056c080df1c765a3f6035626fc94
```

STEP 3 –Proof of work ensure creation of a new block. After addition of the block successfully, the block will then be added to the chain. The following message is displayed upon any tampering being detected in the system:

```
Tamper Detected --- Mining rejected
```

No code outputs are produced at this stage.

STEP 4 – Blockchain needs to be checked upon completion of mining the block for tampering of any type.

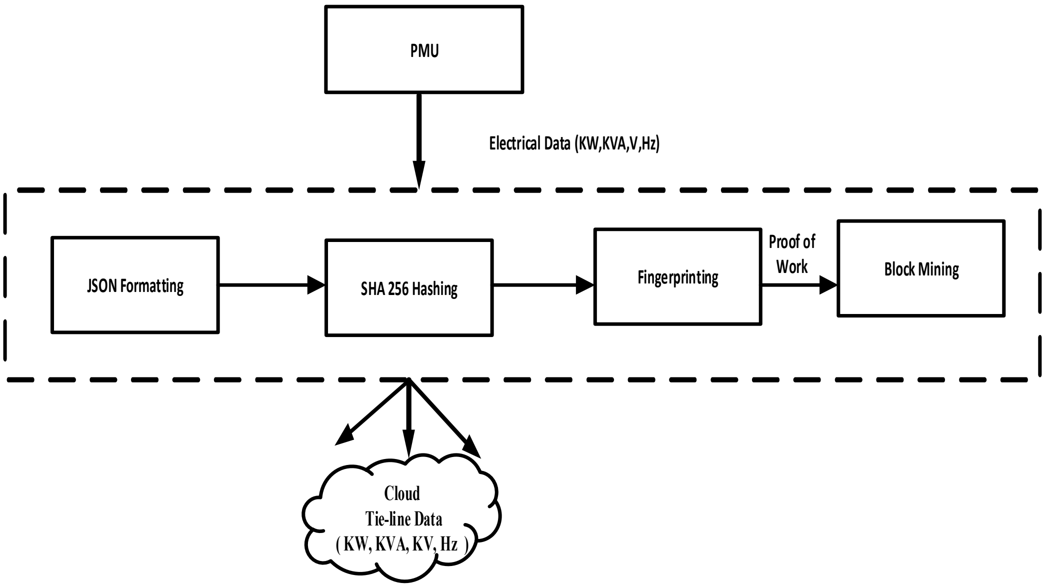


Fig.6.8a: Physical integration of PMU – Blockchain and Cloud

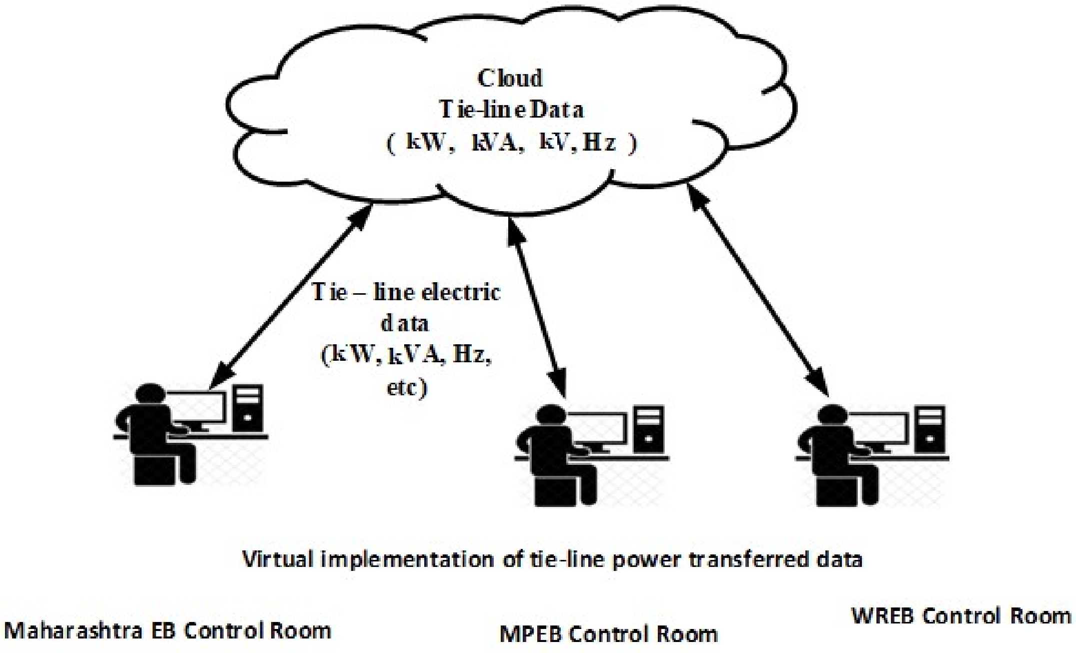

Cloud
Tie-line Data
(kW, kVA, kV, Hz)
Tie – line electric data (kW, kVA, Hz, etc)
Virtual implementation of tie-line power transferred data
Maharashtra EB Control Room
MPEB Control Room
WREB Control Room

Fig.6.8b: Detailed Line Flow Diagram for Blockchain implementation

6.8. IMPLEMENTATION

In order to implement the Blockchain associated PMU, flow chart in Fig. 6.9 is used to develop the protocol for the trust ship among the utilities/power generating owner and consumers. The code along with explanation is given in Appendix- C

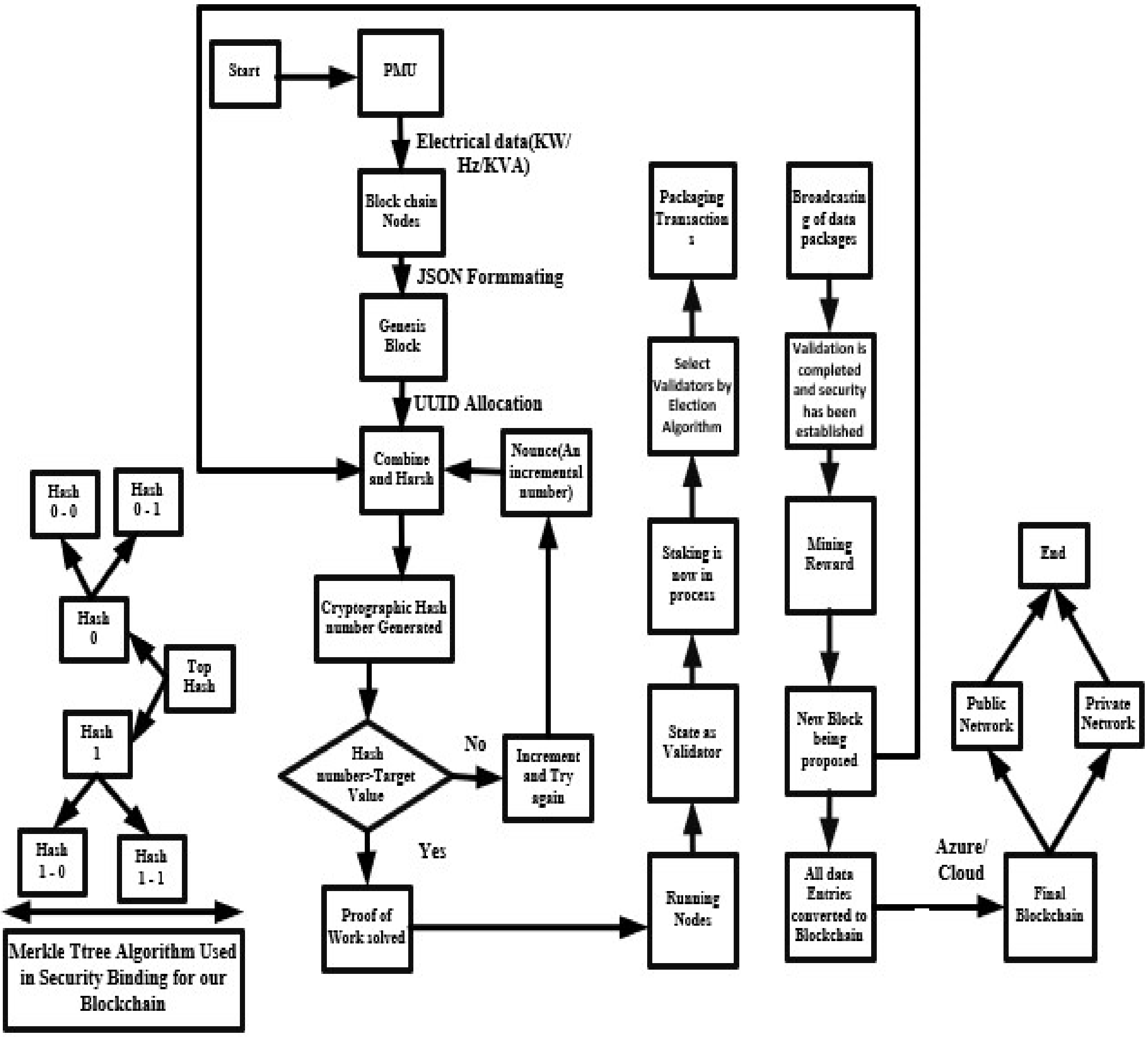


Fig.6.9: Flow chart for Blockchain Implementation on PMU

6.9. RESULTS AND DISCUSSION

Table – 6.6 and 6.7 represent the tie line power transfer and power generated by the non-conventional energy source (photo voltaic power plant), considering the average value for 30 secs. Table - 6.6 shows that Madhya Pradesh Electricity Board(MPEB) transfers the 12MW power to Maharashtra Electricity Board via Nepanagar- Dhani interstate power line at 11Hr 45 Min 03Sec. This was confirmed by Weston Regional Electricity Board (WREB) by monitoring and observing the Nepanagar-Dhani transmission line. Table - 6.7 shows the power generated by roof top solar power plant, consumed by the owner and transferred to the grid by monitoring renewable plants, consumer and grid. The Grid operator confirmed it as neutral party.

Table – 6.6: Tie-LinePowerTransferred conformation

Power transferred by MPEB	Power Received by Maharashtra	Line Name: Neepanagar - Dharni	At Frequency	Conformation With WREB
12MW	12MW	132kV	49.3Hz	12MW

Table 6.7: Power Generated by a Non-Conventional Energy Source

Power Generated by Photo Voltaic Plant (Roof Top)Meter reading (A)	Power used by the Owner Meter reading (B)	Power transferred to Grid Operator Meter Reading (C)	Conformation A=B+C
4.300kW	2.65 kW	1.650kW	2.65+1.650=4.30kW

6.10. CONCLUSION

The present study shows that Blockchain embedded PMU is a highly reliable and secure system for monitoring and transferring of electrical data / parameters. PMU acts as an intelligent transducer whereas Blockchain incorporates cryptography to data processed through it. The study shall be useful to grid operator, protection engineer, utility, power consumers and roof-top photo voltaic power generating owners.

CHAPTER - VII
CONCLUSION AND SCOPE FOR FUTURE WORK

7.1. INTRODUCTION

A Phasor measurement unit is an intelligent device that measures and keeps track of electrical parameters in a power system in real time. Magnitude, phase angle, and frequency are the three main electrical parameters that are frequently measured. These measures can offer a thorough scenario of the behaviour of the electrical grid, enabling early problem diagnosis and more effective grid maintenance and operation. A smart device is in a degraded state if it still performs some of its important activities, but only partially, or if it continues to operate within permissible limitations that are lower than the prescribed values.

This work's primary objective is to explore a crucial factor influencing the Phasor measuring unit's dependability so that it can be utilized more effectively.This work develops the Markov model of each module and their sub module taking into account their redundancy. Reliability and sensitivity are vital parameters and hence are evaluated. As the manufacture data is available in intervals, using that sensitivity calculation w.r.t failure and repair rate is done. The work further covers the uncertainties which are due to operational and environmental factors. For covering the uncertainty a soft computing technique such as fuzzy logic is taken into account. This uncertainty inspire the use of interval type-2 Fuzzy logic (IT2FS). While using IT2FS dynamic nature of data is not taken into account. The Petri Net concept is used in order to address both of these important factors. The ad hoc interaction between the parametric values defined by the PMU module is handled by a Petri Net. Petri Net modeling is a useful tool for PMU design and optimization, as well as for identifying possible malfunctions or defects in the system. Several data security risks related to the collection and evaluation of this real-time data must also be taken into consideration, since the Petri Net concept takes into account both the dynamic nature and uncertainty as well as the availability, confidentiality, and integrity of the data. For this Blockchain is further implemented on PMU to prevent the unauthorized access to data communicated by PMU. No tampering with data is allowed. This security issue with data can severely impact the operation of the electricity grid which can result in outrages and other interruption. So this work focuses on implementation of Blockchain which can overcome the issue of data security.

7.2. MAIN CONCLUSION

Phasor Measurement Units (PMUs) must be reliable and sensitive in order to accurately characterize and anticipate operational efficiency and utilization. The creation of fault tree logic diagrams and Markov probabilistic mathematical models for PMU modules is done to analyze these issues. To assess the performance of these modules and the entire PMU system, numerical parameters like PMU availability, mean time between failures (MTBF), mean time to repair (MTTR), and reliability are computed. The influence of differences in failure rate and repair rate on the reliability indices of PMUs is further investigated using sensitivity analysis.

The results of the sensitivity analysis show that the variation in failure rate has a more significant impact than the variation in repair rate on the reliability indices of PMUs. System designers can use this information to identify the modules that are most vulnerable to outages and to prioritize their upgrade efforts. Additionally, the Markov Model is used to analyze the frequency of probabilities in each of its dwelling states, providing a greater knowledge of the behavior of the system. Additional reliability indices can be assessed by calculating the likelihood that the system is in the 'up state,' 'down state,' or 'de-rated state.' These reliability indices shed light on the system's ongoing operations, maintenance, and repairs.

Analog-to-Digital Converter (ADC) and Central Processing Unit (CPU) synchronization with the GPS receiver module is considered to be the most important functions of PMUs. A standby crystal oscillator is used, which takes over the synchronization task, to lessen the effects of GPS receiver failure. When the cumulative inaccuracy of a 50 Hz power system surpasses the limit of 31 microseconds for more than an hour, the crystal oscillator malfunctions. These studies help with the development and design of PMUs, assuring their accessibility for efficient grid operation.

. The dynamic character of failure is modelled as an event in the Petri Net, and fuzzy logic reasoning is used to deal with the uncertainty related to failures.

By combining fuzzy logic and Petri Net technology, this method creates a Sprouting tree, a logical structural path. The study's methodology is crucial for PMU system designers and smart grid implementation. It offers advantages such as the ability to model and handle extremely complex systems, the participation of various experts, and superior handling of uncertainties and possibilities. These are based on the examination of the PMU design adequacy.

The report also emphasizes how Blockchain incorporated PMUs are dependable and secure for sending and monitoring electrical data and parameters. While Blockchain technology uses encryption to ensure secure data processing, PMUs serve as intelligent transducers. The study's goal is to further Blockchain research in the context of tie-line power transmission data. Results from the study are advantageous to a number of stakeholders, including grid operators, protection engineers, utilities, power users, and owners of rooftop photovoltaic power generating equipment.

The study also emphasizes the security and dependability that Blockchain embedded PMUs provide, advancing Blockchain technology in the context of power systems. The conclusion of the thesis open the door for additional study in the area and offer helpful advice to the many stakeholders engaged in grid functioning.

7.3 SUGGESTIONS FOR FUTURE WORK

