

MAKERERE UNIVERSITY

COLLEGE OF ENGINEERING, DESIGN, ART AND TECHNOLOGY

SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

PROJECT REPORT

Application of IEC 61850 services for Protection, Automation, Control (PAC) Functionalities and Asset Management Applications in Medium-Voltage and Low-Voltage grid Networks in Uganda. (Case Study Area-Kampala Metropolitan-Wandegeya Feeder)

MUWANGUZI EMMA 21/U/1359

MAIN SUPERVISOR: Dr. MURTALA AMINU BABA

CO. SUPERVISOR: Dr. DATIVA TIZIKARA

A Report Submitted in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Science in Electrical Engineering at Makerere University.

June 2026

DECLARATION

I, MUWANGUZI EMMA, hereby declare that I have personally carried out the work presented in this report in partial fulfilment of the requirements for the award of Bachelor of Science in Electrical Engineering at Makerere University. This report is a true and original account of my project work and has not been submitted to any other institution for any academic award.

Signature:…………Date:……26/06/2026……

CONSENT FORM

Digitisation and Self-Archiving Consent Agreement: Theses

Agreement between Makerere University & Students (Authors of Theses / Dissertations / Reports)

1. The author is a student of Makerere University and author of the thesis / dissertation / report titled:
Application of IEC 61850 services for Protection Automation, Control (PAC) functionality and Asset Management Applications in Medium and low voltage grid Networks in Uganda. (Case Study of Kampala Metropolitan-fiches on Nandegeya feeder)

2. The author grants to the University:
   a. The right to deposit the electronic version of the Thesis / Dissertation / Report into Makerere University Institutional Repositories (Mak IR) or (Mak UD); and
   b. The right to store the thesis / dissertation / report in Mak IR / Mak UD and make it permanently available to the general public via the Internet at no cost to the general public after a grace period (if any is specified). **Choose one of the three options below (c, d, or e):**
   c. The Author may opt for immediate open access to the public ..... ✓ Access Granted
   d. Or Restrict access indefinitely: .....
   e. Or Restrict access for the specified number of years: .....
   f. Reason for restriction: .....

3. The author warrants that to the best of the authors knowledge and belief:
   a. The thesis / dissertation / report is an original work;
   b. The author is the owner of all the intellectual property in the thesis / dissertation
   or
   c. The Author is entitled to deal with the intellectual property in the thesis / dissertation / report by publishing it on the Internet
   d. The Author has the right, power and authority to enter into this Agreement and to grant the University the rights contained in this Agreement; and
   e. The University's use of the thesis / dissertation / report pursuant to this Agreement will not infringe the intellectual property rights of any third party.

4. The Author acknowledges and agrees that the University is not responsible or liable for any breach of the intellectual property rights in the thesis / dissertation / report, in particular any breach of copyright, as a result of the use of the thesis / dissertation / report pursuant to this Agreement.

5. The University acknowledges that the rights granted by the Creator in clause 2 of this Agreement, do not cause any transfer or assignment of any proprietary rights in the intellectual property in the article to the University.

Signed by the Author as confirmation that the Author has read and accepted the terms of this Agreement:

Name: MUWANGUZI EMMA

College: CEDAT School: School of Engineering

(Tick) Type of Degree: (Undergraduate / PGD / Masters / PhD), Reg. No.: 21/U/1359

Tel No.: 0707479590 E-Mail: mziemma111@gmail.com

Signature: Date: 20th Oct, 2026

Supervisor's endorsement: Dr. M. A. Bala 21/10/2026

MakIRs Policy

APPROVAL

This is to certify that the project work detailed in this report was carried out under my supervision. I hereby confirm that the work was undertaken in partial fulfillment of the requirements for degree of electrical engineering, and that the student conducted the project with diligence and adherence to the prescribed guidelines. I have reviewed the report and find that it accurately reflects the efforts and outcomes of the project.

DR. MURTALA AMINU BABA

Senior Lecturer, College of Engineering, Design, Art, and Technology, Makerere University, Kampala

Signature……

Date……23rd June 2026.

DR. DATIVA TIZIKARA

Lecturer, college of Engineering Makerere University

Signature……

Date……26/06/2026

Table of Contents

DECLARATION ii
CONSENT FORM iii
APPROVAL iv
List of Figures viii
List of Tables x
Acronyms and Symbols xi
List of equations xi
Abstract xii
Aknowledgements xiii
CHAPTER ONE 1
INTRODUCTION 1
1.1 Project Background 1
1.2 Problem Statement 2
1.3 Objectives 3
1.3.1 Main Objective 3
1.3.2 Specific Objectives 3
1.4 Significance of The Project 3
CHAPTER TWO 5
LITERATURE REVIEW 5
2.1 The Power System 5
2.2 Existing Power Grid Controls 6
2.3 The need for enhanced grid control 7
2.4 General Function Categories in PAC Systems 8
2.5 Communication Interfaces 11
2.6 Communication Nodes 11
2.7 Functional Relationships 14
2.8 Communication network core 20
2.9 Security and Privacy in Communications Infrastructure for MV and LV Grid Sections 22
2.10 Principles of Modern Network Design: VLAN Architecture and Convergence 25
2.101 Strategic VLAN Design (IEEE 802.1Q) 25
2.102 Scaling with Q-in-Q: CVLANs and SVLANs (IEEE 802.1ad) 25
2.103 Running a Converged Network 26

2.11 IEC 61850 Model **26**
1.111 IEC 61850 Logical Node Object Model 27
1.112 IEC 61850 Server Object Model 27
1.113 The IEC 61850 Data Model 28
2.12 IEC 61850 Requirements **29**
2.13 Modeling Requirements in MV and LV Networks **30**
2.14 Modeling Multifunctional IEDs in MV/LV Networks **31**
2.15 The IEC 61850 Standard and Related Documents **31**
2.16 IEC 61850 Sampled Value **33**
2.161 IEC 61850 Sampled Value Model 33
2.162 Busbar Differential Protection 33
2.163 Disturbance Recording 34
2.164 Communication Considerations 34
2.17 IEC 61850 GOOSE **35**
2.171 Reducing Fault Duration on Distribution Feeders 35
2.172 Adapting to Faults on Adjacent Feeders 36
2.173 Adapting to the Loss of a Protection IED 36
2.174 GOOSE Applications for Transmission Line Protection 37
2.175 GOOSE Applications in System Integrity Protection Schemes (SIPS) 37
CHAPTER THREE 39
PROJECT EXECUTION METHOODOLOGY 39
3.1 PHASE ONE: EMPIRICAL DATA COLLECTION AND AGGREGATION **40**
3.1.1 Grid Data Gathered 40
3.1.2 Fiber Network Data Gathered 42
3.1.3 Proposed Power Utility Network Architecture 45
3.2 PHASE TWO: TECHNICAL ANALYSIS AND EVALUATION. **50**
3.2.1 Baseline Analysis 51
3.2.2 Simulation Methodology 55
3.2.3 Simulation Environment: OMNET++ AND INET 57
3.2.4 Network Architecture and Physical Layer Modeling 58
3.2.5 Logic Implementation and Simulation Constraints 77
3.2.6 Network Assessment and Simulation Theory 85
3.2.7 Traffic Modeling and Stress Testing 135

CHAPTER FOUR 137
RESULTS AND ANALYSIS 137
4.1 Utilization Analysis **137**
4.1.1 Dedicated Architecture 137
4.1.2 Shared GPON 139
4.2 Clock Synchronization Accuracy **149**
4.2.1 Dedicated 149
4.2.2 Shared GPON 151
4.3 Goose Protection Latency **154**
4.3.1 Dedicated 154
4.3.2 Shared GPON 155
CHAPTER FIVE 159
CHALLENGES, CONCLUSION AND RECOMMENDATION 159
5.1 Challenges and Limitations **159**
5.2 Recommendations for Future Work **159**
5.3 Conclusion **160**
REFERENCES 161

List of Figures

Figure 1. schematic illustrating the approximate feeder display for the Wandegeya Feeder from KAMPALA NORTH Substation grid segment. 41
Figure 2. The configuration of the Optical Line Terminal (OLT) tier. 45
Figure 3. Logical flow diagram showing substations and feeder linkage. 45
Figure 4. Logical flow diagram indicating how grid flow intersects with residential traffic flow. 46
Figure 5. Dedicated architecture to serve as a benchmark test. 47
Figure 6. layout representing the baseline edge model implemented across the simulation framework to evaluate local traffic behavior, signal propagation, and bottlenecking at the feeder level. 47
Figure 7. schematic representation of the proposed network 48
Figure 8. Feeder level network layout-Feeder service area and substation area served by separate Olt. 49
Figure 9. Feeder level network layout-Feeder service area and substation area served by same Olt 49
Figure 10. Feeder level network layout-Sections of Feeder service area and substation area served by separate Olt 50
Figure 11. Feeder level network layout-Feeder service areas and substation area served by separate Olt 50
Figure 12. Shared GPON package network description file. 64
Figure 13. Network portion topological view showing display of IEDs on the fiber network 71
Figure 14. Dedicated fiber package network description file. 72
Figure 15. Network portion topological view showing display of IEDs on the fiber network 77
Figure 16. A graph illustrating the network utilization percentage across various OLT MAC interfaces over a 120-second simulation 141
Figure 17. A graph illustrates the network utilization percentage across various IED MAC interfaces over a 120-second simulation 142
Figure 18. A graph showing link utilization of residential path last mile fiber link 144
Figure 19. A graph showing last mile link utilization for a residential user path. 147
Figure 20. The graph for GridFeeder.ied20.eth[0].mac 148
Figure 21. The graph for the GridFeeder.olt.eth[3].mac interface depicting the utilization of an Optical Line Terminal (OLT) 149
Figure 22. A plot of Oscillator drift rate against simulation time. 151
Figure 23. The vector graph illustrating the Oscillator Drift Rate (ppm) for the internal clock modules of the IEDs and SCADA units across the simulation timeframe 151

Figure 24. This graph the behavior of an internal clock plotting the absolute Clock time of the GridFeeder.ied20. clock module against the global Simulation Time..... 152
Figure 25. The graph illustrates the Clock Time for the SCADA unit's underlying Clock. 153
Figure 26. Vector graph visualizing the End-to-End Delay (microsec) for the application layer of the 20 Intelligent Electronic Devices..... 156
Figure 27. The scatter plot isolating the End-to-End Delay for IED 1 (GridFeeder.ied1.app[0]). 157
Figure 28. The scatter plot isolates the End-to-End Delay for IED 20 (GridFeeder.ied1.app[0]). 158

List of Tables

Table 1. Structural breakdown of kapala's power rid architecture 40
Table 2. A comprehensive breakdown of the empirical data collected, encompassing 64 distinct power distribution units on the Wandegeya feeder. 41
Table 3. physical and logical data collected during the network audit and field survey phase. ... 42
Table 4. physical layer feasibility test parameters. 51
Table 5. parameters integrated into the simulation environment. 57
Table 6. channel parameters are enforced in the simulation 60
Table 7. Shared Passive Optical Network assigned logical addresses and routing protocols 82
Table 8. The gPTP Hierarchy. Grandmaster to Slave 109
Table 9. The Seven-Phase Stress Test Controller 135
Table 10. the channel utilization metrics derived from the SmartGridFeeder simulation. 137
Table 11. granular view of the channel utilization across the field-level interfaces of the SmartGridFeeder network. 138
Table 12. The ingress throughput captured at the Optical Line Terminal (OLT) field-facing interfaces during the simulation. 138
Table 13. Quantitative summary of data throughput across the primary network interfaces. 139
Table 14. Summary of the link utilization statistics for each Ethernet interface on the Optical Line Terminal (OLT). 140
Table 15. the MAC-layer utilization for the five Municipal Sinks distributed across the network. 143
Table 16. Summary of the MAC-layer utilization for the mission-critical nodes of the network. 145
Table 17. Summary of the performance statistics for each of the 20 Residential User modules. 146
Table 18. simulated oscillator drift rates for the grandmaster clock and various Intelligent Electronic Devices (IEDs) within the SmartGridFeeder network. 150
Table 19. Summary of the time change events recorded by the underlying clock modules during the SmartGridFeeder simulation 150
Table 20. End-to-end delay performance for the Intelligent Electronic Devices (IEDs) across the simulated power grid architecture 154
Table 21. End-to-End (ETE) Latency shared GPON 155

Acronyms and Symbols

Metric Prefixes

giga	G	10^{9}
kilo	k	10^{3}
mega	M	10^{6}
micro	μ	10^{-6}
milli	m	10^{-3}
nano	n	10^{-9}
pico	p	10^{-12}

List of equations

Equation 1. The Blocking Probability Formula 102
Equation 2. the slave clock time in relation to the master time 102
Equation 3. The sensitivity Formula. 103

Abstract

Modernizing of the power utility networks calls for heavy reliance on robust, deterministic communication architectures to support critical Protection, Automation, and Control (PAC) functionalities alongside real-time asset management. In Uganda, particularly within the Kampala Metropolitan area, extending these capabilities to Medium-Voltage (MV) and Low-Voltage (LV) grids presents significant opportunities for enhancing overall grid reliability. Because deploying dedicated, single-use fiber infrastructure across urban distribution networks is often cost-prohibitive, exploring the integration of IEC 61850 services over shared infrastructure is highly justified. Utilizing existing Gigabit Passive Optical Network (GPON) infrastructure running through residential and municipal neighborhoods offers a highly scalable and economically viable approach to delivering critical grid telemetry, provided the strict performance thresholds of utility operations can be guaranteed.

To evaluate the viability of this approach, a comparative technical methodology was executed utilizing the OMNeT++ simulation framework. The study modeled the Wandegeya Feeder's physical and logical topologies to assess data flow, interoperability, and network performance under varying traffic conditions. Two distinct network scenarios were simulated to provide a rigorous baseline: a shared GPON architecture acting as the primary test case, and a dedicated architecture featuring a completely separate fiber network acting as the control benchmark. The simulations were specifically designed to stress-test the network, measuring end-to-end latency, bandwidth consumption, and precision timing to determine if the shared medium could safely support the stringent requirements of PAC and asset management applications.

The simulation results conclusively indicate the viability of running IEC 61850 services over a shared neighborhood fiber network. Bandwidth utilization on the test network never exceeded 96%, validating that ample headroom is always present to reliably support continuous asset management services without bottlenecking the network links. Furthermore, clock synchronization accuracy was not degraded by varying traffic loads; the data demonstrates that synchronization can be effectively managed and corrected in software using gPTP to ensure accuracy remains within the strict limits required for automation telemetry. Crucially, GOOSE (Generic Object-Oriented Substation Event) messaging latency stayed well within the 3-millisecond accepted safety range, peaking slightly above 960 microseconds even under extreme network stress. Because these values remained highly consistent with the performance of the dedicated benchmark architecture, the study validates that a shared GPON can successfully and securely deliver critical grid protection telemetry.

Aknowledgements

This project is the culmination of the dedication and efforts of many individuals whose contributions have been invaluable. I express my deepest gratitude to all those who generously shared their time, knowledge, and commitment to make this work possible.

Special thanks go to the project coordination team, whose thoughtful selection of supervisors ensured that guidance was received from consummate professionals. Their support, encouragement, and insightful feedback were instrumental throughout the project.

I would like to express my deepest gratitude to my project supervisors, **DR. MURTALA AMINU BABA** and **DR. DATIVA TIZIKARA**. Their guidance, technical expertise, and unwavering support were instrumental in shaping the direction of this research. Furthermore, I am immensely thankful to UEDCL and TELMEC SOLITON for providing the foundational data that made this study possible. The collective mentorship and resources I received were essential to the successful completion of this project.

CHAPTER ONE

INTRODUCTION

1.1 Project Background

The demand of energy is drastically increasing in urban and suburban communities and this has pushed immeasurable pressure on the MV and LV distribution networks [18]. Traditional grid infrastructures are characterized with struggle to maintain reliability, operating efficiency, and effective asset management.

The changing utility environment requires the development and implementation of new solutions that will allow the optimization of the protection and control of the electric power system under normal or abnormal system conditions [3]. The surfacing of IEC 61850, an international standard for communication-based substation automation, control and protection, offers a promising pathway to rationalize the medium and low voltage grid sections. This will be through supporting digitization, automation, and data focused asset management [1,14].

This research is directed to assess the application of IEC 61850 for communication based accelerated protection, automation, control (PAC) and asset management in MV and LV grid networks with focus on Uganda. By integrating field devices, communication protocols, control systems, and asset management platforms, IEC 61850 is capable of significantly improving grid reliability, fault response times, and operating efficiency while enabling strategic asset management [6, 8].

In the last few years, energy demand rise has been one of the key concerns drawing a lot of attention, both inside and outside the electric power industry.
The industry is going through a major shift in the use of advanced twenty-first century technology in an effort to successfully meet today's challenges and those of the future in line with providing a more reliable, secure, and efficient power grid [18].

The electric power system that needs control and protection is changing and becoming more complex. The integration of communication-based accelerated protection, automation, and control schemes will be a vital enabler for improving grid performance [7]. These systems depend on high speed, standardized, and interoperable communication networks to support on time decision-making, fault isolation, and restoration all vital for achieving the modern "smart grid." [3]

The modern power system needs on time situational awareness, faster fault response, and foresight asset management to maintain stability and service continuity. This can be achieved mainly through communication-based accelerated protection, automation, and control (PAC) schemes. [2] This enables for instantaneous fault detection, isolation, and service restoration. These schemes are dependent on standardized and interoperable communication protocols that ensure smooth data exchange between intelligent electronic devices (IEDs), sensors, and control centers.

The IEC 61850 standard provides a broad framework to support these capabilities. It defines an assembled communication architecture, object-oriented data modelling, interoperability among intelligent electronic devices (IEDs), and high-speed peer-to-peer messaging encompassing Generic Object-Oriented Substation Event (GOOSE), Manufacturing Message Specification (MMS), and sampled values (SV) that enable both automated protection systems and condition-based asset management. [5, 8]

With all the benefits demonstrated by the IEC 61850 in transmission substations and some high voltage installations, its extension into medium voltage and low voltage grid levels where majority of reliability issues occur remains unexplored. [16, 17]

IEC 61850 enables machine-to-machine communication, data modelling and Its real time data exchange mechanisms that include GOOSE, MMS and Sampled Values, make it a foundation for accelerated protection, automation, and information-based asset management in medium voltage and low voltage levels. [10]

For Uganda, adopting IEC 61850 has the capacity to support grid modernization and also strengthen asset management systems, enabling utility operators to monitor equipment health, foresee failures, and optimize maintenance cycles. However, practical challenges including costs and limited communication infrastructure require context-specific research to guide effective implementation. This study is to assess how IEC 61850 can be leveraged to support communication-based protection, automation, and control (PAC) therefore enhancing asset management, efficient operation, and system reliability in Uganda's distribution networks. [6, 15]

1.2 Problem Statement

The electrical power system is becoming more complex and energy demand is on the rise due to rapid urbanization, population increase and the growing industrial activity [18]. This has raised the need for a reliable, secure and efficient grid infrastructure. Traditional MV and LV distribution networks are characterized by manual operations, limited to no communication capability, and aging assets, resulting in frequent outages, delayed fault restoration, and thus increasing operational costs [2].

The control of the power system during abnormal conditions has been typically based on decisions by the system operator or a limited number of underfrequency and undervoltage protection schemes, as well as special protection or remedial action schemes. Some of the characteristics of these solutions are that, in many cases, they operate when it is already too late to execute any optimal control and that they work after the uncontrolled separation of the system and the formation of islands of different sizes and levels of load-generation balance. The changing utility environment requires the development and implementation of new solutions that will allow the optimization of the protection and control of the electric power system under normal or abnormal system conditions and enhanced asset management [2,3].

1.3 Objectives

1.3.1 Main Objective

To assess and validate the application of IEC 61850 in supporting communication-based accelerated protection, automation, and control (PAC) for amplified asset management and grid performance in medium-voltage and low-voltage networks in Uganda.

1.3.2 Specific Objectives

1. To analyze the existing communication infrastructure in case study area and assess the requirements for integration with the power system.
2. To design an IEC 61850 communication network topology for MV and LV grid sections in case study area and validate it's support for PAC and asset management.

Already existing communication facilities, technologies, and data exchange mechanisms used within the case study area's power distribution network were identified and an audit carried out to assess existing capabilities to support IEC 61850 service integration in configuring PAC functions and produce a gap analysis report that identifies existing communication hardware in the case study area and quantifies technical requirements of bandwidth, latency, security, scalability, and protocol compatibility to support overlay of a power system communication network on the existing infrastructure.

A well-designed network topology for seamless communication between various Intelligent Electronic Devices (IEDs), sensors and the control centers, that complies with IEC 61850 standard across medium-voltage (MV) and low-voltage (LV) grid sections was designed and simulated in OMNeT++. The model tested communication latency, fiber link reliability to determine the fiber link suitability for real time protection and automation. The communication network topology that meets class P1 latency requirements for protection and provides 99.999% asset management services to ensure reliable and efficient operation of the distribution network in the case study area was designed and validated.

1.4 Significance of The Project

The addresses the need for modernizing MV and LV networks through the adoption of IEC 61850-based communication systems. Implementing this international standard will enable utilities to transition from traditional, manually operated grids to automated networks capable of real-time monitoring, protection, and control.

By designing an IEC 61850 communication network topology and developing a strategic implementation framework, this study contributes to improving operational reliability, fault handling, and asset management in Uganda's distribution networks. The integration of communication-based PAC functions will enhance system stability and reduce downtime, while data-driven asset management will support foresight maintenance and extend equipment lifespan.

Furthermore, the project will provide practical insights for power utilities, policymakers, and engineers by establishing a foundation for the transformation of the power distribution sector. Ultimately, the outcomes of the research will help optimize power system performance, ensure

cost-effective operations, and support sustainable energy access in line with Uganda's growing electricity demand and modernization goals.

CHAPTER TWO

LITERATURE REVIEW

2.1 The Power System

Historically, system operators have relied on manual judgments, a limited number of underfrequency and undervoltage protection schemes, or specialized corrective measures to manage abnormal conditions. These approaches typically act after the system has already split into islands with varying levels of load-generation balance, which often prevents ideal control. To improve protection and control under both normal and abnormal conditions, new solutions must be designed and implemented in response to the changing utility environment.

The Utility Power Grid (Transmission System)

The transmission system forms the backbone of the utility grid and in the past years has been the focus of development for protection, monitoring, control, and energy management systems.

Transmission System Islands

These islands form when multiple bulk or transmission lines trip, isolating a section of the system. This is mainly an uncontrolled process, so load-generation balance is rarely achieved at the moment of islanding. Post-disturbance, underfrequency load-shedding schemes can help restore balance. If generation exceeds load at the time of separation, generator over frequency controls may rebalance the island, though this may result in the loss of generation that could be utilized elsewhere in the grid.

The Sub grid

A sub grid is a controlled transmission island. By continuously monitoring power flow, load, and generation across the system, the grid can be intentionally split into subgrids during emergencies, ensuring a relative balance between generation and load. Under normal operation, subgrids function together as part of the overall grid and are continuously monitored to assess balance. Each sub grid consists of one or more substations, which act as mini-grids, each containing distribution feeders. Sub grid balance is determined using multiple sources of system data.

The Substation (Mini-Grid)

Traditionally, a substation's distribution system is powered through one or more transformers without any additional active sources. The increasing integration of distributed generators has changed this model, making it possible to balance the combined output of local generation and storage with at least the critical loads in the distribution system. This requires the capability to dynamically shed non-critical loads.

Consequently, the substation's distribution system can be considered a mini-grid, capable of operating independently if power transformers are disconnected due to faults, abnormal conditions, or intentionally to reduce the impact of wide-area disturbances.

2.2 Existing Power Grid Controls

Over time, various control mechanisms have been developed to maintain stable power system operations while improving reliability and efficiency.

Power-System Protection [2]

Power grids employ a range of protection technologies from simple wire fuses to advanced microprocessor-based relays to safeguard equipment by detecting and isolating short-circuit faults. A short-circuit is identified when voltage or current suddenly changes at the faulted location, prompting circuit breakers to isolate the affected equipment. Protection systems operate very quickly, often within tens of milliseconds, making them a form of fast control. Modern protection systems typically include:

- **Current and voltage transformers** for measurements,
- **Protective relays** for decision-making,
- **Circuit breakers** to interrupt or restore circuits,
- **Batteries** to provide power during disconnection, and
- **Communication channels** for remote monitoring and control.

Frequency Control [3]

System frequency is influenced by the balance between generation and load.
Primary frequency control acts locally at the generator using the governor, which adjusts mechanical input based on shaft speed deviations.
Secondary frequency control, also called automatic generation control (AGC) or load frequency control (LFC), is managed by a central controller that adjusts governor set points to maintain system-wide balance and efficiency.
In deregulated markets, electricity trading indirectly serves as system-wide frequency control by balancing supply and demand while ensuring economic dispatch and system stability.

Voltage Control [4]

Voltage regulation in AC transmission networks is closely tied to reactive power management. Voltage control can be achieved through:

- Generator excitation adjustment,
- Transformer tap changes (OLTC),
- Manually or automatically switched shunt capacitors or reactors, and
- Power electronic devices like static var compensators (SVC) for fast reactive power response.

Since reactive power cannot travel long distances efficiently, voltage control is mostly local. Some regions, such as parts of Europe, have implemented coordinated voltage control over larger areas, and research is ongoing to extend similar strategies in North America.

Transmission Power-Flow Control [3]

Compared to frequency and voltage control, controlling power flow in transmission lines is more limited. Full control of every line is neither feasible nor desirable, but managing main lines helps avoid overloads and ensures scheduled market transactions. Traditional methods include phase-shifting transformers**,** which adjust flow by manipulating phase angles, and HVDC lines**,** which allow fast, controlled transfers over long distances and between unsynchronized systems.

Modern Flexible AC Transmission Systems (FACTS) use power electronics to regulate AC transmission parameters and optimize power flows [5, 6]. Distributed FACTS devices are smaller and more cost-effective, making them suitable for broader deployment [7-10].

Most fast controls are localized within substations, yet power system dynamics often have regional or system-wide effects. This makes achieving global stability using local controllers challenging. Advanced measurement technologies in modern grids help to address this limitation [3].

For effective fast global control design, several factors listed below must be considered:

1. Accurate system modeling,
2. Coherent, real-time measurement data,
3. Sufficient communication infrastructure, and
4. Effective networked control strategies.

Grid Control

Advances in communication and information technologies, particularly cloud computing, enable the integration of emerging energy technologies with existing or evolving management functions. This integration aims to enhance the efficiency, reliability, and quality of the electric power system.

2.3 The need for enhanced grid control

Reliability

Reliability is a core feature of the modern grid, generally defined as the likelihood that a system performs correctly over a given period. In the context of electricity, it reflects the ability of system components to deliver power to consumers within accepted standards and quantities. Reliability can be assessed through the frequency, duration, and magnitude of local, regional, or system-wide disturbances or outages.

Electric Power System Security

System security is closely linked to reliability and refers to the ability of the power system to continue functioning under contingencies without interrupting customer service. Security depends on system design, operational conditions, and the likelihood of disturbances.

Up until now, system security was ensured by building sufficient generation and spinning reserves and continually evaluating transmission performance. Modern systems benefit from synchrophasor measurements in multifunctional IEDs, enabling dynamic state estimation and more precise determination of security margins.

Efficiency

Efficiency is one of the main goals of the modern grid and should be distinguished from effectiveness:
Effectiveness: Achieving objectives regardless of resources used.
Efficiency: Achieving objectives using the least resources possible.
Efficiency assessment considers multiple factors, including:

2.4 General Function Categories in PAC Systems

Improving the reliability and security of the electric power system largely depends on minimizing the duration of short-circuit faults on transmission lines, distribution feeders, and substation equipment. This is critical for maintaining system stability and ensuring the quality of power, especially given the growing number of customers with voltage-sensitive loads. Additionally, better knowledge of equipment conditions and load behavior enables optimization of Protection, Automation, and Control (PAC) systems under faults or other abnormal conditions.

Modern grid functions are diverse, with different performance and communication requirements. For analytical purposes, these functions can be grouped into two main categories:

1. Fault-Clearing Functions. Fault-clearing functions primarily revolve around protection. Successful fault clearing depends not only on protection equipment but also on other devices in the system. These functions encompass all process-level interfaces needed to detect abnormal conditions and the switching devices that isolate faults based on signals from protection devices.
2. Control and Monitoring Functions. Control functions encompass all operations required for system management, including manual and automatic optimization of operation, voltage and frequency regulation, interlocking, and restoration after disturbances. Monitoring functions handle the acquisition, storage, transmission, and visualization of data to support system operation, analyze performance, and track behavior during normal and fault conditions. Alarm and supervision functions are additional examples of control and monitoring activities, which can be applied across various domains of the electric power system.

Types of Functions in PAC Systems

PAC system functions can be classified in multiple ways, particularly in IEC 61850-based systems:

1. Based on Process Interaction:

Primary functions: Directly interact with the process (e.g., protection, control, automation, monitoring).

Support functions: Operate in the background or during specific phases, such as configuration and time synchronization.

2. Based on Distribution Level:

Single-bay functions: Operate on devices within one bay using local process data (e.g., overcurrent or distance protection).

Multi-bay functions: Require information from multiple devices within the same substation (e.g., busbar protection, breaker failure protection).

Multi-station functions**:** Involve devices across different stations, requiring remote process or device status information (e.g., tele protection, WAMS, SIPS, distribution automation).

Protection Functions

Protection functions act directly on station breakers to isolate faults. They monitor system parameters such as voltage, current, frequency, and temperature and issue trip signals when conditions could cause equipment damage or safety hazards. Settings, adjustable by protection engineers, govern the behavior of protection functions.

Control Functions

Control functions involve operator actions for switchgear and process control, usually through an HMI at bay, cluster, or control center level. These functions allow users to operate HV/MV equipment and auxiliary devices and visualize events, alarms, and operational states.

Automation Functions

Automation functions execute predefined sequences automatically when triggered by operator commands or process conditions. They operate alongside interlocking and protection functions and include switching sequences needed to bring a switchyard into operational states. Safety checks are integrated to ensure reliable operation.

Monitoring and Recording Functions

Monitoring functions collect data to detect abnormal conditions, optimize maintenance, and validate system models. Examples include:

- GIS monitoring
- Transformer or circuit breaker monitoring
- Power quality monitoring
- Voltage and current monitoring

Recording functions capture system parameters for forensic analysis, event investigation, or testing. Examples include:

- Transient (waveform) recording
- Fundamental and harmonic signal recording
- Sequence-of-events recording

Supervision Functions

Supervision functions enable operators to visualize real-time data from primary and auxiliary equipment, including:

- Equipment state (open/closed)
- Operating conditions (normal/faulty)
- Alarms
- Electrical measurements (RMS, complex values)
- Data archiving

Auxiliary Functions

Auxiliary functions support PAC and monitoring systems during setup, commissioning, extension, or modifications. They include:

- Device self-monitoring and diagnostics
- Time synchronization
- Data aggregation (summarizing collected information)

Function Elements and Distributed Functions

Modern IEDs often combine multiple functions previously handled by separate devices, reducing installation and maintenance costs. Functionality can be hierarchical, with function elements as the smallest units capable of exchanging data.

Distributed functions involve communication between function elements on different physical devices and can be local or remote. Data exchange occurs between function elements and across functional hierarchy levels, facilitated by communication interfaces such as:

- Analog-to-digital converters (A/D)
- Measurement function elements (e.g., synchrophasors)
- Protection function elements

Function allocation across physical devices determines interface requirements and may involve multiple LANs. Functions can be distributed across:

- Station level
- Voltage level

- Bay/unit level
- Process level

2.5 Communication Interfaces

Typical logical communication interfaces in modern grid systems can be classified as follows:

- **Current and voltage data exchange:** Streaming samples between the process level and bay level, implemented using **peer-to-peer (P2P) connectionless communications.**
- **Switchgear status exchange:** Data transfer between the process level and bay level via **P2P connectionless communications.**
- **Nonelectrical data exchange:** Particularly sample data exchanged between process and bay levels using **P2P communications**.
- **Protection data within bay level:** Exchanged through **P2P communications.**
- **Protection data between bay and station levels:** Transferred using **client-server (C/S) communications.**
- **Inter-substation protection data exchange:** Conducted via **P2P communications.**
- **Control data between process and bay levels:** Exchanged using **C/S communications**.
- **Control data between bay and station levels:** Implemented through **C/S communications.**
- **Control data between substations and control centers:** Managed using **C/S communications.**
- **Data exchange between substations and remote engineering stations:** Can use **C/S communications or file transfer** methods.
- **Direct bay-to-bay data exchange:** Used for fast operations such as interlocking via **P2P communications.**
- **Station-level data exchange:** Carried out using **P2P communications.**

Given the diverse applications of the modern grid, additional interfaces are often necessary, including:

- **Inter-substation control data exchange:** Binary data for interlocking functions via **P2P communications.**
- **PMU to PDC data exchange:** Performed using **P2P communications.**
- **PDC to super PDC (SPDC) exchange:** Facilitated via **P2P communications.**
- **SPDC to state estimator exchange:** Implemented using **P2P communications.**
- **SPDC to system integrity protection scheme (SIPS) exchange:** Conducted via **P2P communications.**
- **SIPS to substation communication:** Managed using **P2P communications.**
- **Substation to remote distribution system device exchange.**

2.6 Communication Nodes

A communication network is essentially a group of interconnected entities, referred to as **nodes**. These physical nodes are electronic devices linked to the network, and depending on their

capabilities, they may generate, send, receive, or forward information across communication channels.

Transmission Modes

The transmission, or communication, mode defines how data flows between devices that are directly connected or communicating over a network. Three primary transmission modes exist:

- **Simplex**
- **Half-duplex**
- **Full-duplex**

Simplex Mode

In power systems, simplex mode applies to components such as sensors and breaker trip coils. A sensor sends information only to an IED, while a trip coil only receives signals from a controller.

Half-Duplex Mode

In grid environments, half-duplex is used for non–time-critical functions that require two-way information exchange but allow devices to take turns. This mode is generally more economical due to fewer resource requirements but may not meet stringent performance needs. In the past, half-duplex was used in legacy networks with bus topologies, particularly those relying on coaxial cables.

Full-Duplex Mode

In power systems, full-duplex operation is essential in protection schemes where multiple protection devices must continuously and simultaneously exchange data for reliable and fast decision-making.

Communication Media

In data communications, the transmission medium refers to the physical channel that carries data from a sender to a receiver. It is the pathway that enables information to move from one node to another. Transmission media fall into two broad categories: wired and wireless**.**

Wired Media

Wired, or guided, media use physical pathways to direct signals from one point to another. These media offer advantages such as high transmission speed and strong security but are generally limited to shorter distances.

Optical Fiber Cable

Optical fiber transmits data as pulses of light through a central glass or plastic core, which is enclosed by cladding of a lower density. It supports both unidirectional and bidirectional transmission and enables wavelength-division multiplexing (WDM).