Reliability and sensitivity are important aspects for any device, equipment, and networks. Any gadgets, equipment, and networks need to be dependable and sensitive. The PMU's availability increases steadily as does its reliability, indicating that the design is getting better and better. Deep learning techniques, which are based on artificial intelligence, are required for PMU estimation with improved reliability. Time series data is used in deep learning techniques to assess reliability. Thus, the reliability and sensitivity of PMU may be computed using deep learning technique.

➢ The present work focuses on computing reliability of PMU considering only the redundancy in repair rate and on failure rate but future work can focus on multiple failure modes which can occur simultaneously.

➢ While computing reliability using IT2FS some assumptions are made in this study like the PMU device is in its prime life, the five modules of PMU have different failure rate, the data supplied by the manufacturer are limited and mathematical computations are not feasible. So the work can be extended considering smaller ratio of repair time (r) to the mission time. Also in the present study the failure rate and repair time are considered constant and failures are independent.

➢ This thesis also shows the work related to FPN use of a method that goes beyond the capabilities of fuzzy Petri Nets for modeling and analyzing complex systems is "Discrete Event Simulation" (DES), it is a powerful technique used to model the behaviour of dynamic systems where events occur at distinct points in time. It can handle a wide range of complexities.

➢ Cyber security mainly prevents hardware, software, and data present in the system that has an active internet connection from external attacks. In the present simulation study, Blockchain technology is explored for tie–line power transfer in trust mode. This further requires field testing to conform the simulation study. Deep learning is the latest technology applied in cyber security. It has been applied to detect different types of cyber attacks in communication networks. It may be explored for tie –line power transfer in trust mode. The latest methods for data encryption are based on DNA Computing.

REFERENCES

[1] N. Gupta, R. Garg, P. Kumar, “Sensitivity and reliability models of a PV system connected to grid”, Renewable and Sustainable Energy Reviews, Volume:69,2017, pp:188-196, ISSN1364321, https://doi.org/10.1016/j.rser.2016.11.031.

[2] F. Aminifar, S. Bagheri-Shouraki, M. Fotuhi-Firuzabad, and M. Shahidehpour, "Reliability Modeling of PMUs using fuzzy sets," IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2384-2390, Oct. 2010.

[3] A. K. Karngala and C. Singh, "Reliability Assessment Framework for the Distribution System Including Distributed Energy Resources," in IEEE Transactions on Sustainable Energy, vol. 12, no. 3, pp. 1539-1548, July 2021, doi: 10.1109/TSTE.2021.3053911.

[4] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," IEEE PES General Meeting, Minneapolis, MN, USA, 2010, pp. 1-6, doi: 10.1109/PES.2010.5590189.

[5] Y. Wang, Wenyuan, et al., "Reliability analysis of phasor measurement unit considering data uncertainty," IEEE Transactions on Power Systems, vol. 27, no. 3, pp. 1503-1510, Aug. 2012.

[6] P. Zhang and K. Wing Chan, "Reliability evaluation of phasor measurement using Monte Carlo dynamic fault tree method," IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1235-1243, Sep. 2012.

[7] P. Mahat, Z. Chen, and B. Bak-Jensen, "A Hybrid Islanding Detection Technique Using Average Rate of Voltage Change and Real Power Shift," IEEE Transactions on Power Systems, vol. 24, no. 2, pp. 764-771, Apr. 2009.

[8] B. S. Dhillon and C. Singh, “Engineering Reliability: New Techniques and Applications”, Wiley, 1981.

[9] M.S Ding, G. Wang, and X.H.Li, “ Reliability Analysis of Digital relay,” in Proc.8th IEEE Int. Conf. Developments Power Syst. Protection, Published: Apr.2004, vol. 1, pp.268-271

[10] Castro, L.R and Crossley L.R., 1999” Reliability evaluation of substation control system”IEEE Pro- Generation. Transmission Distribution, vol.146, pp:626-632.

[11] Y.Ren and J. B Dugan," Design of reliable system using static & dynamic fault trees", IEEE Trans. Rel.,Published:Sep.1998,vol. 47, Issue: 3, pp: 234-244

[12] J. Yuan , "Research on reliability modeling of complex system based on dynamic fault tree," in Proc. Technol. Innovation. Conf., Oct.2009, pp:1-5.

[13] W.Wang, J.Loman, and P. Vassilion," Reliability importance of components in a complex system," in Proc. Annual.Symmetrical.Rel. Maintainability.Published: Aug. 2014,pp:6-11.

[14] Debomita Ghosh, T Ghose and D.K. Mohanta," Reliability analysis of a geographic information system-aided optimal phasor measurement unit location for smart grid operation," Journal Proceedings of Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, DOI: 1177/1748006X13482853

[15] Chen, Y. Qi, and M. Wang. (2017). Reliability Assessment of Phasor Measurement Units in Wide-Area Measurement Systems. IEEE Transactions on Power Delivery.

[16] G. Singh, A. Sharma, and S. Singh. (2017). Performance Evaluation of PMU-based Fault Location Techniques in a Real-time Environment. IEEE Transactions on Power Delivery.

[17] R. Billinton and R.N Allan, "Reliability Evaluation of Engineering system, 2nd Edition New York, Plenum 1994.

[18] C. Wang, X. Yan, and L. Cheng. (2019). A Probabilistic Model for Reliability Evaluation of Phasor Measurement Units. IEEE Transactions on Power Systems.

[19] Nemer Amleh, Mohammad Almuhaini&uhammad Khalid, "Impact of Smart Restoration and Energy Storage systems on its reliability of Electric Microgrid", Published: 23 December 2019, pp. 1-15, Arabian Journal for Sciences and Engineering.

[20] Behahzad Karimi, STA Niaki, HussanHaleh, BahmanNadari, " Reliability optimization of tools with increasing failure rates in a flexiable manufacturing system", Published: March 2019, vol 44, Issue:3, Arabian Journal for Sciences and Engineering

[21] A G Phade, "Synchronised Phase Measurement in Power Systems" IEEE Trans. Computers Applications in Power System", Published:April 1993, vol.6, Issue:2, pp-10-15

[22] P.Mahajan, R Garg,Parmod k, "Sensitivity analysis of railway electric traction system", India International Conference on Power Electronics 2010 (IICPE2010)

[23] Ch. Murthy, MaibamShillakanta Singh and D.K Mohanta, “ Effect of Switching on Stand- by Redundancy Operating Mode of Phasor Measurement Unit”, Conference: Environment and Electrical Engineering (EEEIC), Published: 2013, 12th International Conference

[24] P. Hiber and L. Bertling,” A method for extracting reliability importance indices from reliability simulations of electrical networks,” in Proc. 15th Power System.Computation. Conf.(PSCC), Liege, Belgium, Published: Aug. 2005

[25] Z.H. Dai, Z.P. Wang, and Y. J. Jiao, “Reliability evaluation of the communication network in wide area protection.” IEEE Trans. Power del. June-2019.

[26] James Li, “ Reliability Calculation of a Parallel Redundant System with different failure rate and repair rate using Markov Modeling, J. Reliability and Statistical Studies, Published: June2016,vol 9, Issue:1

[27] S.Gupta, P.Mahajan and R Garg ,“Sensitivity model of energy consumption by railway electric locomotive”, 2015 Annual IEEE India Conference (INDICON)

[28] Peng Li, Hongzhi Su Li, Zhelini Lu, Chengshan Wang, Jianzhong Wu “Voltage Control Method of Distribution Networks Using PMU Based Sensitivity Estimation” Energy Procedia, Published:February 2019,vol.158, pp: 2707-2712

[29] Y. Fu, M. Kezunovic, and X. Sun, "Reliability assessment of phasor measurement units (PMUs) for power system monitoring," IEEE Transactions on Power Delivery, vol. 27, no. 1, pp. 259-267, Jan. 2012.

[30] Singh, Pankaj, Yadav, K, Shrivastava, Abhishek. “A Preliminary study on reliability engineering and its evaluation”, Turkish Journal of Engineering, Science and Technology. 03. pp. 53-55, 2013.

[31] R. Xiao and H. Wang, "PMU-Based Wide-Area Adaptive Fuzzy Control for Power Systems," in IEEE Transactions on Smart Grid, vol. 13, no. 1, pp. 83-92, Jan. 2022, doi: 10.1109/TSG.2020.3047896.

[32] F. Zhang and Q. Wang, "An Improved Type-2 Fuzzy Logic Controller for Renewable Energy Generation in Micro grids," in IEEE Transactions on Fuzzy Systems, vol. 29, no. 2, pp. 273-286, Feb. 2021, doi: 10.1109/TFUZZ.2020.2970573.

[33] M. El Haddad, Y. M. Abdel-Magid and M. N. Abdel-Rahman, "A hybrid neural network-fuzzy logic type 2 controller for power system frequency control," in IET

Generation, Transmission & Distribution, vol. 14, no. 18, pp. 3619-3627, Dec. 2020, doi: 10.1049/iet-gtd.2020.0423.

[34] M. Abedi, M. Abedini and S. S. M. Ghaderi, "PMU-Based Adaptive Fuzzy Logic Controller for Renewable Energy Integration in Distribution Systems," in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4374-4384, July-Aug. 2020, doi: 10.1109/TIA.2020.2972744.

[35] J. Ghaderi and M. Moeini, "A fuzzy type-2 controller for DC micro grids with renewable energy sources," in International Journal of Electrical Power & Energy Systems, vol. 118, p. 105818, Apr. 2020, doi: 10.1016/j.ijepes.2019.105818.