Optical fibers are available in two forms:

- **Single-mode fiber:** carries only one path of light, supports long-distance communication, and offers high bandwidth.
- **Multimode fiber:** carries multiple light modes, designed for shorter distances, and typically lower cost.

Optical fiber provides high bandwidth, immunity to electromagnetic interference, and low weight. However, it is more expensive and requires specialized installation and maintenance.

Wireless Media

Wireless, or unguided, media transmit electromagnetic waves through the air without requiring a physical conductor. They offer convenience and have seen major improvements in speed and quality, but they remain more prone to interference and cybersecurity risks.

Network Area Classifications

Communication networks are often categorized by their physical scope or geographic coverage. The main types include:

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)

Personal Area Network (PAN)

A PAN typically covers a small area ranging from several dozen square meters to a few hundred square meters. These networks may use either wired or wireless communication technologies. PANs are usually connected to an internet service provider through a modem and a wired or wireless router that links all personal devices.

Local Area Network (LAN)

LANs are commonly deployed in office settings to allow computers to exchange information or share resources such as printers. They also make use of both wired and wireless media and currently operate at speeds ranging from 100 Mbps to 10 Gbps.

Metropolitan Area Network (MAN)

MANs use high-capacity wired or wireless communication channels and serve to interconnect multiple LANs. A MAN may be owned by a municipality as a public utility or by a private organization. These networks typically span tens of square kilometers.

Wide Area Network (WAN)

WANs connect multiple MANs and LANs and use a combination of wired and wireless technologies. They often employ mesh topologies and support wide-area monitoring, protection, and control functions, including system integrity protection schemes.

2.7 Functional Relationships
Communication Relationships

When analyzing how nodes interact within a communication network, it is important to consider the type of relationship established between them. These relationships are often named after familiar patterns of human interaction, which makes the concepts easier to understand. Although some relationships appear similar, they differ in how communication is initiated and how requests and responses are handled. In electric power system applications, three major types of communication relationships are commonly used

Master/Slave

The master/slave model describes an asymmetric relationship in which a single “master” node supervises one or more “slave” nodes and acts as the central point of communication. Although this terminology has been used for decades, it has become controversial due to its association with slavery, leading some organizations to replace it with terms such as “controller/agent.”

In electric power systems, this communication pattern historically supported early SCADA systems, where a master station performed data polling or issued breaker control commands, and field devices acted as slaves.

Client/Server

The client/server model resembles the master/slave relationship in that one node sends a request and another provides a response. The main difference lies in directionality: in client/server communications, a single server can respond to requests from multiple clients, whereas in master/slave communication a single master addresses multiple slave.

In electric power systems, client/server communication supports tasks such as data polling and breaker operations, where measurement or control devices function as servers. Unsolicited messages can improve efficiency by immediately reporting breaker status changes or significant measurement deviations without waiting for client requests.

Peer-to-Peer (P2P)

In power system applications, P2P communication is commonly used for protection schemes that demand very fast response times. Multifunctional IEDs often rely on P2P messaging to coordinate protective actions within high-speed protection systems.

Network Topology

Designing communication networks for a digital grid requires considering numerous factors. The choice of network architecture depends not only on application requirements but also on the communication technologies employed and the specific topology selected. Although wired communication remains the preferred option for electric power systems due to its superior reliability, security, and signal integrity, simply choosing a wired medium is not sufficient. An important research opportunity lies in developing decision-support frameworks that help utilities match topologies to evolving grid requirements, including DER integration, resilience needs, and cybersecurity constraints [41].

Below are common topologies used in digital grid communication networks.

Bus Topology

Bus topology, one of the earliest network designs, arranges nodes along a single cable in a linear sequence. All devices share the same communication medium, making the system inherently half-duplex. When one device transmits, the signal propagates to all devices on the backbone cable.

Ring Topology

In a ring topology, devices are connected in a closed loop. Data travels from node to node until reaching its destination. Rings may be unidirectional or bidirectional (dual-ring configurations).

Given the increasing adoption of self-healing substations, research is needed on adaptive or automatically reconfigurable ring topologies that can tolerate failures without interrupting critical grid functions.

Star Topology

A star topology connects all end devices to a central hub. This structure improves reliability: if an individual node or its link fails, the remainder of the network continues operating. Troubleshooting becomes easier because each device has a dedicated link to the hub, and performance improves because data does not pass through multiple intermediate nodes.

Research opportunities include designing fault-tolerant and cyber-secure central nodes, as well as exploring distributed or virtualized hub architectures that eliminate single points of failure.

Mesh Topology

In mesh topologies, nodes connect to one another through multiple point-to-point links. A full mesh connects every node to every other node, while a partial mesh offers selective connectivity.

Emerging research directions include cost-optimized mesh designs, software-defined mesh networks, and mesh architectures that dynamically reconfigure based on load, faults, or cyber threats.

Tree Topology

Also known as a hierarchical topology, the tree structure uses root nodes connected to sub-root nodes that branch into lower-level devices. It blends characteristics of star and bus topologies, offering good scalability and relatively low cost compared to a full mesh. Troubleshooting is simpler because the structure avoids loops.

Research opportunities involve developing resilient hierarchical structures with redundant roots or virtualized hierarchy layers capable of isolating faults without impacting dependent nodes.

Hybrid Topologies

Hybrid topologies combine features of two or more basic designs. They can offer greater flexibility and resilience but require careful expertise to configure, maintain, and optimize.

As modern smart grids become increasingly heterogeneous, research is needed on systematic methods for designing, validating, and managing hybrid topologies especially those blending wired, wireless, edge computing, and cloud components.

Communication Protocols

Any form of digital communication relies on an established set of rules known as a protocol. These rules determine; What information is exchanged within the network, how that information is transmitted, and when the communication occurs.
Protocols ensure that devices interpret transmitted data in a consistent and reliable manner. However, as modern grids incorporate diverse devices from legacy equipment to IoT sensors there is a growing need for adaptive, interoperable protocols capable of supporting mixed communication environments.

Elements of a Communication Protocol

A protocol typically consists of five core components:

1. Message encoding
2. Message formatting and encapsulation
3. Message timing
4. Message size management
5. Message delivery mechanisms

Each of these defines how data is prepared, transmitted, and interpreted by communicating devices.
Current standards handle these elements well in traditional networks, but new challenges arise in cyber-physical systems, calling for research into scalable and resilient protocol designs.

Message Encoding

Message encoding depends on the transmission medium.

- In wired systems, such as computers or protection IEDs, data is converted into electrical signals and communicated through cables.
- In wireless systems, such as smartphones or tablets, the device converts data into electromagnetic waves to match the wireless medium.

In both cases, the device must encode data in a way that matches the physical characteristics of the communication channel. As grids increasingly adopt wireless technologies, new research opportunities involve developing encoding techniques that remain robust in noisy environments, support low latency, and maintain cybersecurity under spectrum congestion and interference.

Message Formatting and Encapsulation

For successful communication, both the sender and receiver must use a mutually understood message format. Additional information such as source and destination addresses are encapsulated with the data to enable proper routing and interpretation.

Research opportunities exist in creating standardized yet flexible formats that can support emerging grid applications such as distributed energy resources, and high-frequency sensor streams, while ensuring backward compatibility with legacy systems.

Message Timing

Protocols also regulate the timing of message exchanges. When a sender transmits data faster than the receiver can process, data loss can occur. Flow control mechanisms help prevent congestion and ensure reliable communication.

As the grid becomes more dynamic, there is a growing research need for adaptive flow-control algorithms that adjust in real time to network congestion, cyber incidents, or fluctuating load conditions especially in time-critical protection functions.

Message Size

Protocols define how large a message can be. When a file exceeds the capacity of the communication link, the sender splits it into smaller numbered segments. The receiver reassembles the segments and uses sequence numbers to detect missing parts.

Emerging research directions include optimizing segmentation methods for constrained networks (e.g., low-bandwidth field networks) and developing efficient reassembly techniques that reduce delays and improve reliability for large-scale grid data exchanges.

Message Delivery Options

Protocols specify how messages should be delivered to recipients:

- Unicast: one sender to one receiver
- Multicast: one sender to selected receivers
- Broadcast: one sender to all devices in the network

Different applications require different delivery modes. Modern grid systems especially those operating in multi-layer, distributed architectures need more intelligent delivery mechanisms that can dynamically switch between unicast, multicast, and broadcast to optimize bandwidth, reliability, and security. Developing such adaptive delivery strategies is a noteworthy research opportunity.

Messages in Modern Grid Systems

A foundational step in understanding communication needs in modern, digitized power systems is identifying the types of messages exchanged among devices and the associated performance and security requirements. Different distributed functions place different demands on communication systems, and these must be carefully considered when designing protection, automation, control (PAC), monitoring, and recording infrastructures. A research need lies in the development of unified methodologies for evaluating message requirements across heterogeneous grid applications, as current approaches remain fragmented.

Modern grid applications rely on message exchanges across diverse communication links, making the transfer time a critical performance parameter. Transfer time refers to the duration from when the first bit of a message leaves the sender until the last bit arrives at the receiver. Because many system elements are geographically dispersed, transfer times often depend on wide-area network conditions, which are inherently variable and difficult to predict. Factors influencing transfer time include device design, link type, message length, communication speed, network traffic, architecture, and services used. Despite its importance, transfer-time prediction models that incorporate dynamic network behavior and real-time cyber-physical interactions remain underdeveloped suggesting a clear research opportunity.

To enable proper implementation of modern grid functions, message types must be categorized into performance classes. These fall into two broad groups:

1. Protection and control applications, which require very stringent performance, and
2. Metering, monitoring, and power quality applications, which allow more flexible timing.

Even within protection and control, requirements vary depending on whether the application supports distribution-level systems, non-critical transmission areas, or critical transmission zones.

Fast Messages

The most time-sensitive messages are those needed for fault clearing, such as breaker-trip signals or breaker-failure protection commands. These must operate at speeds comparable to conventional electromechanical relay contacts (around 3–4 ms). They are also essential for interlocking, inter tripping, and programmable logic–based distributed protection. Ideally, total transfer time for such messages should be within 8–10 ms (approximately half a power cycle).

Fast communication is also necessary for bay-to-bay interactions and process-to-bay exchanges, typically requiring message delivery within one to several cycles. A research gap exists in ensuring that these ultra-fast requirements can be met over shared or congested communication networks, especially when relying on commercial, non-deterministic communication technologies.

Medium-Speed Messages

Medium-speed messages convey information where timing still matters but is less critical for example, changes of state or non-protection-related measurements. These messages are common within bay-level exchanges or between bay and station levels. Acceptable transfer times are generally below 100 ms. Future research could focus on optimizing medium-speed communication under variable load conditions, especially as the volume of sensor data grows with grid digitalization.

Low-Speed Messages

Low-speed messages carry time-tagged complex data used in automation, configuration changes, or transmission of event and fault records. Transfer times up to 500 ms are considered acceptable. These messages span numerous interfaces across modern smart grid applications. However, as system complexity grows, there is a need for strategies that balance low-speed traffic with high-priority, time-critical flows an area where current network management techniques remain insufficient.

Raw Data Messages

Raw data messages originate from analog interface devices such as digital instrument transformers. These streams carry time-synchronized measurements essential for protection, often requiring rapid transfer (3–4 ms). Slow-changing nonelectrical parameters such as temperature may be sent with much less stringent timing (up to 500 ms). A promising research avenue is the development of adaptive messaging schemes that dynamically adjust data rates and priorities based on grid conditions, sensor behavior, or cyber constraints.

File Transfer

Modern grid functions often require transferring files such as transient and disturbance recordings, harmonic data, settings, and system configuration files. Although file transfers are not time-sensitive, they may burden networks that also carry time-critical messages, requiring strategies

that mitigate congestion. These files may contain sensitive information, making access control such as role-based access control (RBAC) important.

Research opportunities include designing intelligent file-transfer scheduling algorithms, studying the effects of bulk data transfer on mission-critical traffic, and integrating cybersecurity measures that do not compromise grid performance.

Time Synchronization Messages

Time synchronization ensures uniform timing across devices that rely on time-stamped data. Event-based applications generally require accuracy around 1 ms, while sampled values and synchrophasors require similar precision. Different communications methods may be used to meet these accuracy requirements. A research gap remains in achieving resilient, attack-tolerant, and low-latency time synchronization over heterogeneous and often insecure communication networks.

Command Messages

Operators and maintenance personnel frequently use command messages to issue control actions locally or remotely. Depending on the application, these messages may require authentication, encryption, and RBAC to ensure secure operation.

With the continued evolution of the modern grid, new message types will undoubtedly emerge. Research is needed to anticipate these future requirements and develop scalable frameworks for incorporating new message classes without compromising reliability, interoperability, or cybersecurity.

2.8 Communication network core

An outstanding challenge in communication-based PAC and asset management is achieving interoperability among diverse system components, made more difficult by the absence of open standards [12]. Significant heterogeneity can also be found within a single network, such as differences in programming languages, communication protocols, hardware devices, and databases [13]. This diversity complicates system interaction, creating the need for an adaptable, dependable, reusable, and trustworthy communication architecture for PAC and asset management applications [15].

A potential approach is to adopt a service-oriented architecture (SOA) built on web services [12, 13]. SOA is a software architecture that organizes systems into modular units known as services, which interact through defined interfaces and contracts that are typically independent of communication protocols, hardware, or programming languages. This design enables consistent interaction among various systems or services. To ensure interoperability, however, appropriate services and interfaces must be specified using web-service description language (WSDL). In addition to facilitating service interaction, SOA offers strong flexibility and scalability to support future system growth [14].

Internet-based virtual private network (Internet VPN)

Traditional IP networks are flexible but only provide best-effort delivery, meaning they cannot guarantee the quality of service (QoS) required for modern grid operations. Grid applications depend on strict QoS constraints such as latency, jitter, throughput, and packet-loss limits. Internet VPNs offer a stronger alternative, delivering both security and QoS capabilities needed for grid communications [16].

Internet VPNs form a shared but cost-effective, high-speed communication backbone that replicates many advantages of dedicated private networks. They can deliver secure, robust connectivity with strict QoS guarantees while still operating over shared infrastructure. However, challenges remain in areas like routing efficiency, resource allocation, and cross-domain network management; these require further development for modern grid use.

Hybrid use of TCP and UDP

Another option is to rely on the transport-layer protocols within the IP suite: TCP and UDP. Although both protocols enable universal communication, they serve different purposes. TCP provides retransmission for lost packets but introduces delays and overheads [13], and it does not support multicast an important feature for simultaneously sending control messages to multiple grid devices during emergencies.

In contrast, UDP has low overhead and supports multicast but lacks reliability mechanisms. Using a hybrid of TCP and UDP can provide the grid with a simple, dependable, and orderly communication service [12]. Both protocols can run over either IPv4 or IPv6 networks.

Communication and networking middleware

Middleware offers an abstraction layer that enhances interoperability, flexibility, and portability in communication systems. It bridges high-level application QoS needs with low-level resource management tasks, such as bandwidth allocation and real-time data tracking. As a result, middleware can support protocol interoperability and strengthen TCP/IP performance for smart grid operations.

An example is GridStat [18], a publish–subscribe middleware being deployed by Avista Utilities in Washington. Integrated with the SCADA system, GridStat gathers data directly from sensors and distributes status variables and alerts throughout the electrical grid.

Last-mile connection

The term “last-mile connection” describes the link that extends connectivity from a communication provider to the end user. In the modern grid context, it involves connecting control centers and field devices to the core high-speed communication network. This requirement introduces additional challenges for building a cost-efficient and dependable communication system. Various technologies such as power-line communication (PLC), wireless systems, satellite links, and optical fiber can be employed to establish this last-mile connection.

Control center

In modern power-system automation and substation automation, numerous operational, control, and protection functions must be optimized to achieve maximum efficiency and ensure reliable electricity supply [13]. Power grids encounter a wide range of issues, from minor variations in voltage, frequency, or phase angle to major disturbances like cascading failures and widespread blackouts. A control center is essential for preventing such events, which requires collecting data from different parts of the grid.

Traditional SCADA systems already support continuous but non-synchronous data collection through a centralized server, yet they lack the necessary integration capabilities and scalability for advanced grid operations. To enable real-time monitoring, improved protection, and enhanced control, wide-area measurement systems (WAMS) are being deployed. Integrating WAMS with existing SCADA platforms enables smoother transition toward more advanced functionalities [19].

Distributed communication offers the advantage of enabling decentralized control and protection functions across a range of computing platforms within the grid. Given the growing importance of WAMS and its critical role in smart grids, reliability analysis has become a major research focus. WAMS failures can have serious consequences, so reliability studies help uncover hidden risks and guide emergency response planning. Work such as [31] examines interdependencies among key WAMS factors, while [32, 33] present detailed reliability evaluations of real-world systems. Common analytical tools include influence diagrams [31], fault-tree analysis, and Markov models [32, 33].

Sensor and Actuator Networks (SANETs)

Sensor and actuator networks (SANETs) have emerged as one of the components in modern grid communication architectures. SANETs are heterogeneous networks composed of numerous nodes that may function as sensors, actuators, or both, enabling continuous monitoring and control of modern grid assets [34]. Their primary role is to observe operational states and detect abnormal behavior so that outages, disturbances, or equipment failures can be mitigated in advance. Data collected by sensors is typically forwarded to a sink node, often located at a network gateway such as a data aggregation unit (DAU), which links network segments like neighborhood area networks (NANs). This information may be processed locally by actuators or transmitted through gateways to utility control centers for further analysis and response.