[36] R. Su, M. J. Hossain and J. Lu, "Adaptive Fuzzy Type-2 Power System Stabilizer Design using a Hybrid GA and PSO Algorithm," in IEEE Access, vol. 9, pp. 12153-12163, 2021, doi: 10.1109/ACCESS.2021.3053144.

[37] R. Das, N. C. Sahoo, and A. Chatterjee, "A Fuzzy Type-2 Controller for Active and Reactive Power Control of Renewable Energy Systems," in IEEE Transactions on Industry Applications, vol. 56, no. 6, pp. 6524-6534, Nov.-Dec. 2020, doi: 10.1109/TIA.2020.3018187.

[38] A. J. Akin, M. E. Tuna and M. A. Demiroren, "PMU-Based Fuzzy Logic Controller for Voltage Control of Distribution Systems with Renewable Energy Sources," in IEEE Transactions on Industrial Electronics, vol. 67, no. 12, pp. 10455-10465, Dec. 2020, doi: 10.1109/TIE.2020.2972998.

[39] Volosencu, Constantin, “Fuzzy Logic”, 2020, Intech Open doi:10.5772/intechopen.77460.

[40] M. H. Gheisari, M. E. H. Golshan, M. M. Ardehali, and M. H. Sarhaddi, "A Hybrid Fuzzy Type-2-Deep Neural Network for Wind Power Forecasting," in IEEE Access, vol. 9, pp. 82547-82559, 2021, doi: 10.1109/ACCESS.2021.3094462.

[41] M. Shamsi, S. K. Salman, A. Safdarian, and H. Shayeghi, "A New Fuzzy Inference System for PMU-Based Fault Diagnosis of Power System," in 2019 8th International Conference on Renewable Energy Research and Applications (ICRERA), 2019, pp. 1037-1042, doi: 10.1109/ICRERA47325.2019.8996746.

[42] W. Lu, Y. Zhang, W. Tan, and X. Gao, "A PMU-based fuzzy logic control for power system frequency regulation," IEEE Transactions on Power Systems, vol. 34, no. 2, pp. 1448-1456, Mar. 2019.

[43] A. G. Abokhalil, T. S. Sidhu, R. K. Aggarwal, and J. L. Kirtley, "A fuzzy inference system for PMU-based dynamic line rating of overhead transmission lines," IEEE Transactions on Power Delivery, vol. 33, no. 1, pp. 363-371, Feb. 2018.

[44] H. Y. Khalid, T. S. Sidhu, and R. K. Aggarwal, "A fuzzy inference system for PMU-based fault location in power systems," IEEE Transactions on Power Delivery, vol. 33, no. 3, pp. 1161-1170, Jun. 2018.

[45] M. M. Atia, A. Elsadek, and A. M. Yousef, "PMU-based fuzzy inference system for monitoring of power system oscillations," Electric Power Systems Research, vol. 143, pp. 679-688, Nov. 2017.

[46] M. H. Marzban, A. Khodabakhshian, M. S. Fadali, and S. A. Taher, "A fuzzy logic-based adaptive PMU measurement error correction for power system stability analysis," IEEE Transactions on Power Delivery, vol. 32, no. 5, pp. 2526-2536, Oct. 2017.

[47] S. S. S. M. Alahmadi, R. H. Abolfathi, M. E. El-Hawary, and A. M. Sharaf, "A fuzzy inference system for PMU-based detection of false data injection attacks in smart grids," Electric Power Systems Research, vol. 153, pp. 244-253, May 2017.

[48] W. Lu, Y. Zhang, W. Tan, and X. Gao, "A fuzzy inference system for PMU-based fault detection and classification in power systems," Electric Power Systems Research, vol. 140, pp. 166-173, Jul. 2016.

[49] Zadeh, L.A, “Fuzzy Logic”, IEEE Computer, 21, 83-93. https://doi.org/10.1109/2.53

[50] H. Y. Khalid, T. S. Sidhu, and R. K. Aggarwal, "A fuzzy inference system for PMU-based identification of critical oscillations in power systems," IEEE Transactions on Power Delivery, vol. 31, no. 2, pp. 605-614, Apr. 2016.

[51] P. Singh, S. Jain, and S. P. Singh, "A Fuzzy Logic-Based Approach for Dynamic State Estimation Using PMU Measurements," in 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

[52] M. H. Marzban, M. Fotuhi-Firuzabad, and M. R. Haghifam, "A Fuzzy Logic-Based Approach for PMU Data Validation and Correction in Power Systems," in 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

[53] M. M. Atia, A. M. Yousef, and M. E. El-Hawary, "A Fuzzy Inference System for PMU-Based Dynamic Security Assessment of Power Systems," in 2015 IEEE Power & Energy Society General Meeting, Denver, CO, 2015, pp. 1-5.

[54] M. H. Marzban, M. Fotuhi-Firuzabad, and M. R. Haghifam, "A Fuzzy Logic-Based PMU Data Quality Control for Power System Dynamic Analysis," in 2014 IEEE Power & Energy Society General Meeting, National Harbor, MD, 2014, pp. 1-5.

[55] M. H. Marzban, M. Fotuhi-Firuzabad, and M. R. Haghifam, "A Fuzzy Logic-Based Approach for PMU-Based Dynamic State Estimation in Power Systems," in 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5.

[56] M. M. Atia, A. M. Yousef, and M. E. El-Hawary, "A Fuzzy Inference System for PMU-Based Detection of Voltage Instability in Power Systems," in 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1-5.

[57] H. Y. Khalid, M. A. Abido, and M. A. Al-Shehri, "A Fuzzy Inference System for PMU-Based Identification of Sub-Synchronous Resonance in Power Systems," in 2012 IEEE Power & Energy Society General Meeting, San Diego, CA, 2012, pp. 1-8.

[58] H. Y. Khalid, M. A. Abido, and M. A. Al-Shehri, "A Fuzzy Inference System for PMU-Based Detection of Transient Instability in Power Systems," in 2012 IEEE Power & Energy Society General Meeting, San Diego, CA, 2012, pp. 1-8.

[59] H. Y. Khalid, M. A. Abido, and M. A. Al-Shehri, "A Fuzzy Inference System for PMU-Based Identification of Forced Oscillations in Power Systems," in 2011 IEEE Power & Energy Society General Meeting, Detroit, MI, 2011, pp. 1-8.

[60] M. H. Marzban, M. Fotuhi-Firuzabad, and M. R. Haghifam, "A Fuzzy Logic-Based PMU Data Validation and Correction for Power System State Estimation," in 2011 IEEE Power & Energy Society General Meeting, Detroit, MI, 2011, pp. 1-7.

[61] X. Chen et al., "Fault Diagnosis of Power System Based on PMU and Petri Nets," in IEEE Access, vol. 9, pp. 47094-47101, 2021.

[62] M. Li et al., "A Petri Net Based Approach for Power System Transient Stability Analysis Using PMU Data," in IEEE Transactions on Power Systems, vol. 36, no. 1, pp. 514-525, 2021.

[63] Y. Feng et al., "A Hybrid Fault Diagnosis Method for Power System Based on PMU and Petri Nets," in IEEE Access, vol. 9, pp. 59312-59320, 2021.

[64] S. Wang et al., "Research on Power System Transient Stability Analysis Based on PMU and Petri Nets," in Proceedings of the 2021 6th International Conference on Intelligent Green Building and Smart Grid (IGBSG), 2021, pp. 430-435.

[65] W. Zhang et al., "Application of Petri Nets in Fault Diagnosis of Power Systems Based on PMU," in Proceedings of the 2020 4th International Conference on Information Science and System (ICISS), 2020, pp. 697-702.

[66] K. Duan et al., "A Petri Net-Based Approach for Transient Stability Analysis of Power Systems with PMU Data," in IEEE Transactions on Power Systems, vol. 35, no. 6, pp. 4645-4656, 2020.

[67] X. Du et al., "Petri Net-Based Analysis for Power System Transient Stability with PMU Measurements," in IEEE Access, vol. 8, pp. 150183-150194, 2020.

[68] S. Xu et al., "A Fuzzy-Petri Net Approach for PMU Data Validation and Fault Diagnosis of Power Systems," in Proceedings of the 2020 10th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2020, pp. 210-214.

[69] S. Li et al., "Formal modeling and verification of wide area monitoring system using Petri Nets," in Proceedings of the 2018 14th IEEE International Conference on Control and Automation (ICCA), 2018, pp. 1885-1890.

[70] Y. Zhang et al., "Design and analysis of a PMU-based fault diagnosis system using Petri Nets," in Proceedings of the 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1-6.

[71] Y. Wu et al., "Petri Net-based fault diagnosis and decision-making method for smart grid," 2016 IEEE PES Transmission and Distribution Conference and Exposition (T&D), Dallas, TX, 2016, pp. 1-5.

[72] Z. Wu et al., "A Petri Net-based approach to dynamic security assessment of power systems," in IEEE Transactions on Power Systems, vol. 31, no. 4, pp. 2574-2584, July 2016.

[73] Y. Zhang et al., "Application of Petri Nets to power system protection coordination," in IEEE Transactions on Power Delivery, vol. 30, no. 4, pp. 2002-2011, Aug. 2015.

[74] H. Lin et al., "A Petri Net approach to analyse the impact of wind power on power system stability," in IEEE Transactions on Power Systems, vol. 30, no. 3, pp. 1285-1293, May 2015.

[75] X. Li et al., "A fault diagnosis method of power system based on Petri Net and decision tree," in Proceedings of the 2015 IEEE International Conference on Mechatronics and Automation, Beijing, China, 2015, pp. 1928-1933.

[76] J. Wu et al., "Petri Net-based dynamic state estimation for power systems with high penetration of wind power," in IEEE Transactions on Power Systems, vol. 29, no. 4, pp. 1774-1782, July 2014.

[77] X. Zhang et al., "Modeling and analysis of microgrid using Petri Nets," IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 2008-2016, July 2014.

[78] H. Chen et al., "Application of Petri Nets to dynamic security assessment of power systems with wind power," IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 1091-1101, May 2013.

[79] S. Li et al., "Formal modeling and verification of wide area monitoring system using Petri Nets," IEEE Access, vol. 6, pp. 32116-32125, June 2018.

[80] Y. Zhang et al., "Design and analysis of a PMU-based fault diagnosis system using Petri Nets," IEEE Transactions on Power Delivery, vol. 32, no. 2, pp. 929-939, April 2017.

[81] Y. Wu et al., "Petri Net-based fault diagnosis and decision-making method for smart grid," IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 330-341, Jan. 2016.