2.9 Security and Privacy in Communications Infrastructure for MV and LV Grid Sections

Ensuring the security and privacy of communication infrastructures in medium-voltage (MV) and low-voltage (LV) sections of the modern grid has become a critical research focus. As modern grids increasingly integrate diverse systems and subsystems, their expanded interconnectivity creates more potential entry points for intrusions, cyberattacks, and other malicious activities. Documented incidents including the 2003 cyberattack on the Port of Houston and the 2009 demonstration of a successful compromise of a commercial smart meter at the Black Hat Conference illustrate the vulnerability of power systems to cyber threats [25]. These events

underscore the risks introduced by the convergence of information and communication technologies within the grid.

While this integration increases exposure to security breaches, it also offers opportunities to strengthen system resilience. Advanced communication frameworks can enhance monitoring, control, and anomaly detection, thereby enabling the grid to better resist or mitigate cyberattacks.

Researchers commonly categorize modern grid cyber security into:

1. **Component-wise security**, addressing protection of devices such as smart meters, intelligent electronic devices (IEDs), and wide-area measurement systems (WAMS);
2. **Protocol security**, focusing on safeguarding communication standards including IEC 61850 and DNP3; and
3. **Network-wise security**, which ensures secure operation over communication media such as cellular networks, fibre-optic links, wireless LANs, and power-line communications.

Component-Wise Security

Component-wise security has become a critical area of focus in smart grid research due to the extensive deployment of intelligent electronic devices (IEDs), including smart meters, phasor measurement units (PMUs), wide-area measurement systems (WAMS), advanced metering infrastructure (AMI), remote terminal units (RTUs), and various control devices. Many of these components are installed in secondary or remote locations outside utility facilities and are connected through public or semi-public communication networks, such as the Internet. This distributed deployment introduces significant vulnerabilities, as remote access interfaces may allow unauthorized third parties to gain control of devices, thereby compromising grid operations.

To address these risks, the literature emphasizes the importance of robust authentication and trust management mechanisms. Existing industrial main management systems can be adapted for modern grids to reduce additional implementation costs, while cryptographic technologies such as public key infrastructure (PKI), advanced encryption standard (AES), and triple data encryption algorithm (3DES) are widely recommended for secure and private data exchange [26]. Device attestation has also been proposed as a critical security enhancement, allowing verification that a device has not been tampered with. Attestation certificates, installed by certified manufacturers, strengthen trust in the integrity of field devices. Ensuring device-to-device authentication through well-designed trust-anchor management systems further reduces security risks [26].

Higher-level communication infrastructures such as WAMS also face security challenges, particularly due to interoperability requirements among heterogeneous solutions. Several strategies have been proposed to address these vulnerabilities, including isolating operational functions (e.g., real-time measurement and monitoring) from administrative functions (e.g., disturbance logging) to reduce potential attack surfaces [35]. Domain-oriented security architectures [27] and dedicated security layers [36] have likewise been explored as non-intrusive ways to enhance protection without undermining system reliability.

Protocol Security

Protocol security is a central concern in modern grid research, as reliable grid management depends on secure, bi-directional communication between devices and control systems. Communication protocols form the backbone of information exchange across the grid, and their vulnerabilities expose the system to cyber threats ranging from falsified measurement data to manipulated control commands capable of causing grid overloads or operational instability. Consequently, ensuring the security of both legacy and emerging communication protocols is essential for maintaining grid reliability.

A variety of standardized automation protocols developed by the International Electrotechnical Commission Technical Committee 57 (IEC TC 57) are widely used in modern power systems. These include DNP3 for process automation [85], IEC 61850 for IED communication and data models, IEC 61850-7-420 for distributed energy resource (DER) communications, IEC 60870-5 for telecontrol and teleprotection, IEC 61970 for energy management systems, and IEC 60870-6 (ICCP) for wide-area control center data exchange [37]. While these protocols enable interoperability and functionality across the grid, their implementation over shared communication platforms introduces multiple security vulnerabilities, especially because many of them are open standards.

To address these concerns, several studies have proposed adding encryption and authentication mechanisms to existing protocol stacks. For example, security extensions such as Pretty Good Privacy (PGP) [37] and the open-access-compatibility (OAC) layer [38] have been explored as means to introduce cryptographic protection specifically, public key-based authentication and encryption to the DNP3 data-link layer. Although such pseudo-layers enhance security, researchers emphasize that comprehensive protection requires formal integration of these measures directly within the protocols themselves rather than as add-ons.

In recognition of this need, IEC TC 57 established Working Group 15 (WG15) under the IEC 62351 series to develop dedicated security standards for the TC 57 protocol family, including IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, and IEC 61968 [37]. WG15 defines a broad set of security objectives, encompassing digital signature–based authentication, access control, eavesdropping prevention, replay and spoofing protection, and basic intrusion detection capabilities. Additionally, advanced encryption standard (AES) technologies have increasingly been adopted within smart grid communication protocols, AES already forms part of the ZigBee specification and is considered a strong candidate for securing other protocol layers [39].

Network-Wise Security

Network-wise security has become a central topic in the evolution of modern grid communications, as the grid's communication backbone connects numerous components while simultaneously interfacing with external networks for power system coordination and electricity market operations. This extensive connectivity increases exposure to cyber threats, including network outages, sabotage, and unauthorized access, any of which may disrupt critical grid functions [23]. Although private communication networks offer strong security by limiting third-party access, they are often costly, inefficient, and hinder interoperability across utilities. As a

result, researchers advocate for hybrid approaches that combine open communication infrastructures with strong security mechanisms.

IP-based virtual private networks (VPNs), WiMAX, and conventional TCP/UDP-based systems have emerged as promising alternatives, offering both flexibility and enhanced security through standardized protection methods. Technologies such as IP Security (IPSec) provide packet-level authentication and encryption, mitigating vulnerabilities in IP-based smart grid networks. NIST also recommends using isolated or disjoint protocols for high-risk operational areas to reduce potential attack surfaces [24]. WiMAX further strengthens network security by supporting multiple cryptographic standards, including AES and EAP-TTLS, making it a feasible candidate for secure smart modern communications.

2.10 Principles of Modern Network Design: VLAN Architecture and Convergence

The design of a modern, scalable network relies heavily on the logical abstraction of physical infrastructure.

As organizations move away from disparate, single-purpose networks (such as separate physical links for IT data, voice, and operational telemetry), the reliance on logical segmentation and traffic engineering becomes vital. This is achieved through Virtual Local Area Network (VLAN) architectures and specialized encapsulation techniques.

2.101 Strategic VLAN Design (IEEE 802.1Q)

A VLAN logically segments a single physical Local Area Network (LAN) into multiple distinct broadcast domains at its core. Effective VLAN design is critical for three fundamental reasons:

Security and Isolation: By assigning different departments, services, or hardware types to distinct VLANs, sensitive traffic is isolated. A compromised device on a public VLAN cannot directly access internal management VLANs via Layer 2.

Broadcast Containment: Without VLANs, broadcast traffic (like ARP requests) floods the entire network, consuming bandwidth and CPU cycles on edge devices. VLANs restrict these broadcasts to their specific logical domains.

Traffic Management: VLANs allow network administrators to apply specific routing policies, access control lists (ACLs), and Quality of Service (QoS) profiles to different traffic classes.

2.102 Scaling with Q-in-Q: CVLANs and SVLANs (IEEE 802.1ad)

In large-scale enterprise environments or Service Provider networks, the standard 802.1Q VLAN limitation of 4,094 distinct tags is often insufficient. Furthermore, service providers need a way to transport customer traffic across a backbone without having customer VLAN IDs conflict with the provider's internal routing, or with other customers' VLANs.

This challenge is solved using VLAN Stacking or Q-in-Q encapsulation (IEEE 802.1ad). This architecture utilizes two distinct tags:

CVLAN (Customer/Client VLAN): This is the inner tag (standard 802.1Q). It is defined and managed by the end-user or edge equipment. For example, a local site might use CVLAN 10 for Administration and CVLAN 20 for Security Cameras.

SVLAN (Service/Provider VLAN): This is the outer tag applied by the core network edge router or Optical Line Terminal (OLT). When traffic leaves the local site and enters the core backbone, the network wraps the CVLAN-tagged packets inside an SVLAN tag. The core network only routes based on the SVLAN.

This architecture allows a service provider to assign a single SVLAN to a specific site or customer, seamlessly transporting all of their internal CVLANs across a shared backbone intact and fully isolated.

2.103 Running a Converged Network

A converged network consolidates multiple distinct types of communication (standard internet data, voice-over-IP, video surveillance, and real-time operational telemetry) onto a single shared physical infrastructure. While highly cost-effective and scalable, convergence introduces the risk of low-priority traffic saturating links and disrupting critical services.

Operating a converged network successfully requires strict traffic engineering:

Class of Service (CoS) and QoS: Utilizing the priority bits within the VLAN tags (IEEE 802.1p), traffic must be classified at the edge. Voice or real-time control traffic is tagged for strict priority queuing, ensuring it is transmitted before standard web traffic during periods of congestion.

Bandwidth Policing: Strict bandwidth limits must be enforced per CVLAN or SVLAN to prevent any single service (such as municipal data sinks or heavy video streams) from overwhelming the core trunk links.

Deterministic Performance: For critical operational technology (like grid protection relays), the converged backbone must guarantee maximum latency and jitter thresholds. This is achieved by combining robust physical paths (like full-mesh fiber topologies) with strict logical SVLAN separation and QoS prioritization.

2.11 IEC 61850 Model

Virtualization of PAC systems requires tools that can accurately represent all components and their behavior under varying conditions. The IEC 61850 standard was developed to support this using object-oriented design principles. The original model focused on substation automation systems, reflecting the functionality of microprocessor-based protection devices and communication technologies at the end of the 20th century [7].

As protection and control technology evolved, and as electric power grid requirements expanded, the focus of IEC 61850 shifted from just substations to broader power system automation. This led to updates in the model to cover different power system domains while improving virtualization accuracy, reliability, and PAC system efficiency.

Below an exploration of the evolution of the IEC 61850 model is laid, representing multifunctional IEDs collaborating over communication networks to perform distributed functions. It begins with the IED object model as a server, its component hierarchy, and data modeling using data objects and attributes. The standard also defines semantic naming principles used in object and data modeling. Part 5 of IEC 61850 outlines the model requirements and concepts, while Part 7 defines the actual model at three levels [10]:

1. Abstract Communication Service Interface (ACSI): Specifies models and services for accessing object elements, such as reading/writing values or controlling substation equipment.
2. Common Data Classes (CDCs) and data attributes: CDCs define structures containing one or more data attributes.
3. Logical node classes and data classes: These are specialized versions of CDCs tailored for specific applications.

While IEC 61850 effectively standardizes logical nodes, data objects, and attributes, it does not standardize the use of logical devices. Their implementation is left to device developers, resulting in varied models.

1.111 IEC 61850 Logical Node Object Model

The PAC system modeling relies on functional decomposition, where logical nodes represent the smallest functional elements in IEDs that perform specific functions. These nodes allow the exchange of information between devices but do not standardize the algorithms or logic behind the functions.

Each logical node resides in a physical device and can participate in local or distributed functions. Local functions exchange data internally, while distributed functions communicate over a network. Logical nodes are grouped by application, such as protection or measurement, and Part 5 of the standard categorizes them into:

- Logical nodes for substation PAC functions
- Logical nodes for primary substation or power system equipment

1.112 IEC 61850 Server Object Model

In IEC 61850, a server represents any physical device in a PAC system and exposes the device's communications-visible behavior. Servers can range from simple merging units publishing current and voltage samples to complex multifunctional IEDs for transformer protection. Examples of intermediate devices include distribution feeder protection relays.

The server model includes a set of attributes and services defined in Part 7-2, such as:

- Server access point: An abstraction to identify the server; multiple access points are possible.
- Logical device: Identifies one or more logical devices within the server, depending on complexity.
- File system: Identifies a file system if present.
- Two-party application associations**:** Identifies clients for bidirectional, connection-oriented communication.
- Multicast application associations**:** Identifies subscribers for unidirectional communication, where the server acts as a publisher.

The GetServerDirectory service supports self-description, enabling the server to provide information about its implemented functions without consulting the device manual. The server responds with logical device names or file system names when queried [5].

This version simplifies some of the technical details while keeping all essential information intact and in a logical flow.

1.113 The IEC 61850 Data Model
Data Modeling Principles

Logical nodes contain the data required for specific functions within a PAC system. The attributes of these nodes, called data objects, can have either simple or complex structures depending on the type of information they represent.

Logical nodes typically hold not only data but also data sets, control blocks, logs, and other elements as defined by the standard. The data represents domain-specific information available in devices integrated into a power system automation system [3]. Data may be grouped into data sets based on the needs of the application, and all data must follow the structure defined in IEC 61850. Each data object includes the components listed below:

- **DataName:** The instance name of the data object.
- **DataRef:** The object reference, defining the path to the data object instance.
- **Presence:** A Boolean attribute indicating whether the data object is mandatory, optional, or conditional.
- **DataAttributes:** Each data object must have at least one DataAttribute, which may be simple or nested. Nested attributes use the name DAComponentName for each level beyond the first.

DataAttributes are assigned a data type, which can be either primitive (BasicType) or composite (DAType). They can be grouped according to their specific function, such as indicating the logical node's status, configuration parameters, or measurement values. Each DataAttribute has a functional constraint (FC) that defines its intended use. Common functional constraints include:

- **ST:** Status information
- **CO:** Control
- **SP:** Set point not belonging to a setting group
- **CF:** Configuration
- **DC:** Description (human-readable information)

- **SG:** Setting group (part of a group of settings)
- **MX:** Measurements (analog values)

This structured approach ensures that the data in IEC 61850 devices is clearly defined, organized, and usable across various applications within the power system automation system.

2.12 IEC 61850 Requirements

Interoperability

One of the main requirements of IEC 61850 is interoperability, the ability of devices from different manufacturers to exchange and correctly interpret data, enabling coordinated operation. In MV and LV networks, this ensures that devices such as protection relays, meters, and controllers can communicate seamlessly. For example, in a permissive overreaching transfer trip (POTT) scheme, if a relay on an MV feeder receives a message indicating a Zone 2 trip from another relay, it can respond faster, improving protection performance. IEC 61850 focuses on standardizing the data exchange and semantics, not the internal algorithms, ensuring devices "speak the same language" without enforcing identical protection logic across manufacturers.

Free Configuration

IEC 61850 supports free configuration, allowing utilities to implement diverse protection, automation, and control philosophies in MV and LV networks. Modern multifunctional IEDs can integrate measurement, protection, control, recording, and analysis within a single device, or these functions can be distributed across devices in the power system cluster yard. Cloud-based or centralized PAC (Protection, Automation, and Control) implementations are also supported. The standard ensures that changes in technology or architecture such as moving from a distributed MV/LV PAC system to a cloud-based one can occur without redesigning the system, as long as data models and flows remain consistent.

Long-Term Stability

Long-term stability is essential due to ongoing advancements in both the grid and digital technology. IEC 61850 ensures that MV and LV network PAC systems can evolve from traditional IED-based setups to centralized or cloud-based systems while maintaining the same functionality. Similarly, interfacing systems such as SIPS (System Integrity Protection Schemes) should work consistently whether they interact with large generators or distributed DERs like solar or wind farms. The standard also supports extending substation-level modeling and communication to wider areas, including MV/LV distribution automation and DER integration, ensuring consistent operation even under cybersecurity threats.

Flexibility

Flexibility allows designers to implement their preferred methods for protection and automation. In MV and LV networks, this means function elements may differ between implementations. While extreme flexibility may reduce interoperability, IEC 61850 accommodates profiles or

guidelines to limit variability and enhance device compatibility, ensuring devices can still work together effectively.

Communication Support

Communication is critical for MV and LV network automation. IEC 61850 defines interfaces and services to meet diverse PAC requirements, including event-driven and streaming peer-to-peer communications, client-server communications, reporting, time synchronization, and file transfers. Performance classes are defined to ensure the communications meet operational needs. Substation communications are generally secure, but for MV/LV networks extending beyond the substation, cybersecurity measures are essential.
This version emphasizes how IEC 61850's principles directly impact MV and LV networks, especially in terms of interoperability, configuration flexibility, and reliable communication across protection and automation systems.

2.13 Modeling Requirements in MV and LV Networks

The requirements of IEC 61850; interoperability, free configuration, and long-term stability translate into a range of detailed modeling needs for digitalized power systems, including MV and LV networks. These requirements cover multiple aspects:

- Modeling multifunctional devices: MV and LV networks increasingly use IEDs that integrate protection, control, and measurement functions. Accurate modeling of these devices is essential for consistent operation and communication.
- Modeling function elements: Each IED consists of multiple functional components (function elements), such as overcurrent protection, voltage monitoring, or breaker control. In MV and LV systems, defining these elements clearly ensures correct interaction between devices.
- Modeling data within function elements: The data exchanged between elements like current or voltage measurements, status signals, and control commands must be consistently represented to support applications such as feeder protection or LV network automation.
- Grouping function elements and defining hierarchies: Organizing elements into functions and establishing a hierarchy mirrors the physical and operational structure of MV and LV grid sections, helping operators and automation systems understand relationships between devices.
- Defining specific data types: Different functions require different types of data (e.g., real-time analog measurements for overcurrent protection, or event records for fault analysis). Standardized data types in MV/LV networks reduce miscommunication and ensure interoperability.
- Modeling complete PAC systems: Digital modeling must represent not only IEDs but also the primary equipment (transformers, feeders, breakers) and the communications network that links them, enabling MV and LV grids to function cohesively.
- Associating functions to primary equipment and networks: Every function and its data exchange must be tied to the actual physical components and the power system communications infrastructure, which is crucial when replacing traditional hardwiring with digital communication.

Transitioning from wired connections to digital communications in MV and LV networks fundamentally changes system testing and maintenance. For example, live testing requires virtual isolation of components under test and distinguishing between messages from real devices versus test equipment. Accurate time synchronization is also critical to ensure coordinated operation and event recording across the network.

2.14 Modeling Multifunctional IEDs in MV/LV Networks

Creating accurate models for multifunctional devices such as a modern transformer protection relay in an MV grid requires a deep understanding of the device's functions and interactions. The models focus on the communication-visible aspects of the IED, allowing different PAC philosophies to be implemented. Simpler devices, like a basic LV feeder relay, have straightforward functions that are easy to model. More complex devices, such as advanced transformer protection relays on three-winding transformers in MV networks, require careful organization of function elements to capture all protection, control, and measurement capabilities.

2.15 The IEC 61850 Standard and Related Documents

The IEC 61850 standard was initially developed to define modeling and communication requirements for substation automation, and it has since expanded to cover a broader range of power utility automation, including smart grid applications in MV and LV networks. Directors and senior managers rely on the standard to guide system architecture, ensure interoperability, and plan the digitization of MV/LV networks while integrating substation automation and distributed energy resources (DERs).

Documents with a publication year indicate completed standards, while those without a year are still under development. Technical Specifications (TS) and Technical Reports (TR) provide guidance, analysis, and recommendations that directors rely on to make informed decisions about system upgrades, interoperability, and integration with legacy equipment. Amendments (AMD) reflect updates to previous editions, which directors must consider when planning system expansions or retrofits [11].

- **Part 1: Introduction and Overview**. IEC 61850-1 (TR, 2003; Edition 2, 2013) provides an overview of the standard, including applications beyond substations to MV and LV networks, such as DER monitoring, power quality, and substation-to-substation communication. Directors use this part to assess strategic adoption across distribution networks.
- **Part 2: Glossary**. IEC 61850-2 (TS, 2003; revised 2019) defines terms relevant to both substation and distribution automation. This ensures directors, engineers, and operators have a shared understanding of terminology for MV/LV network automation, DER integration, and smart grid expansion.
- **Part 3: General Requirements**. IEC 61850-3 (2002; revised 2013) outlines functional, reliability, and environmental requirements for IEDs, including devices used in MV and LV distribution networks. Directors use this part to guide procurement and risk management for IED deployment in lower voltage networks.
- **Part 4: System and Project Management**. IEC 61850-4 (2002; revised 2011, AMD1 2020) covers engineering processes, project management, and lifecycle requirements. Directors

leverage this for planning MV/LV automation projects, ensuring consistent engineering practices across substation and distribution automation.

- **Part 5: Communication Requirements for Functions and Device Models** IEC 61850-5 (2003; revised 2013) defines logical node modeling and communication requirements. In MV and LV networks, it ensures interoperability between IEDs, switches, reclosers, and DER controllers. Directors use this part to evaluate integration feasibility across distribution networks.
- **Part 6: Configuration Description Language (SCL)**. IEC 61850-6 (2004; revised 2009, AMD1 2018) introduces SCL for modeling IEDs and substation/distribution network connectivity. This enables MV/LV automation planning, including DERs, feeders, and network monitoring. Directors benefit by seeing how multi-vendor systems can interoperate across the distribution level.
- **Part 7: Basic Communication Structures**

7-1**:** Provides architecture for communication between substation and feeder devices, relevant for MV/LV distribution automation, hierarchical logical devices, and testing.

7-2**:** Defines the Abstract Communication Service Interface (ACSI) for high-speed communication and sampled values in both substation and distribution network IEDs.

7-3**:** Specifies common data classes for status, measurements, and control information in MV/LV networks.

7-4: Defines logical nodes and compatible data objects, supporting interoperability in smart MV/LV networks, DERs, and feeder automation.

- **Part 8: Specific Communication Service Mappings (SCSM)**

8-1: Maps ACSI to MMS and Ethernet for substation LANs and MV/LV network communications.

8-2: Maps to XMPP for wide-area or public network applications, including distribution-level smart grid communications. Directors use these parts to plan communication architecture, network security, and integration of MV/LV networks with utility automation systems.

- **Part 9: Sampled Values and Process Bus**

9-1: Ethernet-based transmission of sampled values, foundational for the process bus in MV/LV networks.

9-2: Precision Time Protocol (PTP) for time synchronization, crucial for fast control and protection in distribution automation. Directors consider these parts when designing MV/LV automation systems and process-level digitization.

- **Part 10:** Conformance Testing. IEC 61850-10 (2005; revised 2012) specifies testing procedures for IEDs, engineering tools, and communication services. Directors rely on this to

ensure compliance, reliability, and interoperability in MV/LV network automation, supporting smart grid and DER integration.

This version highlights where IEC 61850 supports MV and LV network automation, distributed generation, feeder automation, and smart grid integration, while still referencing directors' roles in oversight, planning, and decision-making.

2.16 IEC 61850 Sampled Value

Sampled value transmission is a main technology in modern IEC 61850-based digital substations, offering significant benefits for protection, control, and disturbance recording, including in medium- and low-voltage networks [1].

2.161 IEC 61850 Sampled Value Model

The evolution of SV communications benefited from prior experience with IEC 60044-8 and was formalized in IEC 61850-7-2 (2003). The standard defines the SV class model, which uses publisher-subscriber communications similar to GOOSE messages, but streams continuous analog measurements rather than event-based status changes [15]. Directors involved in system architecture and planning must understand the two main transmission methods:

- **Multicast:** Delivers SV data to multiple subscribers simultaneously, optimizing network usage for large-scale implementations.
- **Unicast:** Sends SV data point-to-point via a two-party association, though this method is less common in practical applications.

The SV model ensures time-controlled and synchronized transmission, often using GPS signals for precise sampling coordination. Directors and technical leaders are responsible for specifying these synchronization requirements to ensure interoperability and system reliability [2].

IEC 61850 leaves the definition of logical devices to manufacturers, but the standard promotes interoperability by defining a merging unit (MU) logical device profile. Each current transformer (TCTR) or voltage transformer (TVTR) logical node digitizes a single phase or neutral signal, with sampled values organized in the PhsMeas1 dataset transmitted via the ASDU (Application Service Data Unit). Directors overseeing substation upgrades must account for these standards when approving equipment selection and integration strategies.

By adopting SV communications, directors can facilitate a more streamlined, accurate, and high-speed data flow between IEDs, reducing wiring complexity, improving system reliability, and enabling flexible, scalable PAC system architectures.

2.162 Busbar Differential Protection

A prime example of the benefits of sampled values is busbar differential protection. Traditionally centralized, these systems summed currents from all CTs to define the protection zone. With sampled values and high-speed substation communications, bus differential protection can now

adopt a distributed architecture. This enables dynamic adjustment of the protection zone based on real-time knowledge of substation topology and breaker or switch status. Merging units digitize analog signals from sensors and publish sampled values over the process bus to a central unit that calculates differential currents and detects faults. This distributed setup ensures accurate protection and avoids the safety risks associated with manual changes to current circuits [4].

The main components include:

- **Central differential unit:** Performs fault detection and related functions.
- **Merging units:** Convert analog signals into sampled values for transmission.
- **Ethernet switches:** Facilitate high-speed process bus communications.
- **Time synchronization devices:** Ensure precise timing for sample alignment.

GOOSE messages from switchgear interface units allow the central unit to continuously track substation topology, enabling automatic adaptation of protection zones without interrupting service. Breaker and switch statuses are represented using XCBR and XSWI logical nodes, which provide phase and auxiliary contact information for accurate topology modeling. The system configuration description (SCD) file standardizes substation topology, facilitating interoperability and configuration.

2.163 Disturbance Recording

IEC 61850 sampled values also enhance disturbance recording in medium- and low-voltage networks. Transient or waveform recording captures detailed current and voltage samples, while centralized disturbance recorders can subscribe to multiple sampled value streams and GOOSE messages. Triggering can be internal (e.g., based on instantaneous measurements or superimposed components) or external via GOOSE messages from protection devices. Records are typically stored in COMTRADE format, supporting detailed analysis of faults, relay operations, or system behavior.

Process interface devices (PIDs) play a central role, often including:

- **Merging Units (MU):** Interface with sensors to publish sampled values.
- **Switchgear Interface Units (SIU):** Provide GOOSE-based information from breakers and disconnectors.

PIDs are precisely time-synchronized, enabling accurate M- or P-class synchrophasor measurements for disturbance recording. Centralized disturbance recording reduces the need for dedicated devices, improves engineering efficiency through SCD files, and provides high reliability with redundant interfaces.

2.164 Communication Considerations

Sampled value transmission relies on high-speed network infrastructure. While IEC 61850 9-2 LE is commonly used today, IEC 61869-9 will reduce traffic while increasing frame size. In medium- and low-voltage substations with star or ring topologies, 1 Gbps links are usually sufficient, but

larger substations with many merging units may require 10 Gbps to accommodate the increased traffic from protection testing and waveform recording [6].

2.17 IEC 61850 GOOSE

Given that several members of IEC TC 57 Working Groups 10 and 11 were actively involved in developing GOMSFE, it was natural for GOOSE to be incorporated into the IEC 61850 standard. Even before its formal inclusion, multiple manufacturers had implemented UCA GOOSE in multifunctional IEDs, and a few substations were already using it. These early implementations provided valuable insights that shaped the evolution of GOOSE communications within IEC 61850.

When IEC 61850-7-2 was published in 2003, it introduced the Generic Substation Event (GSE) class model, which was fundamentally based on the UCA GOOSE model for peer-to-peer communications between publishers and subscribers. The standard defined two control classes and corresponding message structures [6]:

1. **Generic Substation State Event (GSSE):** Essentially the UCA GOOSE, included to maintain backward compatibility with existing devices and systems that used UCA GOOSE bit pairs to indicate state changes.
2. **GOOSE:** Designed to support the exchange of a broader range of data from logical nodes, organized into user- or manufacturer-defined data sets.

IEC GOOSE is object-oriented, allowing data sets to contain multiple data objects or attributes to support a variety of applications. When a new value for a data attribute triggers a GOOSE message, a repetition mechanism ensures that the message is repeatedly sent with varying time intervals until the next change occurs.

The contents of a GOOSE message allow receiving devices to process the data and execute the necessary actions. A notable feature is the support for analog GOOSE, which can carry values of analog system parameters, such as the load on a distribution feeder. This enables IEDs without client capabilities to subscribe to analog GOOSE messages and receive updated values whenever a monitored parameter moves outside its deadband, with each update carrying an incremented state number.

2.171 Reducing Fault Duration on Distribution Feeders

The need to shorten the duration of short-circuit faults on distribution feeders and substation equipment has grown due to the increasing number of DERs and customers with voltage-sensitive loads. High-speed fault clearing can be achieved through advanced communications-based protection schemes that adapt to changing conditions, enhancing both sensitivity and performance.

The performance of protection and control IEDs is often influenced by the configuration of the substation or power system. For example, with conventional relays, adjusting to changes in system grounding is challenging [8]. If a feeder relay is in a substation with two transformers one grounded on the high side and the other on the low side taking one transformer out of service alters zero-

sequence current levels for ground overcurrent protection. If the distribution-side transformer (T1) is taken offline, the system changes from solidly grounded to isolated, necessitating significant adjustments in protection settings. Phase fault currents also vary depending on which transformer is out of service.

To address these changes, transformer protection IEDs monitor the status of transformers and send GOOSE messages when a transformer is taken out of service. Feeder protection IEDs subscribe to these messages and switch to the appropriate setting group to maintain optimal sensitivity under the new conditions.

2.172 Adapting to Faults on Adjacent Feeders

Faults on one feeder can impact sensitive loads on other feeders and may trigger protection devices on healthy feeders. Detecting a fault on a neighboring feeder allows relays on healthy feeders to temporarily adjust settings during the inrush condition following fault clearance. This approach, known as a **sympathetic trip scheme**, helps avoid unnecessary trips due to temporary current surges.

When a relay detects a fault on its feeder, it sends a signal to all other relays indicating an expected inrush. The relays on adjacent feeders then adjust their settings, either by blocking sensitive overcurrent settings or raising the pickup thresholds for the duration of the inrush. In conventional hardwired substations, this is often impractical due to limited relay outputs. GOOSE messaging overcomes this limitation by allowing the faulted feeder relay to broadcast the fault condition to all neighboring relays, which then adapt automatically.

2.173 Adapting to the Loss of a Protection IED

Many utilities rely on a single protection IED per feeder. If this relay fails, faults are cleared by backup overcurrent protection on transformers or sectionalizing breakers, often resulting in long fault-clearing times that can affect sensitive loads. Adaptive protection reduces fault duration by enabling backup relays to respond when a primary IED fails.

This method uses normally closed contacts of feeder relays that open when the relay fails. If a transformer or breaker detects a fault and receives no blocking signal from the feeder relays, it considers two possibilities:

1. The fault is on the feeder with the failed relay.
2. The fault is on the distribution bus.

The relay first trips the breaker of the failed feeder. If the fault persists, it then clears the bus fault by tripping the source breakers. While this can be implemented in substations with few feeders using hardwiring, it becomes impractical for larger substations due to the need for multiple dedicated inputs.

GOOSE messaging solves this challenge by allowing the transformer protection device to subscribe to messages from all feeder relays. If messages from a specific relay are not received

and no communication failure is detected, the system can infer the relay has failed and implement the adaptive fault-clearing logic, even in large substations with many feeders.

2.174 GOOSE Applications for Transmission Line Protection

Traditionally, accelerated protection schemes have been applied to transmission lines where slower fault clearing could negatively affect the dynamic stability of the power grid. A major limitation of these schemes has been the high cost of communication equipment, which has restricted their use to only the most critical locations. Short-circuit faults at the transmission level can cause voltage dips that propagate to the distribution network, potentially affecting the ride-through capability of distributed energy resources (DERs). Consequently, modern protection schemes aim to minimize fault duration at the transmission level in as many cases as possible.

This can be achieved by implementing accelerated protection schemes that use communication between relays at both ends of the protected line while addressing the cost of communication channels. One example is the permissive directional comparison scheme, widely used to speed up clearing for all types of faults, including high-resistance faults that may not be detected by distance protection elements or line differential relays. In this scheme, the forward-looking relay element is represented in the IEC 61850 model by the logical node RDIR.

When the relay detects a forward fault:
RDIR.Dir.dirGeneral = forward

A GOOSE message containing the RDIR.Dir or RDIR.Dir.dirGeneral data is sent to the relay at the other end of the line. If the remote relay also identifies a forward fault upon receiving this signal, the protection scheme represented by PDIR is triggered.

This approach provides significant benefits, particularly when high-speed directional detection methods based on superimposed current and voltage components are used. Permissive schemes are generally more secure than blocking schemes because a forward directional decision must be confirmed at both ends before tripping occurs. If the communication channel fails, no signal is sent, and the relay does not trip based solely on a single-end forward detection, preventing false operations.

In systems with weak sources, such as networks with high DER penetration, the permissive directional comparison scheme incorporates weak infeed logic. Additionally, current reversal guard logic prevents false tripping caused by high-speed current reversals, which can occur in double-circuit lines when breakers operate sequentially. In the event of communication failure, the basic distance protection scheme usually remains available as a backup.

2.175 GOOSE Applications in System Integrity Protection Schemes (SIPS)

System Integrity Protection Schemes (SIPS) are distributed applications that rely on the exchange of information and control signals between Intelligent Electronic Devices (IEDs) across multiple substations or feeders in the power system.

SIPS generally consist of three main types of functional elements:

1. **System monitoring elements**
2. **Protection elements**
3. **Execution elements**

The system monitoring elements detect changes in the power system, such as shifts in topology, load, or generation. Information about these changes is communicated between SIPS components via R-GOOSE messages**,** which carry status updates or analog data

CHAPTER THREE

PROJECT EXECUTION METHOODOLOGY

A mixed-methods approach was employed in this study, combining qualitative and quantitative techniques, to evaluate the application of the IEC 61850 standard for communication-based protection, automation, and control (PAC) and asset management within medium-voltage (MV) and low-voltage (LV) grid networks in Uganda.

The research was executed in two primary phases:

Phase 1: Empirical Data Collection

Primary Data: Gathered through interviews, surveys, and direct consultations with utility engineers and regulatory officials at UEDCL and at TELMEC SOLITON.

Secondary Data: Collected from telecommunications engineers at TELMEC SOLITON and Power System engineers at UEDCL, established IEC 61850 documentation, and comparative case studies on MV and LV network digitization.

Phase 2: Technical Analysis and Evaluation

Protocol Evaluation: IEC 61850 functionalities and communication protocols were critically evaluated regarding their impact on accelerated protection and asset management.

Network Proposal: A communication network topology was proposed specifically for the MV distribution grid within the case study area (Kampala Metro-Wandegeya Feeder), applying IEC services to test their viability for PAC operations.

Performance Simulation: Mathematical models defining data flow and network behavior were simulated utilizing the OMNeT++ framework to rigorously assess system interoperability, reliability, and end-to-end response times.

This section provides a high-fidelity performance evaluation of a converged smart grid communication architecture.

Specifically, it tests the viability of running critical IEC 61850 telemetry over a shared 29.6 km passive optical network (PON) for feeder automation. If utilities are to shift toward cost-efficient, converged fiber infrastructures, ensuring that mission-critical protection data remains isolated from volatile public broadband traffic is paramount.

Through a detailed examination of both edge nodes and intermediate splitting stages, this section serves as a technical validation for deploying secure, high-performance telemetry within modern converged distribution feeders.

3.1 PHASE ONE: EMPIRICAL DATA COLLECTION AND AGGREGATION

To establish an accurate simulation baseline for this evaluation, preliminary distribution grid parameters from UEDCL and optical fiber infrastructure specifications from TELMEC SOLITON were sourced.