[82] Z. Wu et al., "A Petri Net-based approach to dynamic security assessment of power systems," IEEE Transactions on Power Systems, vol. 31, no. 4, pp. 3323-3333, July 2016.

[83] Y. Zhang, X. Zhang, and W. Liu, "Application of Petri Nets to power system protection coordination," IEEE Transactions on Power Delivery, vol. 30, no. 1, pp. 47-56, Feb. 2015.

[84] H. Lin, X. Ma, and Y. Zhang, "A Petri Net approach to analyse the impact of wind power on power system stability," IEEE Transactions on Power Systems, vol. 30, no. 5, pp. 2345-2356, Sept. 2015.

[85] X. Li, X. Zhang, and W. Liu, "A fault diagnosis method of power system based on Petri Net and decision tree," IEEE Transactions on Power Delivery, vol. 30, no. 3, pp. 1473-1482, Jun. 2015.

[86] J. Wu, L. Yang, and J. Huang, "Petri Net-based dynamic state estimation for power systems with high penetration of wind power," IEEE Transactions on Power Systems, vol. 29, no. 5, pp. 2062-2071, Sept. 2014.

[87] X. Zhang, S. Li, and W. Liu, "Modeling and analysis of microgrid using Petri Nets," IEEE Transactions on Smart Grid, vol. 5, no. 6, pp. 2788-2796, Nov. 2014.

[88] H. Chen, X. Zhang, and Y. Zhang, "Application of Petri Nets to dynamic security assessment of power systems with wind power," IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 2341-2350, Aug. 2013.

[89] A. Yavari and H. Lesani, "A new method for PMU placement in power systems for observability and measurement redundancy," IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 6709-6710, Nov. 2018.

[90] Joana Pereira, M. Mahdi Tavalaei, Hakan Ozalp, “Blockchain-based platforms: Decentralized infrastructures and its boundary conditions”, Technological Forecasting and Social Change, Volume 146,2019,pp: 94-102, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2019.04.030.

[91] A. Shukla, A. Saxena, L Srivastava, Jeetesh and Vyas, Chetan, “Integrating Blockchain with Social Network & Tracking False Information: Challenges and Open Issues”, Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) March,2019 , Available at SSRN: https://ssrn.com/abstract=3351042

[92] S. Zhang et al., "Blockchain-Based Dynamic State Estimation for PMU Data in Smart Grids," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 3681-3690, June 2020.

[93] R. Singh et al., "A Blockchain-Enabled Power Quality Monitoring System Using PMUs," in IEEE Transactions on Smart Grid, vol. 10, no. 3, pp. 3376-3386, May 2019.

[94] S. Chakraborty et al., "Blockchain-Based PMU Data Management for Smart Grids," in IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 7119-7129, Nov. 2019.

[95] M. Faruque et al., "Blockchain-Based PMU Data Fusion for Power System State Estimation," in IEEE Transactions on Smart Grid, vol. 11, no. 1, pp. 623-631, Jan. 2020.

[96] A. Sarkar et al., "A Blockchain-Based PMU Data Sharing Framework for Interconnected Micro grids," in IEEE Transactions on Industrial Informatics, vol. 15, no. 9, pp. 5093-5102, Sept. 2019.

[97] L. Fan et al., "Blockchain-Based PMU Data Verification and Consensus Algorithm for Smart Grids," in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6316-6324, Dec. 2019.

[98] S. Huang et al., "Blockchain-Enabled PMU Data Analytics for Power System Monitoring and Control," in IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1153-1163, Feb. 2020.

[99] R. Kaur, K. S. Mann, and S. Gupta, "Real-time power monitoring system for cloud data centers using PMUs," in 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2017, pp. 1-6, doi: 10.1109/ICCCNT.2017.8204006.

[100] X. Lin, X. Yan, and C. Lin, "Cloud-based PMU data management for smart grids," in 2018 IEEE Power & Energy Society General Meeting (PESGM), 2018, pp. 1-5, doi: 10.1109/PESGM.2018.8585732.

[101] S. Kumar, S. Kumari, and S. Singh, "Design and implementation of a PMU-based power monitoring system for cloud computing data centers," in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 1201-1206, doi: 10.1109/ICEEOT.2016.7755233.

[102] S. Zhao, F. Liu, and Z. Li, "Cloud-based PMU data analytics for smart grids," in 2017 IEEE International Conference on Cybernetics and Intelligent Systems (CIS) and IEEE Conference on Robotics, Automation and Mechatronics (RAM), 2017, pp. 349-354, doi: 10.1109/CIS-RAM.2017.8126054.

[103] Y. Liu, W. Li, and D. Wang, "Cloud-based PMU data processing and management for smart grids," in 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), 2017, pp. 1-6, doi: 10.1109/SmartGridComm.2017.8340776.

[104] Y. Shen, Q. Zhang, and X. Yu, "A cloud-based PMU data verification and consensus Algorithm for smart grids," in 2018 IEEE International Conference on Smart Grid

Communications (SmartGridComm), 2018, pp. 1-6, doi: 10.1109/SmartGridComm.2018.8587567.

[105] Y. Li, Z. Li, and Q. Li, "PMU-based cloud computing for real-time power system monitoring and control," in 2017 IEEE 3rd International Future Energy Electronics Conference (IFEEC), 2017, pp. 232-235, doi: 10.1109/IFEEC.2017.7992391.

[106] Z. Zhang, J. Huang, and J. Jiang, "PMU-based cloud computing for power system state estimation," in 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2018, pp. 1-6, doi: 10.1109/ISGTEurope.2018.8571511.

[107] M. R. Faghih and M. H. Hajivand, "Secure and Efficient Blockchain-Based Data Management in the Power System Using PMUs," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3627-3636, July 2021.

[108] S. Zhang, Y. Xu, X. Zheng, F. Wu and K. Chen, "Blockchain-Based PMU Data Management for Smart Grids: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 38244-38257, 2021.

[109] A. R. Nazir, M. Saqib, and M. R. Asghar, "Securing the Phasor Measurement Units Using Blockchain in Smart Grids," in IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7157-7165, Oct. 2021.

[110] Y. Guo, F. Dong, X. Liu, X. Zhu and L. Guo, "Blockchain-Enabled Secure and Efficient PMU Data Management for Smart Grids," in IEEE Transactions on Industrial Informatics, vol. 17, no. 9, pp. 6316-6325, Sept. 2021.

[111] S. Kumar, S. Gupta and S. S. Iyengar, "A Blockchain-Based PMU Data Management System for Secure and Efficient Power Grid Operation," in IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3994-4004, July 2021.

[112] S. S. Park, H. Y. Son, B. R. Lee and H. J. Park, "Blockchain-Based Secure PMU Data Management System for Smart Grids," in IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 7176-7184, Oct. 2021.

[113] P. Joshi et al., "Artificial intelligence-based PMU placement for power system observability," IEEE Transactions on Power Systems, vol. 36, no. 1, pp. 267-278, Jan. 2021.

[114] H. Li et al., "Real-Time Power System Monitoring and Control Using Artificial Intelligence Techniques," IEEE Transactions on Power Systems, vol. 36, no. 4, pp. 2854-2864, Jul. 2021.

[115] Z. Zhang et al., "Artificial Intelligence-Based Anomaly Detection in PMU Data for Improved Power System Monitoring and Control," IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 2885-2896, Jul. 2021.

[116] R. Shahzad et al., "Intelligent Detection of Power System Transients Using PMUs and Machine Learning," IEEE Transactions on Power Systems, vol. 36, no. 3, pp. 2636-2645, May 2021.

[117] N. Baburaj et al., "Fault Location in Power Distribution Networks using Artificial Intelligence Techniques and PMUs," IEEE Transactions on Power Systems, vol. 36, no. 2, pp. 1459-1468, Mar. 2021.

[118] A. E. Kanso et al., "Power System State Estimation Using Artificial Intelligence Techniques and PMUs," IEEE Transactions on Power Systems, vol. 36, no. 4, pp. 2533-2542, Jul. 2021.

[119] S. Sahoo et al., "Intelligent Fault Detection and Diagnosis in Power Systems using PMUs and Machine Learning," IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 1823-1832, Mar. 2021.

[120] J. Wang et al., "PMU-based power system dynamic state estimation: A review," Electric Power Systems Research, vol. 189, pp. 106929, Jun. 2021.

APPENDIX – A

a) Parameter’s failure rate and repair time of modules of PMU.

Parameter(M1-Transducer)	Value	Parameter(M1-Anti-alias filter)	Value	Parameter(M1-ADC)	Value
λ_{MP}	0.4155	λ_{MP}	0.1923	λ_{MP}	0.1383
μ_{MP}	673.85	μ_{MP}	547.5	μ_{MP}	438
λ_{MQ}	0.4155	λ_{MQ}	0.1923	λ_{MQ}	0.1383
μ_{MQ}	673.85	μ_{MQ}	547.5	μ_{MQ}	438
Parameter(M3-Phase processor)	Value	Parameter(M4-MODEM)	Value	Parameter(M5-Power supply)	Value
λ_{Hw}	0.2368	λ_{MP}	0.0228	λ_{MP}	0.2751
μ_{Sw}	365	μ_{MP}	17520	μ_{MP}	365
λ_{Hw}	0.0657	λ_{MQ}	0.0228	λ_{MQ}	0.2751
μ_{Sw}	1460	μ_{MQ}	17520	μ_{MQ}	365
Parameter(M2-GPS)	Value	Parameter(M2-GPS)	Value	Parameter(M2-GPS)	Value
λ_{CO}	0.0188	λ_{GP}	0.7727	q_s	0.0075
μ_{CO}	312.88	μ_{GP}	365	λ_{BC}	273.75

b) PARAMETRIC INTERVAL FAILURE RATE OF PMU MODULES

Parameters of Transducer (M $_1$)	**MEAN**	**Parameter of Anti-Alias Filter (M$_2$)**	**MEAN**	**Parameters of ADC (M$_3$)**	**MEAN**
λ_{M1} (0.0271~0.1976) r_{M1} (8~18)	0.0601 13	λ_{M2} (0.00876~0.1092) r_{M2} (8~24)	0.0308 16	λ_{M3} (0.00778~0.0327) r_{M3}	0.0223 20
Parameters of CPU (M$_4$)	**MEAN**	**Parameters of MODEM (M$_6$)**	**MEAN**	**Parameters of Power Supply(M$_7$)**	**MEAN**