3.1.1 Grid Data Gathered

SUBSTATIONS AND SERVICE FEEDERS

The table presents a structural breakdown of Kampala's power grid architecture. It catalogs major substations and their associated localized feeder networks, substation capacity metrics required for effective grid management and load profiling.

Table 1. Structural breakdown of kapala's power rid architecture

Feedername	**Substation**
Nakasero 33 kV from Kampala North	KAMPALA NORTH
Acacia Mall 11 kV from Kampala North	KAMPALA NORTH
Down Town 11 kV from Kampala North	KAMPALA NORTH
Kololo 11 kV from Kampala North	KAMPALA NORTH
Mulago Hospital 1 11 kV from Kampala North	KAMPALA NORTH
Wandegeya Market 11 kV from Kampala North	KAMPALA NORTH
Crested Towers 11 kV from Kitante Road	KITANTE ROAD
Dewinton Road 11 kV from Kitante Road	KITANTE ROAD
Kitante 11 kV from Kitante Road	KITANTE ROAD
Motormart 11 kV from Kitante Road	KITANTE ROAD
Mukwano 11 kV from Kitante Road	KITANTE ROAD
Kampala Industrial 11 kV from Lugogo	LUGOGO
Amber House 11 kV from Motor Mart	MOTOR MART
Neeta Cinema 11 kV from Motor Mart	MOTOR MART
Uganda Railways 11 kV from Motor Mart	MOTOR MART
Kitante Road 33 kV from Queensway	QUEENSWAY
Kisenyi 11 kV from Queensway	QUEENSWAY
Katwe 1 11 kV from Queensway	QUEENSWAY
Katwe 2 11 kV from Queensway	QUEENSWAY
Lukuli 11 kV from Queensway	QUEENSWAY
Nabugabo 11 kV from Queensway	QUEENSWAY
Motormart 11 kV from Queensway	QUEENSWAY
Namirembe Road 1 11 kV from Queensway	QUEENSWAY
Namirembe Road 2 11 kV from Queensway	QUEENSWAY
Nsambya 11 kV from Queensway	QUEENSWAY
Pioneer Mall 11 kV from Queensway	QUEENSWAY
South Street 11 kV from Queensway	QUEENSWAY
Wilson Lane 11 kV from Queensway	QUEENSWAY

TRANSFORMERS ON THE CASE STUDY FEEDER (WANDEGEYA FEEDER)

The Table below provides a comprehensive breakdown of the empirical data collected for this study, encompassing 64 distinct power distribution units on the Wandegeya feeder. The data is categorized by unit identification, rated capacity, and functional area, spanning from high-capacity primary transformers at the Kampala North Substation to localized Urban Fringe units.

The sampled infrastructure represents a hierarchical distribution network, beginning with the 40 MVA, 132/11kV primary power transformers and extending to secondary distribution units ranging from 50kVA to 500kVA. This dataset captures a diverse range of load profiles, including industrial, residential, and relief sectors

Table 2. A comprehensive breakdown of the empirical data collected, encompassing 64 distinct power distribution units on the Wandegeya feeder.

Unit IDs	Capacity	Area
01 – 02	40 MVA, 132/11kV 40 MVA, 132/11kV	Primary Power Transformers KAMPALA NORTH SUBSTATION
03 - 20	500, 315,200, 100kVA	Wandegeya Feeder Mainline
21 – 30	200kVA	Mawanda Road
31 – 40	100kVA	Makerere Residential Fringe
41 – 50	50kVA	Urban Fringe
51 – 60	315kVA	Load Relief
61 – 64	500kVA	Industrial

APPROXIMATE FEEDER DISPLAY

The provided schematic illustrates the approximate feeder display for the Wandegeya Feeder from KAMPALA NORTH Substation grid segment. It details the logical and hierarchical distribution network from the main substation source through various primary, midline, and branch transformer nodes.

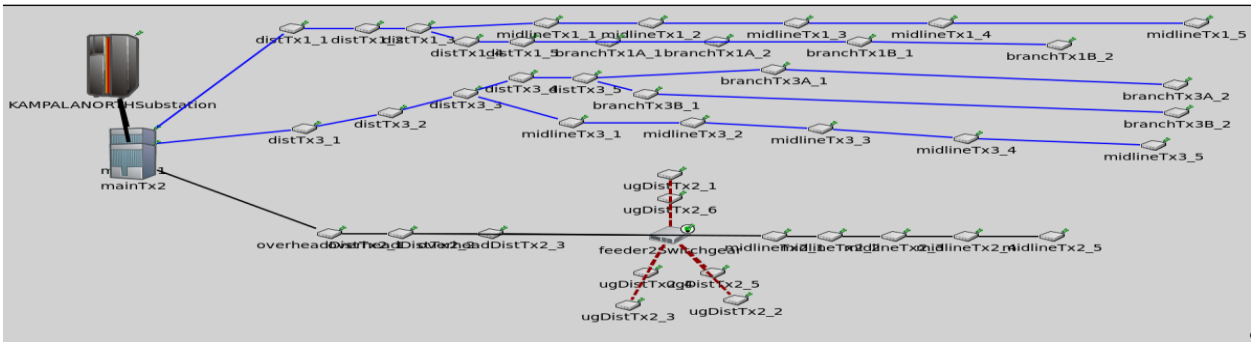


Figure 1. schematic illustrating the approximate feeder display for the Wandegeya Feeder from KAMPALA NORTH Substation grid segment.

This diagram provides a comprehensive visual mapping of the network's structural relationships, highlighting the integration of overhead lines, switchgear nodes, and underground distribution clusters within the Wandegeya Feeder service area.

3.1.2 Fiber Network Data Gathered

This section outlines the physical and logical data collected during the network audit and field survey phase. The objective was to catalog existing assets, verify routing integrity, and assess the current capacity of the fiber infrastructure to support grid IEC 6180 service integration.

Physical Infrastructure and Route Diversity

To support the strict high-availability requirements of feeder automation, physical path data was collected to verify true redundancy. Data gathered focused on Optical fiber cables (OPGW) along transmission lines and optical line terminals near distribution transformer approaches and feeder service areas.

Table 3. physical and logical data collected during the network audit and field survey phase.

Asset Type	**Distance / Quantity**	**Condition**
OPGW (Transmission)		
Optical Line Terminals (OLT)	Several units	Positioned at substation approaches and feeder zones.
Feeder Service Areas		
Substation Entry Points	8 sites	

Logical Network and Capacity Data

Because IEC 61850 traffic specifically Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) messages requires deterministic performance, the logical network audit focused on bandwidth availability and Quality of Service (QoS) configurations.

Bandwidth Utilization:

Current core network utilization on the fiber ring was assessed to establish whether there is ample headroom for the continuous streams of IEC 61850 data required for modern relay protection and asset management.

VLAN and QoS Auditing:

Gathering data on the VLAN segmentation required for grid traffic was a priority in this research. This ensures that Layer 2 QoS tagging (IEEE 802.1p) can be properly standardized across all switches to prioritize critical GOOSE messages over standard operational traffic.

Time Synchronization:

Data on existing Precision Time Protocol (PTP/IEEE 1588) hardware capabilities was to be gathered to evaluate current edge switch support for hardware timestamping, which is a strict requirement for accurate phase measurement synchronization.

Optical Performance and Latency Metrics

In addition to base optical signal testing, understanding current network constraints was a priority for maintaining low-latency environments. Data on existing residential and municipal fiber usage patterns was gathered to properly map out bandwidth allocation and ensure that public or commercial network spikes do not interfere with the under 3millisecond delivery times required for critical grid protection signaling.

NETWORK USAGE DATA AND TRAFFIC MODELLING

Residential Traffic Modeling

Upper limit daily usage on the fiber was modeled at 20GB per single user (data usage per user estimated at 10 – 20 GB a day). Referencing the standard telecommunications rule of thumb that 10% of this daily usage occurs during the busiest hour of the day, this data was converted into a packet send interval. This calculation was utilized to simulate peak load conditions and ensure that commercial network spikes do not interfere with the strict `< 3 millisecond` delivery times required for critical grid protection signaling.

$$peak\ hour\ traffic\ = 20\ \times 0.1\ \times 3$$

$$bitrate\ for\ the\ 3\ users = \frac{20\ \times 0.1 \times 3 \times 8000 Mbits}{3600\ seconds}$$

$$total\ Node\ bitrate\ = 13.33\ Mbps$$

Assuming a standard MTU payload 0f 1450 Bytes (translates to 11600 bits)

$$send\ interval = \frac{11600}{13.33 \times 10^6}$$

$$packetsendInterval = 0.85 msec$$

Municipal Traffic Modeling

To account for high-density public infrastructure, data aggregation nodes were evaluated under a dedicated municipal traffic model. This model assumes a conservative upper limit of 230GB of data usage per day per sink (representing municipal facilities and centralized civic infrastructure hubs).

$$peak\ hour\ traffic\ = 230\ \times 0.1$$

$$bitrate\ for\ the\ \ Musers = \frac{230\ \times 0.1 \times 8000 Mbits}{3600\ seconds}$$

$$send\ interval = \frac{11600}{51.11 \times 10^6}$$

$$packetsendInterval = 0.23msec$$

Referencing the standard telecommunications rule of thumb that 10% of daily traffic occurs during the busiest hour of the day, both the 20GB user profile and the 230GB municipal sink profile were converted into peak packet-send intervals.

These intervals were injected into the network simulations to verify that the fiber ring can sustain worst-case concurrent bursts while still meeting the strict < 3 millisecond delivery times required for IEC 61850 protection signaling.

OLT TIER

The diagram presented demonstrates a highly resilient aggregation layer architecture, modeling the configuration of the Optical Line Terminal (OLT) tier, clustered in a configuration that emphasizes massive redundancy.

This configuration was intended to ensure unparalleled fault tolerance. If any single fiber pathway is severed between nodes, or if a catastrophic hardware failure occurs at an adjacent OLT site, multiple alternate paths are instantaneously available. This allows traffic flows to be rerouted seamlessly without interrupting services at the customer edge or overloading single uplinks to the core routers. This extreme logical mesh design maximizes available bandwidth for direct east-west traffic patterns between OLT sites, minimizing latency for localized service delivery and enhancing load-balancing capabilities across the entire access network.

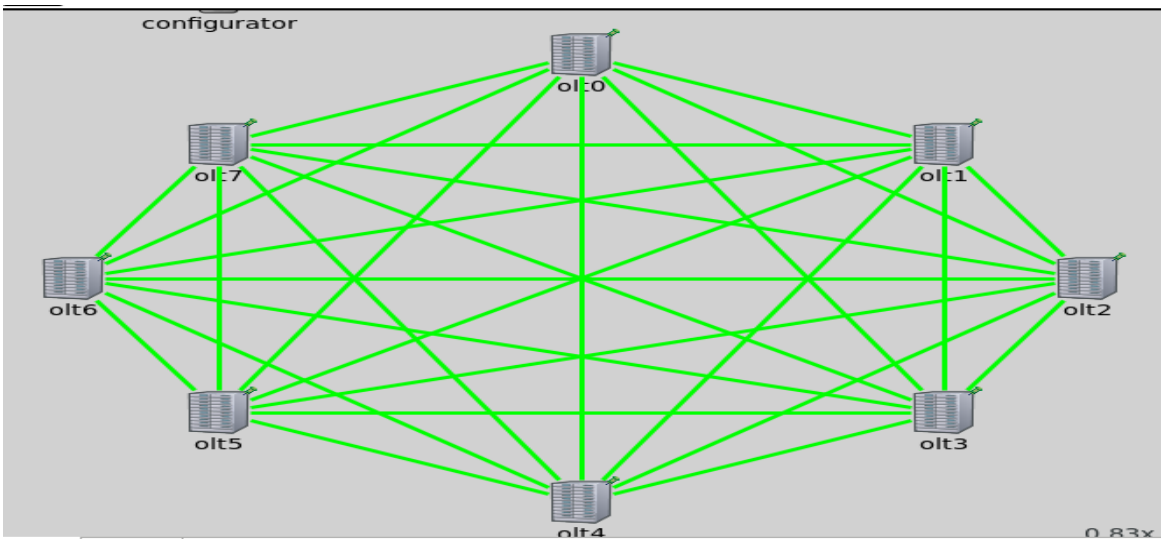


Figure 2. The configuration of the Optical Line Terminal (OLT) tier.

3.1.3 Proposed Power Utility Network Architecture

NETWORK LOGICAL FLOW DIAGRAM

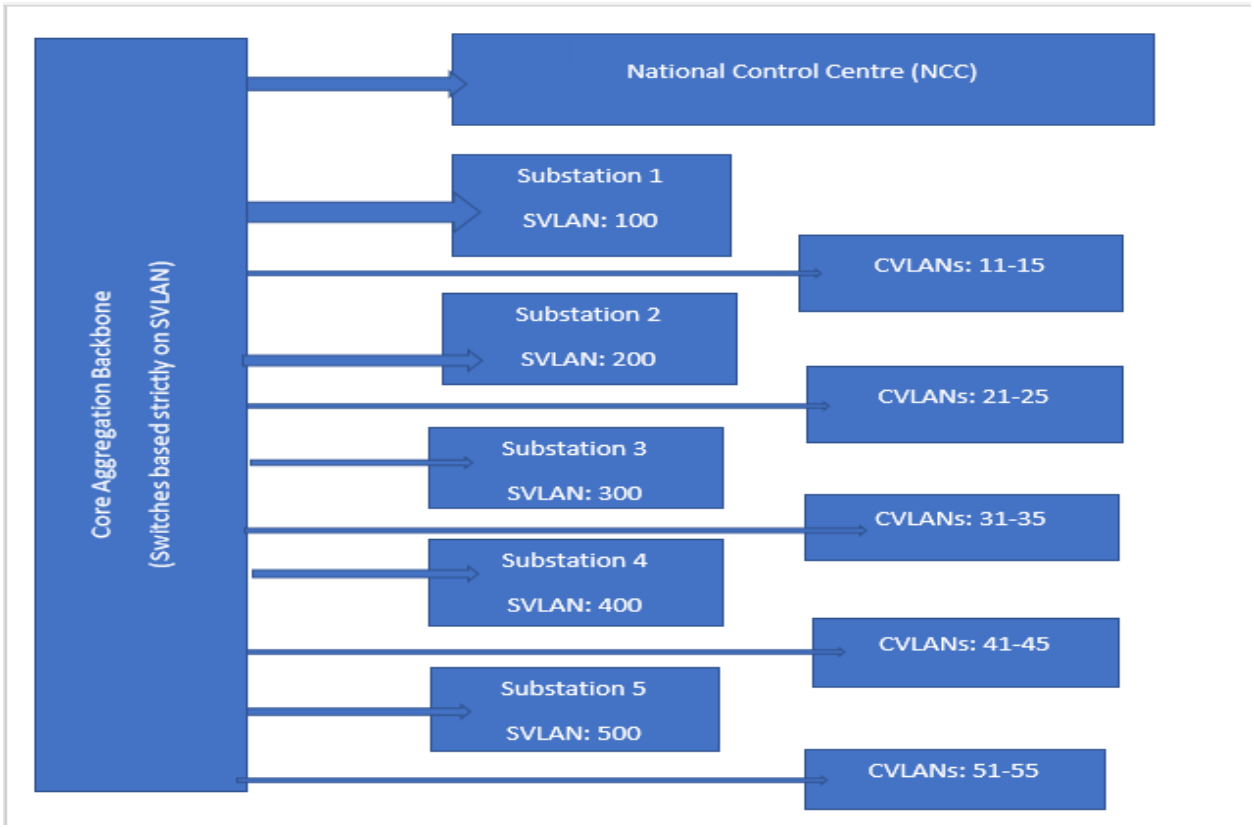


Figure 3. Logical flow diagram showing substations and feeder linkage.

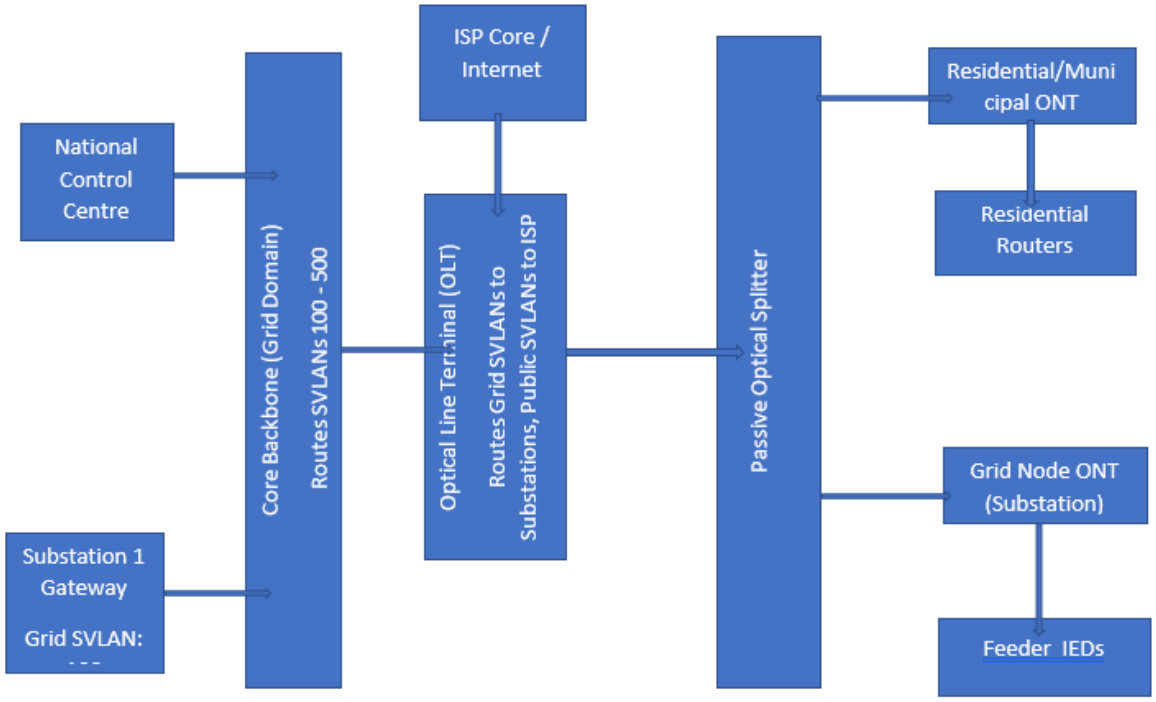


Figure 4. Logical flow diagram indicating how grid flow intersects with residential traffic flow.