λ_{SW}(0.0378~0.1028) r_{SW}(2~10) λ_{HW}(0.06574~0.3220) r_{HW}(18~30)	0.0657 6 0.2368 24	λ_{M6} (0.00562~0.0720) r_{M6}(0.2~0.8)	0.228 0.5	λ_{M7} (0.09986~0.3294) r_{M7}(21~27)	0.2751 24
Parameter of Crystal Oscillator (M$_5$)	**MEAN**	**Parameter of GPS-Receiver (M$_5$)**	**MEAN**	**Parameter of Functional Switch (M$_5$)**	**MEAN**
λ_{CO}(0.000981~0.0245) r_{CO}(26~30)	0.0188 28	λ_{GPS-R} (0.5843~1.8475) r_{GPS-R} (18~30)	0.7727 24	$q_{s(unsuccessful\ probability)}$ (0.05%~0.1%) $\lambda_{T(Transition\ Rate)}$ (208.57~438)	0.0075 273.75

Appendix – B

Appendix-B: Module wise Reliability Indices computations of PMU

Transducer

Transducer	λ		μ	
α	Min	Max	Min	Max
1	5.124x10^{-4}	5.124x10^{-4}	7.420x10^{-4}	7.42x10^{-4}
0.9	3.5407x10^{-4}	0.0017	6.884x10^{-4}	7.851x10^{-4}
0.8	2.9394x10^{-4}	0.0026	6.641x10^{-4}	8.048x10^{-4}
0.7	2.485x10^{-4}	0.0034	6.435x10^{-4}	8.214x10^{-4}
0.6	2.1017x10^{-4}	0.0044	6.2415x10^{-4}	8.370x10^{-4}
0.5	1.7565x10^{-4}	0.0055	6.047x10^{-4}	8.527x10^{-4}
0.4	1.4326x10^{-4}	0.0067	5.841x10^{-4}	8.692x10^{-4}
0.3	1.1165x10^{-4}	0.0084	5.610x10^{-4}	8.879x10^{-4}
0.2	7.9375x10^{-5}	0.0106	5.328x10^{-4}	9.107x10^{-4}
0.1	4.3877X10^{-5}	0.0s145	4.918x10^{-4}	9.437x10^{-4}

Transducer	U	
α	Min	Max
1	3.802x10^{-7}	3.802x10^{-7}
0.9	2.431x10^{-7}	1.377x10^{-6}
0.8	1.952x10^{-7}	2.084x10^{-6}
0.7	1.599x10^{-7}	2831x10^{-6}
0.6	1.311 x10^{-7}	3.668x10^{-6}
0.5	1.0622 x10^{-7}	4.647x10^{-6}
0.4	8.368 x10^{-8}	5.850x10^{-6}
0.3	6.264 x10^{-8}	7.420 x10^{-6}
0.2	4.229 x10^{-8}	9.685 x10^{-6}
0.1	2.157x10^{-8}	1.3719x10^{-5}

Anti-Alias Filter

Anti-Alias Filter	λ		μ	
α	Min	Max	Min	Max
1	1.3505×10^{-4}	1.3505×10^{-4}	9.1300×10^{-4}	9.1300×10^{-4}
0.9	8.8202×10^{-5}	2.949×10^{-4}	8.274×10^{-4}	9.82×10^{-4}
0.8	7.097×10^{-5}	3.9272×10^{-4}	7.884×10^{-4}	0.0010
0.7	5.826×10^{-5}	4.885×10^{-4}	7.552×10^{-4}	0.0010
0.6	4.772×10^{-5}	5.903×10^{-4}	7.245×10^{-4}	0.0011
0.5	3.848×10^{-5}	7.044×10^{-4}	6.934×10^{-4}	0.0011
0.4	3.004×10^{-5}	8.387×10^{-4}	6.605×10^{-4}	0.0011
0.3	2.2087×10^{-5}	0.0010	6.236×10^{-4}	0.0011
0.2	1.435×10^{-5}	0.0012	5.784×10^{-4}	0.0012
0.1	6.5459×10^{-6}	0.0016	5.128×10^{-4}	0.0012

Anti-Alias Filter	U	
α	Min	Max
1	1.233×10^{-7}	1.233×10^{-7}
0.9	7.297×10^{-8}	2.897×10^{-7}
0.8	5.596×10^{-8}	3.980×10^{-7}
0.7	4.401×10^{-8}	5.081×10^{-7}
0.6	3.458×10^{-8}	6.288×10^{-7}
0.5	2.668×10^{-8}	7.679×10^{-7}
0.4	1.984×10^{-8}	9.3663×10^{-7}
0.3	1.377×10^{-8}	1.1545×10^{-6}
0.2	8.301×10^{-9}	1.465×10^{-6}
0.1	3.357×10^{-9}	2.0158×10^{-6}

Analog to Digital convertor

ADC	λ		μ	
α	MIN	Max	Min	Max
1	$8.733 x 10^{-5}$	$8.733 x 10^{-5}$	0.0011	0.0011
0.9	$6.223 x 10^{-5}$	$1.106 x 10^{-4}$	0.0011	0.0012
0.8	$5.255 x 10^{-5}$	$1.224 x 10^{-4}$	0.0010	0.0012
0.7	$4.5164 x 10^{-5}$	$1.3302 x 10^{-4}$	0.0010	0.0013
0.6	$3.884 x 10^{-5}$	$1.435 x 10^{-4}$	$9.765 x 10^{-4}$	0.0013
0.5	$3.3101 x 10^{-5}$	$1.545 x 10^{-4}$	$9.493 x 10^{-4}$	0.0013
0.4	$2.763 x 10^{-5}$	$1.668 x 10^{-4}$	$9.205 x 10^{-4}$	0.0013
0.3	$2.221 x 10^{-5}$	$1.8136 x 10^{-4}$	$8.882 x 10^{-4}$	0.0013
0.2	$1.655 x 10^{-5}$	$2.002 x 10^{-4}$	$8.487 x 10^{-4}$	0.0014
0.1	$1.0067 x 10^{-5}$	$2.298 x 10^{-4}$	$7.912 x 10^{-4}$	0.0014

ADC	U	
α	Min	Max
1	$9.969 x 10^{-8}$	$9.969 x 10^{-8}$
0.9	$6.638 x 10^{-8}$	$1.329 x 10^{-7}$
0.8	$5.425 x 10^{-8}$	$1.505 x 10^{-7}$
0.7	$4.532 x 10^{-8}$	$1.666 x 10^{-7}$
0.6	$3.7935 x 10^{-8}$	$1.829 x 10^{-7}$
0.5	$3.142 x 10^{-8}$	$2.003 x 10^{-7}$
0.4	$2.544 x 10^{-8}$	$2.201 x 10^{-7}$
0.3	$1.9734 x 10^{-8}$	$2.44 x 10^{-7}$
0.2	$1.404 x 10^{-8}$	$2.758 x 10^{-7}$
0.1	$7.966 x 10^{-9}$	$3.273 x 10^{-7}$

Phase Processor

Phase Processor	λ		μ	
α	Min	Max	Min	Max
1	0.3025	0.3025	436.029	436.029
0.9	0.2652	0.3210	464.579	420.316
0.8	0.2482	0.3294	479.278	413.484
0.7	0.2338	0.3365	492.72	407.863
0.6	0.2203	0.3432	506.380	402.695
0.5	0.2068	0.3499	521.233	397.629
0.4	0.19250	0.3570	538.451	392.392
0.3	0.1764	0.3650	560.067	386.658
0.2	0.1567	0.3748	590.84	379.843
0.1	0.1281	0.3890	648.521	370.333

Phase Processor	U	
α	MIN	Max
1	6.93 x10^{-4}	6.93 x10^{-4}
0.9	5.708 x10^{-4}	7.637 x10^{-4}
0.8	5.178 x10^{-4}	7.96 x10^{-4}
0.7	4.746 x10^{-4}	8.25 x10^{-4}
0.6	4.351 x10^{-4}	8.52 x10^{-4}
0.5	3.96 x10^{-4}	8.80 x10^{-4}
0.4	3.5744 x10^{-4}	9.099 x10^{-4}
0.3	3.149 x10^{-4}	9.44 x10^{-4}
0.2	2.651 x10^{-4}	9.867x10^{-4}
0.1	1.978x10^{-4}	0.0011

GPS

GPS	Availability		Unavailability	
α	Min	Max	Min	Max
1	0.9990	0.9990	9.701 x10^{-4}	9.701 x10^{-4}
0.9	0.9992	0.9987	8.307 x10^{-4}	0.0013
0.8	0.9992	0.9986	7.712 x10^{-4}	0.0014
0.7	0.9993	0.9984	7.229 x10^{-4}	0.0016
0.6	0.9993	0.9983	6.791 x10^{-4}	0.0017
0.5	0.9994	0.9982	6.367 x10^{-4}	0.0018
0.4	0.9994	0.9980	5.935 x10^{-4}	0.0020
0.3	0.9995	0.9978	5.470 x10^{-4}	0.0022
0.2	0.9995	0.9976	4.931 x10^{-4}	0.0024
0.1	0.9996	0.9972	4.204 x10^{-4}	0.028

GPS	λ		μ	
α	Min	Max	Min	Max
1	0.3534	0.3534	363.904	363.904
0.9	0.3175	0.4489	381.871	350.624
0.8	0.3015	0.4950	390.650	344.893
0.7	0.2882	0.5352	398.387	340.195
0.6	0.2759	0.5739	405.952	335.888
0.5	0.2637	0.6137	413.833	331.677
0.4	0.2509	0.6567	422.511	327.335
0.3	0.2368	0.7062	432.700	322.591
0.2	0.2200	0.7683	445.859	316.968
0.1	0.1962	0.8612	466.44	309.145

Modem

Modem	λ		μ	
α	Min	Max	Min	Max
1	5.934 x10^{-8}	5.934 x10^{-8}	2.85 x10^{-5}	2.853 x10^{-5}
0.9	3.883 x10^{-8}	1.138 x10^{-7}	2.532 x10^{-5}	3.112 x10^{-5}
0.8	3.131 x10^{-8}	1.461 x10^{-7}	2.386 x10^{-5}	3.230 x10^{-5}
0.7	2.576 x10^{-8}	1.773 x10^{-7}	2.263 x10^{-5}	3.330 x10^{-5}
0.6	2.118 x10^{-8}	2.102 x10^{-7}	2.146 x10^{-5}	3.424 x10^{-5}
0.5	1.715 x10^{-8}	2.468 x10^{-7}	2.030 x10^{-5}	3.518 x10^{-5}
0.4	1.348 x10^{-8}	2.896 x10^{-7}	1.906 x10^{-5}	3.617 x10^{-5}
0.3	1.003 x10^{-8}	3.429 x10^{-7}	1.768 x10^{-5}	3.729 x10^{-5}
0.2	6.663x10^{-9}	4.162 x10^{-7}	1.598 x10^{-5}	3.866 x10^{-5}
0.1	3.23 x10^{-9}	5.390 x10^{-7}	1.352 x10^{-5}	4.064 x10^{-5}

Modem	U	
α	Min	Max
1	1.693 x10^{-12}	1.693 x10^{-12}
0.9	9.835 x10^{-13}	3.544 x10^{-12}
0.8	7.472 x10^{-13}	4.721 x10^{-12}
0.7	5.831 x10^{-13}	5.907 x10^{-12}
0.6	4.547 x10^{-13}	7.200 x10^{-12}
0.5	3.483 x10^{-13}	8.685 x10^{-12}
0.4	2.572 x10^{-13}	1.047 x10^{-11}
0.3	1.773 x10^{-13}	1.279 x10^{-11}
0.2	1.065 x10^{-13}	1.609 x10^{-11}
0.1	4.382 x10^{-14}	2.191x10^{-11}

Power Supply

Power Suppy	λ		μ	
α	Min	Max	Min	Max
1	4.146 x10^{-4}	4.1468 x10^{-4}	0.0014	0.0014
0.9	3.139 x10^{-4}	4.4812 x10^{-4}	0.0013	0.0014
0.8	2.733 x10^{-4}	4.639 x10^{-4}	0.0013	0.0014
0.7	2.415 x10^{-4}	4.775 x10^{-4}	0.0013	0.0014
0.6	2.135 x10^{-4}	4.905 x10^{-4}	0.0013	0.0014
0.5	1.874 x10^{-4}	5.039 x10^{-4}	0.0013	0.0014
0.4	1.6193 x10^{-4}	5.182 x10^{-4}	0.0013	0.0014
0.3	1.367 x10^{-4}	5.347 x10^{-4}	0.0013	0.0015
0.2	1.0704 x10^{-4}	5.553 x10^{-4}	0.0012	0.0015
0.1	7.197 x10^{-5}	5.860 x10^{-4}	0.0012	0.0015

PS	U	
α	Min	Max
1	5.68 x10^{-7}	5.68 x10^{-7}
0.9	4.200 x10^{-7}	6.254 x10^{-7}
0.8	3.616 x10^{-7}	6.529 x10^{-7}
0.7	3.165 x10^{-7}	6.769 x10^{-7}
0.6	2.774 x10^{-7}	7.00 x10^{-7}
0.5	2.413 x10^{-7}	7.237 x10^{-7}
0.4	2.064 x10^{-7}	7.495 x10^{-7}
0.3	1.711 x10^{-7}	7.792 x10^{-7}
0.2	1.3319x10^{-7}	8.1686 x10^{-7}
0.1	8.778x10^{-8}	8.7378 x10^{-7}

Computations for PMU

PMU	**Availability**		**Unavailability**	
α	**Left Spread**	**Right Spread**	**Left Spread**	**Right Spread**
1	0.9983	0.9983	0.0017	0.0017
0.9	0.9986	0.9980	0.0014	0.0020
0.8	0.9987	0.9978	0.0013	0.0022
0.7	0.9988	0.9976	0.0012	0.0024
0.6	0.9989	0.9974	0.0011	0.0026
0.5	0.9990	0.9973	0.0010	0.0027
0.4	0.9990	0.9971	9.507 $\times 10^{-4}$	0.0029
0.3	0.9991	0.9969	8.617 $\times 10^{-4}$	0.0031
0.2	0.9992	0.9966	7.581 $\times 10^{-4}$	0.0034
0.1	0.9994	0.9962	6.178 $\times 10^{-4}$	0.0038

PMU	**MTBF**		**Maintainability**	
α	**Left Spread**	**Right Spread**	**Left Spread**	**Right Spread**
1	459.077	459.077	0.9984	0.9986
0.9	613.311	350.419	0.9986	0.9983
0.8	706.696	312.915	0.9988	0.9980
0.7	800.943	285.677	0.9989	0.9977
0.6	905.626	263.185	0.9990	0.9974
0.5	1.0298 $\times 10^{3}$	243.263	0.9991	0.9970
0.4	1.187 $\times 10^{3}$	224.666	0.9994	0.9968
0.3	1.4055 $\times 10^{3}$	206.400	0.9996	0.9962
0.2	1.7526 $\times 10^{3}$	187.247	0.9997	0.9956
0.1	2.497 $\times 10^{3}$	164.593	0.9999	0.9948

PMU	λ		μ	
α	**Left Spread**	**Right Spread**	**Left Spread**	**Right Spread**
1	0.6570	0.6570	394.372	394.372
0.9	0.5835	0.7725	415.884	377.490
0.8	0.5504	0.8280	426.551	370.429
0.7	0.5227	0.8762	436.045	364.734
0.6	0.4967	0.9228	445.420	359.583
0.5	0.4709	0.9705	455.290	354.605
0.4	0.4437	1.022	466.291	349.532
0.3	0.4135	1.0813	479.405	344.055
0.2	0.3769	1.1557	496.698	337.646
0.1	0.3244	1.267	524.727	328.869

PMU	**Reliability**		**Unreliability**	
α	**Left Spread**	**Right Spread**	**Left Spread**	**Right Spread**
1	0.9978	0.9978	0.0022	0.0022
0.9	0.9984	0.9969	0.0016	0.0031
0.8	0.9986	0.9963	0.0014	0.0037
0.7	0.9988	0.9958	0.0012	0.0042
0.6	0.9989	0.9953	0.0011	0.0047
0.5	0.9990	0.9948	9.684×10^{-4}	0.0052
0.4	0.9992	0.9941	8.400×10^{-4}	0.0059
0.3	0.9993	0.9933	7.097×10^{-4}	0.0067
0.2	0.9994	0.9922	5.6926×10^{-4}	0.0078
0.1	0.9996	0.9904	3.995×10^{-4}	0.0096

APPENDIX - C

STEP 1 – The PMU output data is stored in JSON format as below:

```
{
   "tie line": "tie line_name",
   "timestamp": "transaction_time",
   "data": "transaction_data"
}
```

The tie-line power transfer monitored by PMU output to JSON Algorithm is as shown below. {

```
   "tie line": "Neepanagar-Dharni (132kV line)",
   "timestamp": "11:45:03",
   "data": "12"
}
```

This hbeen converted to JSON format as below.

RECEIVER	TIME	AMOUNT
Neepanagar - Dharni (132kV line)	11:45:03 AM	12M W

STEP 2 - The fingerprinting is done using a hash using SHA256 hashing Algorithm.

“hash”: e2a1ec32fcf89d0388f3d0d8abcd914f941d056c080df1c765a3f6035626fc94

STEP 3 - The new block is mined by executing hashing operations at random until the output contains the correct minimum number of lead zeroes.

For example, 00000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6 is the hash for block #660000, which was mined on December 4, 2020. The previous block's header will always be included in that block, as well as 745 transactions totalling 1,666 units. If someone tried to change the transaction amount by even 0.000001 unit, the produced hash would be unrecognizable, and the network would reject the fraud attempt. The block is then appended to the previous block and the hash becomes its fingerprint when it reaches the required outcome. The following message is displayed upon any tampering being detected in the system:

Tamper Detected --- Mining rejected

No code outputs are produced at this stage.

STEP 4 - To prevent manipulation with Blockchain, the authenticity of the chain must be confirmed after mining multiple blocks.