DEDICATED ARCHITECTURE (BENCHMARK TEST)

This configuration was designed as a control benchmark test to evaluate against the proposed shared GPON architecture. In this model, a dedicated OLT is assumed at every individual substation, from which all the localized feeder networks served by that substation are directly connected.

Each independent substation cluster features a dedicated OLT splitting traffic down to its respective feeders, while the central control station is isolated on its own separate OLT node to prevent localized traffic faults from impacting core visibility.

Substation-Specific OLT Allocation:

Each major grid node is provisioned with its own standalone OLT and intermediate gateway layer. For example, KAMPALANORTH maps exclusively to gateway1 / olt1, QUEENSWAY maps to gateway2 / olt2, LUGOGO maps to gateway4 / olt4, and MOTORMART maps to gateway5 / olt5.

Isolated National Control Infrastructure:

The NATIONALCENTRE is decoupled from the substation field hardware, interfacing directly through its own dedicated processing chain via gateway6.

By removing the shared elements of the GPON architecture, this topology serves as the ideal performance baseline for evaluating worst-case latency, packet drop rates, and maximum deterministic throughput for critical IEC 61850 GOOSE and Sampled Values (SV) messaging.

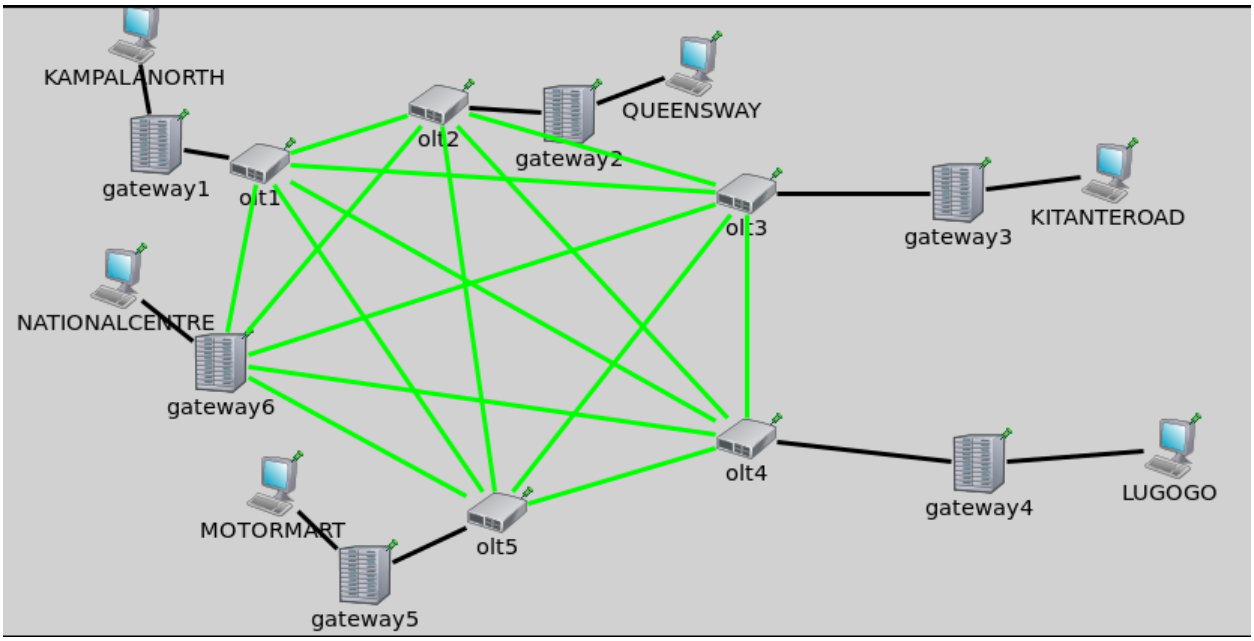


Figure 5. Dedicated architecture to serve as a benchmark test.

SINGLE SUBSTATION NETWORK CLUSTER LAY OUT

The layout models five distinct, independent feeder branches (FEEDER1 through FEEDER5) extending outward from the OLT. Each branch is configured with a two-tier node structure

This layout represents the baseline edge model implemented across the simulation framework to evaluate local traffic behavior, signal propagation, and bottlenecking at the feeder level.

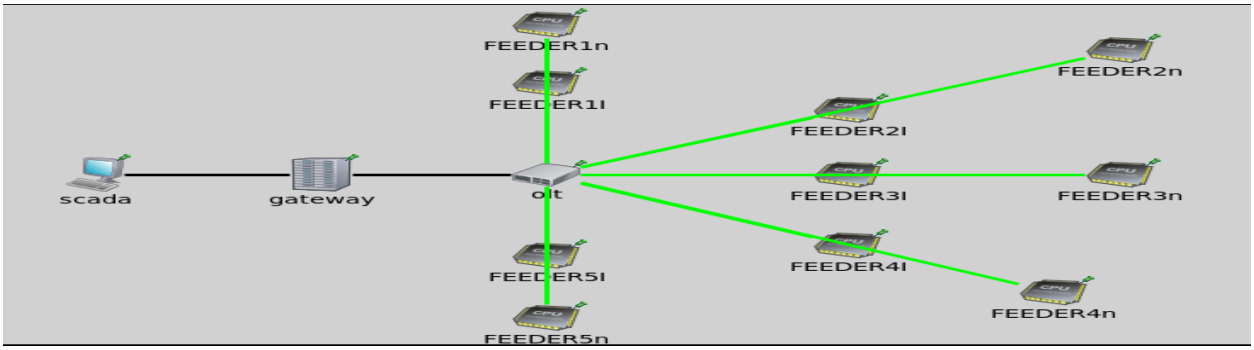


Figure 6. layout representing the baseline edge model implemented across the simulation framework to evaluate local traffic behavior, signal propagation, and bottlenecking at the feeder level.

SHARED GPON

Based on the gathered topology data, a clustered grid network architecture is proposed, as illustrated in the schematic below. The network is logically segmented into distinct, independent substation clusters centered around primary aggregation nodes: QUEENSWAY, KAMPALANORTH, LUGOGO, KITANTE, and MOTOR MART. To enforce strict logical isolation, a two-tier VLAN architecture is implemented. Locally, each substation operates as a separate network cluster utilizing Customer VLANs (C-VLANs) to segregate horizontal traffic across its individual distribution feeders. This localized monitoring layer is represented by dedicated control center nodes (e.g., QUEENSWAYC and LUGOGOC). Furthermore, to securely transmit data across the shared GPON backhaul, each substation gateway is configured with a unique Service VLAN (S-VLAN) via IEEE 802.1ad (QinQ) stacking. This ensures complete, end-to-end isolation of critical grid traffic as it is routed toward the National Control Center.Each substation cluster links to the network backbone through the closest OLT node (for instance, KampalaNorth links through olt1, and LUGOGO links through olt5). The robust core backbone itself is formed by the intensely meshed network of OLTs (olt0 through olt7) and olt8, ensuring a highly available, self-healing path for all traffic. The use of OLTs across these locations confirms the proposed use of a flexible, shared GPON topology.

The National Control Center serves as the apex of the network hierarchy, designed for centralized SCADA aggregation. It interfaces with the broader topology via a dedicated gateway node, NATIONALCENTER, which terminates directly at olt4. Operating as the primary master aggregator within the core GPON mesh, olt4 is strategically positioned to collect and route isolated S-VLAN telemetry from all underlying substation clusters. Together with the nationalControlCenter operator terminal, this centralized structure provides a highly optimized and secure convergence point for grid monitoring across the entire regional network.

Below is a schematic representation of the proposed network:

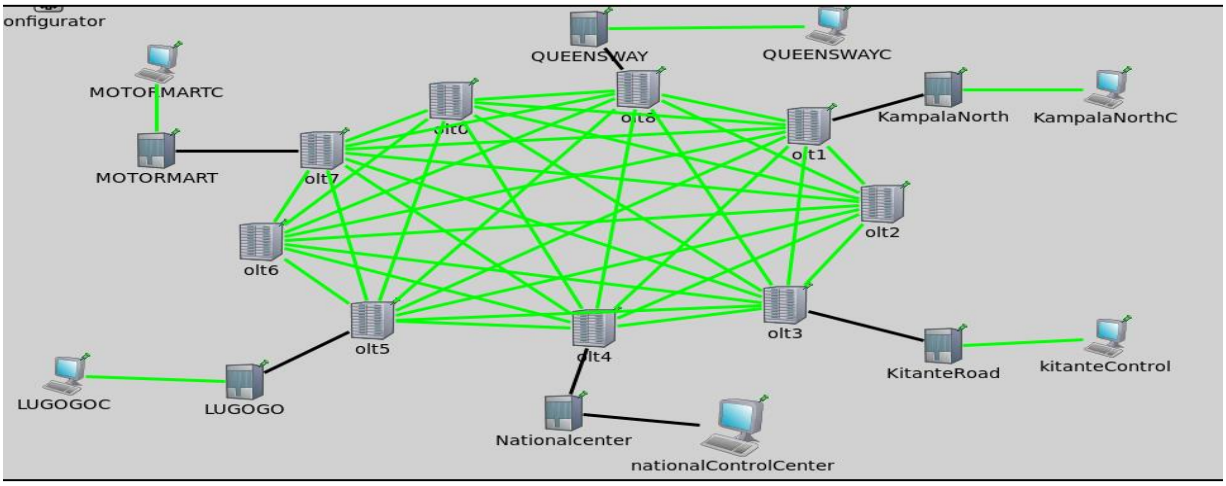


Figure 7. schematic representation of the proposed network

FEEDER LEVEL NETWORK LAYOUT

1) FEEDER SERVICE AREA AND SUBSTATION AREA SERVED BY SEPARATE OLT

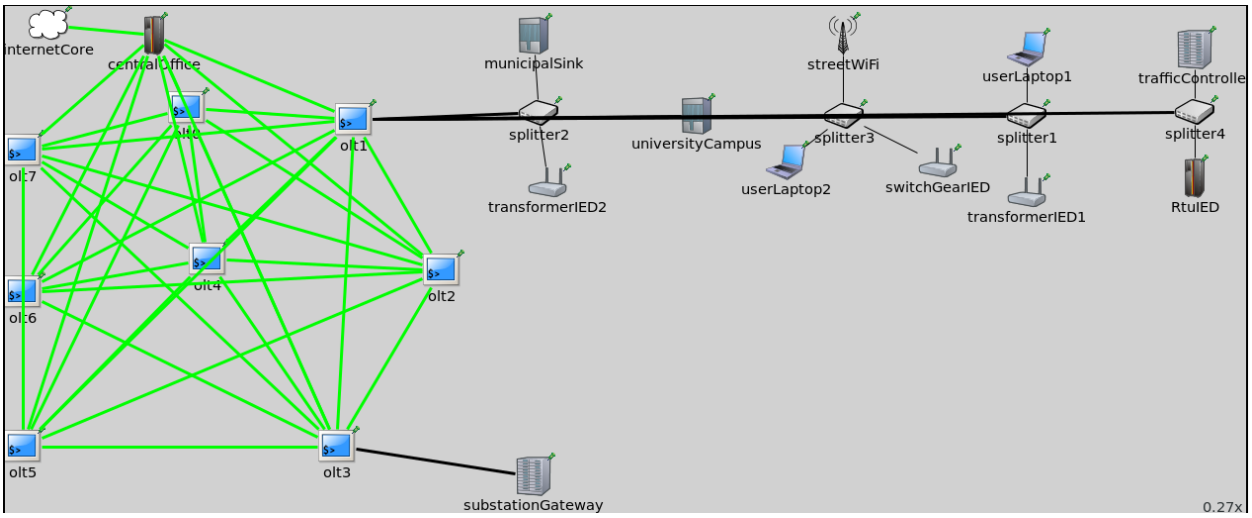


Figure 8. Feeder level network layout-Feeder service area and substation area served by separate Olt.

2) FEEDER SERVICE AREA AND SUBSTATION LOCATION SERVED BY THE SAME OLT

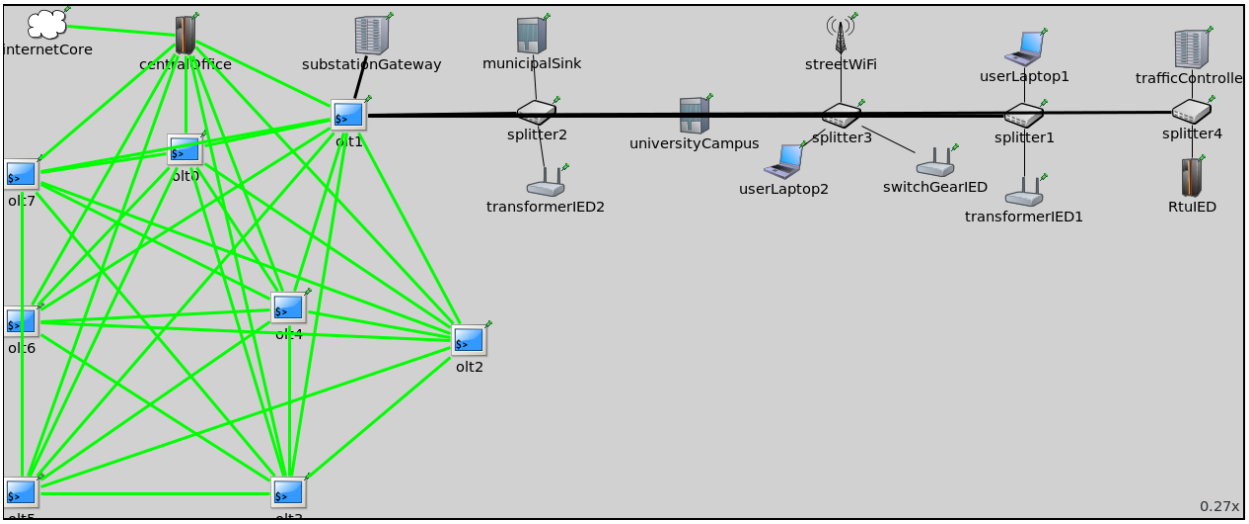


Figure 9. Feeder level network layout-Feeder service area and substation area served by same Olt

3) SECTIONS OF FEEDER SERVICE AREA SERVED BY DIFFERENT OLT

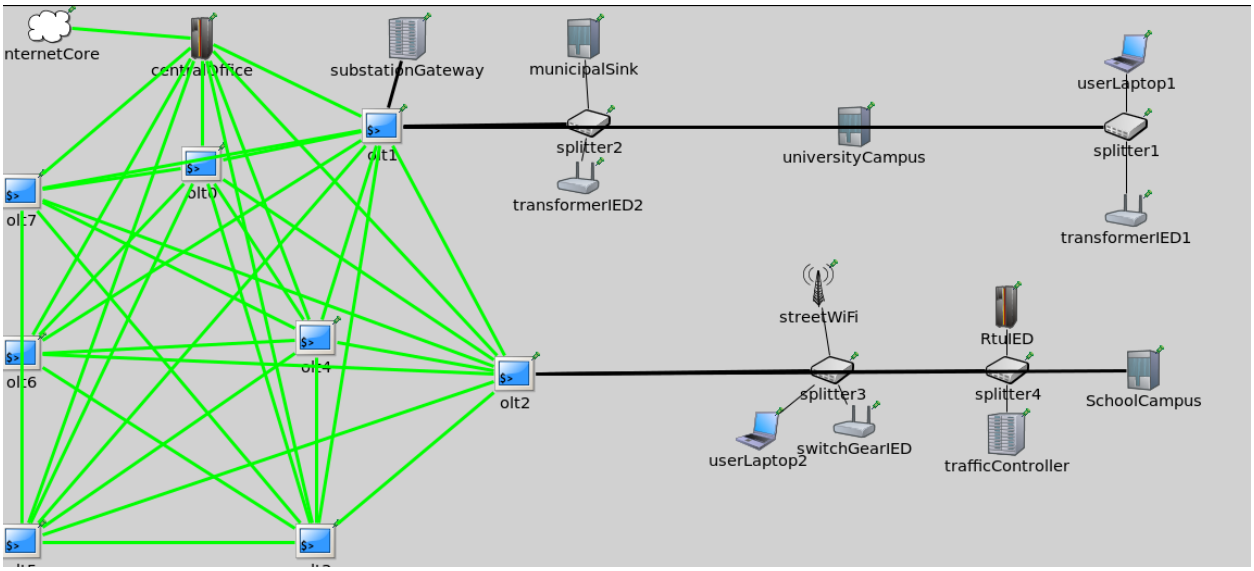


Figure 10. Feeder level network layout-Sections of Feeder service area and substation area served by separate Olt

4) FEEDER SERVICE INTO AREAS SERVED BY SEPARATE OLTS

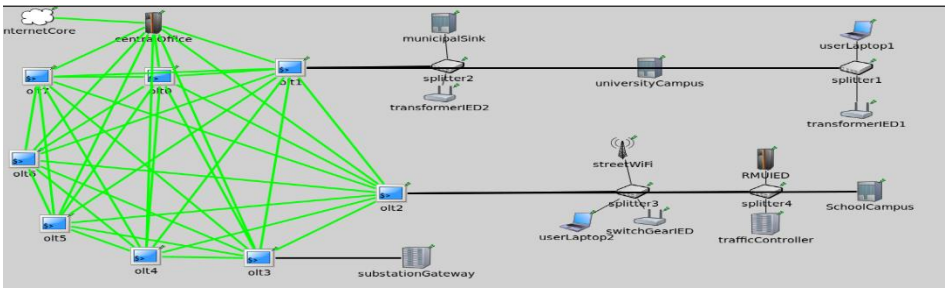


Figure 11. Feeder level network layout-Feeder service areas and substation area served by separate Olt

3.2 PHASE TWO: TECHNICAL ANALYSIS AND EVALUATION.

The technical analysis and evaluation specifically focused on IEC 61850 functionalities and communication protocols as they relate to real-time asset management and accelerated Protection, Automation, and Control (PAC). To contextualize this, a communication network topology for Medium Voltage (MV) distribution was designed for the case study area.