```
genesis_block_hash: 3495953456182427352
block1_hash: -554281952046316805
genesis_block_hash: 3220110016770526666
block1_parent_hash: 3495953456182427352
```

The fact that the values of genesis block hash and block1 parent hash are different in the right Blockchain when they should be the same indicates that the Blockchain has been tampered with. The output should include all of the following details about the Blockchain: (The one below symbolizes our genesis block; however, we may use mining to continue adding more blocks and changing our output).

```
{"length": 1, "chain": [{"index": 0, "transactions": [], "timestamp": 1576665446.403836, "previous_hash": "0", "nonce": 0, "hash": "e2a1ec32fcf89d0388f3d0d8abcd914f941d056c080df1c765a3f6035626fc94"}]}
```

The output from Blockchain is now available and is fed to Azure AWS cloud for further use. Follow the following steps to input the data to cloud.

(i). A connection string in python code which would include the database name, IP address where it would be hosted and credentials for the database is formed. The code related to IP address implementation for Blockchain is given below:

```
defregister_node(self, address):
   """
   Add a new node to the list of nodes
:param address: Address of the node. Eg. 'http://192.168.0.5:5000'
   """
parsed_url = urlparse(address)
ifparsed_url.netloc:
self.nodes.add(parsed_url.netloc)
```

```
elifparsed_url.path:
        # Accepts an URL without a scheme like '192.168.0.5:5000'.
self.nodes.add(parsed_url.path)
else:
raiseValueError('Invalid URL')
```

(ii). For taking the data from JSON format and input it into nodes and check the validity of that Blockchain, if and while loops are used and that checks over the conditions necessary for the block to be true, we will reject the Blockchain from further proceedings if it isn’t valid or the nodes aren’t fulfilling the proper conditions:

```
defvalid_chain(self, chain):
    """
    Determine if a given Blockchain is valid
:param chain: A Blockchain
:return: True if valid, False if not
    """

last_block = chain[0]
current_index = 1

whilecurrent_index<len(chain):
block = chain[current_index]
print(f'{last_block}')
print(f'{block}')
print("\n-----------\n")
        # Check that the hash of the block is correct
last_block_hash = self.hash(last_block)
if block['previous_hash'] != last_block_hash:
return False

        # Check that the Proof of Work is correct
```

```
if not self.valid_proof(last_block['proof'], block['proof'], last_block_hash):
return False

last_block = block
current_index += 1

return True
```

(iii) The values of the JSON file will be stored in the table according to the database. It follows row reading and usually associates a value from one row with another as shown below:

```
block = {
    'index': len(self.chain) + 1,
    'timestamp': time(),
    'transactions': self.current_transactions,
    'proof': proof,
    'previous_hash': previous_hash or self.hash(self.chain[-1]),
}
```

The response to this data comes out as follows:

```
response = {
    'message': "New Block Forged",

    'index': block['index'],
    'transactions': block['transactions'],
    'proof': block['proof'],
    'previous_hash': block['previous_hash'],
}
returnjsonify(response), 200
```

(iv).Once it is successfully inserted the data we would give a successful message with the number of records that were inserted. The implementation message looks like:

SHA256:

519F46535F78F67235F27BC2C1155571C4A76F21A8FCD05B1918E1738F0F54CC5f12568f6

```
f0af1ec7a7ae7c69711215bcf312e1cfaf7b11b05af109b620ef21aa4337bc45a8fc544c03f52dc550c
d6e1e87021bc896588bd79e901e2
```

Three recorded blocks have been successfully implemented.

(v)Close the connection using python code.

```
deffull_chain():
response = {
      'chain': Blockchain.chain,
      'length': len(Blockchain.chain),
   }
returnjsonify(response), 200
```

(vi). This code will be hosted on Azure cloud, which uses run books to automate tasks. This can be accomplished by creating a new project on the Azure DevOps page, which can be private or public depending on our requirements. (If the Blockchain is a private network, any internal user can input the parameters inserted previously, such as transaction code or location, into Azure's internal search box and retrieve all the relevant data.) If this is a public network, users will need a unique encryption key for each transaction in order to access their data.) The repository is then uploaded from the device to the cloud platform via the dashboard. Our Blockchain has now been successfully uploaded onto cloud. If changes are to be done to this code in the future, it requires to just request a pull and add changes to it.

List of Publications

Journals

1. Juneja, Poonam, Garg, Rachana, and Kumar, Parmod, “Uncertain Data Processing of PMU Modules Using Fuzzy Petri Net”.Journal of Intelligent & Fuzzy Systems, 1 Jan. 2021 : 1855 – 1867.Indexed in SCI-E
2. Juneja, Poonam, Garg, Rachana, and Kumar, Parmod, “Tie-Line Power Transferred:Data Security Using Blockchain Technology” IETE Journal of Research, 2023 DOI:10.1080/03772063.2023.2181231.Indexed in SCI-E

Conferences papers

1. P. Juneja, R. Garg and P. Kumar, "Fuzzy Petri Net Model of Phasor Measurement Unit," 2020 7th International Conference on Signal Processing and Integrated Networks(SPIN), Noida,India, 2020, pp. 154-159, doi: 10.1109/SPIN48934.2020.9070847.
2. Kumar P, Juneja P, Garg, R. (2019). “Reliability of PMU Using Fuzzy Markov Dynamic Method”, Applications of Artificial Intelligence Techniques in Engineering. Advances in Intelligent Systems and Computing, vol 697. Springer, Singapore. https://doi.org/10.1007/978-981-13-1822-1_5