This logical topology was digitally overlayed onto the existing physical fiber infrastructure to model the real-world application of IEC 61850 services accurately.

The initial physical analysis focused heavily on the measured parameters of a single baseline fiber route (the Wandegeya link), the resulting performance metrics were extrapolated across the broader proposed topology. This analytical extrapolation was conducted to justify and validate the network's overall capacity to support rigorous IEC 61850 services on a national, multi-substation scale.

3.2.1 Baseline Analysis
PRELIMINARY OPTICAL LINK POWER AND LATENCY BUDGET

To establish a robust baseline, the link budget utilizes 1310 nm upstream attenuation as the limiting factor. This wavelength experiences significantly higher loss than the 1490 nm or 1550 nm downstream channels, making it the critical variable for worst-case performance analysis.

1) A shared passive mode utilizing VLAN and Priority Tagging.

The proposed network utilizes a shared passive mode with VLAN and Priority Tagging to manage traffic across the Grid Feeder network. For this logical mapping to function, the physical optical path must meet strict power requirements. The calculations below detail the transition from the +2.0 dBm launch power at the OLT to the -28.0 dBm sensitivity threshold required at the IED (Intelligent Electronic Device)

To ensure the reliability of the shared passive architecture, this section establishes the physical layer feasibility through a rigorous optical power budget analysis. By validating the link against ITU-T G.984.2 standards, confirmation that the infrastructure can support the VLAN-tagged data flow across a total reach of 29.6 km while maintaining a standards-compliant Class C+ transceiver classification is achieved.

Table 4. physical layer feasibility test parameters.

Parameter	Value (Typical)	Description
Launch Power (P_{TX})	+2.0 dBm (ITU-T G.984.2 for GPON)	Minimum average launch power at OLT
Receiver Sensitivity (P_{RX})	-28.0 dBm	Minimum power required at IED for 10^{-12} BER
Operating Wavelength	1490 nm	Standard downstream wavelength
Fiber Type	G.652	Standard Single-Mode Fiber (SMF)

Power budget calculation

The total available power budget (P_B) is derived from the difference between the transmitter's launch power (P_{TX}) and the receiver's sensitivity threshold (P_{RX})

$P_B = P_{TX} - P_{RX}$

$= 2\ dBm - (-28dBm)$

$= 30\ dB$

Link Loss Estimate

Feeder Fiber: 24.6 km.

Branch Fiber: 5.0 km.

Total Reach: 29.6 km.

Splitter Configuration: 1:8 optical splitter.

Estimated Total Fiber Distance: 29.6 km

Fiber Attenuation:

Assumption: 0.35 dB/km.

(ITU-T G.652.D. The standard specifies a maximum attenuation of 0.4 dB/km at 1310 nm, but mandates that typical cabling for ODN engineering should use 0.35 dB/km for accurate worst-case power budgeting.)

29.6 km × 0.35 dB = 10.36 dB.

Fiber Attenuation = 10.36 dB

Splitter Insertion Loss (1:8):

Assumption: 10.5 dB maximum loss for a 1x8 Planar Lightwave Circuit (PLC) splitter.

(ITU-T G.671 (Transmission characteristics of optical components and subsystems). The standard explicitly caps the maximum allowable insertion loss for a 1:8 passive optical splitter at 10.5 dB across all operating wavelengths and temperatures.)

Splitter Insertion Loss (1:8) = 10.5 dB

Connector Loss:

Assumption*:* 4 mated pairs (OLT port, Splitter In, Splitter Out, ONU port) at 0.75 dB per pair.

(TIA/EIA-568.3-D (Optical Fiber Cabling Components Standard). This standard specifies that the maximum allowable loss per mated optical connector pair is 0.75 dB. While field technicians often achieve approx. 0.3 dB, strict engineering budgets must use the 0.75 dB standard maximum to guarantee intermate-ability performance over time.)

Connector Loss = 3.0 dB

Splice Loss:

Assumption: 15 fusion splices (roughly 1 every 2 km of cable run) at 0.1 dB per splice.

*(*TIA/EIA-568.3-D and ITU-T G.671 set the absolute maximum fusion splice loss at 0.3 dB. However, standard ODN engineering guidelines (and modern fusion splicers) dictate a typical design allowance of 0.1 dB per splice.)

Splice Loss = 1.5 dB

System / Maintenance Margin:

Assumption*:* 3.0 dB reserved power margin.

(ITU-T G.984.2 (Gigabit-capable passive optical networks: Physical Media Dependent layer specification). The standard formally recommends a 3.0 dB optical path penalty/maintenance margin to account for component aging, temperature fluctuations, and future emergency fiber splice repairs.)

Maintenance Margin = 3.0 dB

Total Worst-Case Link Loss:

10.36 + 10.5 + 3.0 + 1.5 + 3.0 = 28.36 dB

Optical Power Margin = 30 dB – 28.36 dB

= 1.64 dB

Transceiver Classification (ITU-T G.984.2)

Evaluating the standardized link loss of 28.36 dB against ITU-T GPON transceiver classes:

Class C+ (32 dB Budget):

PASS. ITU-T G.984.2 Amendment 2 defines Class C+ optics with a 32 dB maximum budget. This is the mandatory requirement for the Grid Feeder network to maintain standards-compliant operation.

The 1.64 dB margin, while narrow, is sufficient for Class C+ operation, ensuring that latency-sensitive VLAN traffic is not compromised by Physical Layer signal degradation (bit error rates exceeding 10^{-12})

2)A dedicated fiber strand with an OLT at the substation.

This configuration involves a direct, unshared fiber strand connecting the Optical Line Terminal (OLT) at the substation to the Optical Network Unit (ONU) or Intelligent Electronic Device (IED).

Because this is a dedicated strand, the 'Shared Mode' overhead is removed. In the context of IEC 61850 requirements, this physical layer robustness ensures that time-critical GOOSE packets are not subject to re-transmission delays caused by marginal signal-to-noise ratios (SNR).

The selection of a dedicated fiber path serves as a 'high-availability' alternative for the Grid Feeder network. With a calculated link loss well below the Class B+ and C+ thresholds, this configuration ensures that even under severe environmental stress or multiple emergency repairs, the optical budget remains firmly within operational limits.

Feeder Fiber: 24.6 km.

Branch Fiber: 5.0 km.

Total Reach: 29.6 km.

Estimated Total Fiber Distance: 29.6 km

Fiber Attenuation:

Assumption*:* 0.35 dB/km.

(ITU-T G.652.D. The standard specifies a maximum attenuation of 0.4 dB/km at 1310 nm, but mandates that typical cabling for ODN engineering should use 0.35 dB/km for accurate worst-case power budgeting.)

29.6 km × 0.35 dB = 10.36 dB.

Fiber Attenuation = 10.36 dB

Connector Loss:

Assumption: 4 mated pairs (OLT port, ONU port) at 0.75 dB per pair.

(TIA/EIA-568.3-D (Optical Fiber Cabling Components Standard). This standard specifies that the maximum allowable loss per mated optical connector pair is 0.75 dB. While field technicians often achieve approx. 0.3 dB, strict engineering budgets must use the 0.75 dB standard maximum to guarantee intermate-ability performance over time.)

Connector Loss = 1.5 dB

Splice Loss:

Assumption: 15 fusion splices (roughly 1 every 2 km of cable run) at 0.1 dB per splice.

*(*TIA/EIA-568.3-D and ITU-T G.671 set the absolute maximum fusion splice loss at 0.3 dB. However, standard ODN engineering guidelines (and modern fusion splicers) dictate a typical design allowance of 0.1 dB per splice.)

Splice Loss = 1.5 dB

System / Maintenance Margin:

Assumption: 3.0 dB reserved power margin.

(ITU-T G.984.2 (Gigabit-capable passive optical networks: Physical Media Dependent layer specification). The standard formally recommends a 3.0 dB optical path penalty/maintenance margin to account for component aging, temperature fluctuations, and future emergency fiber splice repairs.)

Maintenance Margin = 3.0 dB

Total Worst-Case Link Loss:

10.36 + 1.5 + 1.5 + 3.0 = 16.36 dB

Transceiver Recommendations (ITU-T G.984 / G.987)

Standard PON transceivers are classified by their allowable optical loss budgets.

Class B+ (28 dB Budget):

PASS. The calculated loss of 16.36 dB fits within this budget, it leaves over 10 dB of headroom. Even with a Class B+ transceiver, the 11.64 dB margin provides ample protection against common field issues like dirty connectors or emergency fiber repairs, ensuring the link remains operational under sub-optimal conditions.

Class C+ (32 dB Budget):

PASS. This provides an additional 15.64 dB of headroom above the system margin, easily accommodating the 29.6 km reach and ensuring long-term stability for critical SCADA/GOOSE traffic.

3.2.2 Simulation Methodology

Study Focus and Assumptions

The primary objective of this simulation is to evaluate the technical feasibility of applying IEC 61850 communication profiles specifically GOOSE (Generic Object-Oriented Substation Events)

and MMS (Manufacturing Message Specification) over medium and low voltage (MV/LV) distribution networks.

The study assesses how varying optical topologies impact the delivery of time-critical protection signals and high-bandwidth asset management data.

Accelerated Protection Evaluation

The simulation specifically models a Permissive Overreach Transfer Tripping (POTT) scheme. By simulating a fault at the 29.6 km mark, we can measure if the communication delay of the shared passive network adds significant "dead time" to the relay trip logic compared to the dedicated fiber baseline.

Asset Management Convergence

A main focus is "Traffic Convergence." The simulation will stress-test the network by injecting high-bandwidth asset management data (large MMS file transfers or firmware updates) to observe if the shared VLAN architecture can maintain the strict latency requirements for protection signaling without packet loss.

To provide a comprehensive performance benchmark, the simulation models two distinct architectural philosophies:

Scenario A: Dedicated Point-to-Point Fiber

A dedicated, unshared fiber strand directly connecting the Substation OLT to the field IED.this will establish a "Gold Standard" baseline for latency and reliability, representing a zero-contention environment.

Scenario B: Shared Passive Optical Network (GPON) with VLAN/QoS

A shared-medium approach utilizing 1:8 optical splitters, leveraging VLAN Tagging and Priority Tagging (IEEE 802.1p). This will aid to evaluate the impact of traffic contention, queuing delays, and encapsulation overhead on time-sensitive protection packets. Testing whether a cheaper, shared infrastructure (GPON) can actually handle the life-safety, millisecond-accurate requirements of a modern smart grid.

Performance Indicators (KPIs)

1. End-to-End (ETE) Latency: Measuring the "trip time" for GOOSE messages. This is compared against the IEC 61850-5 requirement for Type 1A (P1/P2) messages, which mandates a transfer time of less than 3ms.
2. Packet Jitter: Analyzing the variation in packet delay, which is critical for the synchronization of Sampled Values (SV).

3. VLAN/Priority Efficiency: Assessing how effectively the Class of Service (CoS) mechanisms protect high-priority protection traffic from background asset management (MMS) or SCADA data.

To ensure a high-fidelity representation of the physical layer described in the power budget, the following parameters are integrated into the simulation environment.

Table 5. parameters integrated into the simulation environment.

Parameter	**Value (Standard)**	**Rationale**
Traffic Type 1	IEC 61850 GOOSE	Time-critical protection (High Priority).
Traffic Type 2	IEC 61850 MMS	Asset management/Monitoring (Standard Priority).
Background Load	40% - 60%	Simulates varying levels of network congestion.
Bit Error Rate (BER)	10^{-12}	Standard optical threshold for signal integrity.
Queue Algorithm	Strict Priority (SP)	Ensures GOOSE packets bypass MMS data in Scenario B.

3.2.3 Simulation Environment: OMNET++ AND INET

To ensure high-fidelity, reproducible results, the network model was developed using the OMNeT++ discrete event simulation framework in conjunction with the INET framework. OMNeT++ provides a robust, component-based architecture, while INET supplies deeply validated, hardware-accurate models of the TCP/IP stack, optical fiber links, and Layer 2 Ethernet mechanics. This combination is essential for capturing the complex, microsecond-level interactions required within a converged utility network.

Protocol Accuracy and IEC 61850

The selection of OMNeT++ is heavily supported by recent academic and industrial literature, which has validated its specialized modules for handling IEC 61850 traffic over Ethernet. Because smart grid automation relies on time-critical protocols specifically GOOSE (Generic Object-Oriented Substation Event) messages and high-frequency Sampled Values (SV) the simulator must accurately process strict timing constraints and hardware-level clock synchronization mechanisms, such as IEEE 802.1AS (gPTP).

Advanced Modeling Capabilities Operating a smart grid over a shared Passive Optical Network (PON) introduces significant shared-medium risks. OMNeT++ and INET allow for the explicit, granular modeling of these variables, providing a realistic assessment of grid stability under stress.

1) Bursty ISP Traffic: The framework accurately simulates the erratic, high-volume nature of public broadband traffic competing for the same optical bandwidth.

2) Network Degradation: It tracks microsecond-level queuing delays, buffer overflows, and packet loss during phased network saturation events.
3) QoS Enforcement: It simulates IEEE 802.1p/Q VLAN tagging and strict Priority Queuing at the switch and MAC layer, proving whether critical grid protection data can successfully preempt commercial internet traffic.

OMNeT++ Performance Modeling

To move beyond theoretical capacity, the network proposals were subjected to rigorous digital testing. Robust mathematical models defining data flow, queuing behavior, and network performance were simulated utilizing the OMNeT++ network simulation framework.

These comprehensive simulations were critical in assessing three primary metrics:

Interoperability: Verifying smooth logical communication between diverse node types, SCADA gateways, and edge Intelligent Electronic Devices (IEDs).

Reliability: Ensuring the mesh and shared GPON architectures could sustain traffic during peak municipal loads without dropping critical protection packets.

Response Times: Benchmarking end-to-end latency to ensure deterministic GOOSE and Sampled Values (SV) messaging remains well within the strict sub-3-millisecond thresholds required for grid safety.

3.2.4 Network Architecture and Physical Layer Modeling

A shared passive mode utilizing VLAN and Priority Tagging

This scenario models a highly integrated environment where the utility's communication needs are met via a shared Passive Optical Network (PON), carrying both critical Smart Grid (SG) traffic and standard Internet Service Provider (ISP) residential data.

The simulation environment is built upon the INET Framework, specifically tailored to evaluate the "Coexistence Performance" of mission-critical protection traffic and best-effort consumer data

Traffic Convergence and Encapsulation

To maintain security and operational integrity, a virtualized approach is modeled:

Logical Isolation

Critical grid traffic (IEC 61850) and public broadband traffic are partitioned using Virtual Local Area Networks (VLANs).

Priority Tagging

Traffic is classified via IEEE 802.1p Class of Service (CoS) markings to ensure the Optical Line Terminal (OLT) prioritizes protection packets over best-effort residential data.

The QoS Saturation Stress Test

The primary objective of this simulation is to perform a rigorous Quality of Service (QoS) stress test. This is to evaluate the resilience of three critical IEC 61850 traffic profiles:

GOOSE (Generic Object-Oriented Substation Events). High-speed, mission-critical protection signals.

SV (Sampled Values). Real-time digitized waveforms requiring strict synchronization.

MMS (Manufacturing Message Specification). Monitoring and asset management data.

The simulation measures whether these packets can meet their required arrival deadlines when the residential portion of the network experiences a broadband usage spike (e.g., peak-hour streaming or high-volume downloads) that pushes the aggregate link to saturation.

Congestion Modeling

Unlike a dedicated link, a shared PON is subject to the "noisy neighbor" effect. We model the residential load using a Poisson distribution to simulate unpredictable traffic bursts, allowing the identification of the exact saturation point at which the grid's protection-tripping signals begin to experience jitter or drop-outs.

Hierarchical Network Topology

The model utilizes a Hierarchical Star/Tree Topology, mimicking a standard Passive Optical Network (PON) deployment used in Fiber-to-the-x (FTTx) architectures.

Core Tier (The Substation):

A high-capacity backbone where the SCADA Server and ISP Core converge at the Optical Line Terminal (OLT). These connections utilize the StationBus channel to ensure internal substation latency remains negligible (0.1microsec).

Distribution Tier (The Feeder):

The OLT distributes signals across a 24.6 km Feeder Fiber link. This stage represents the primary transit path where signal propagation delay becomes a factor in GOOSE message timing.

Access Tier (The Last Mile):

Signal splitting occurs at 10 Optical Splitters, which fan out via Branch Fiber to a heterogeneous mix of end-nodes, including Intelligent Electronic Devices (IEDs) and high-bandwidth residential consumers.

Channel Definitions (NED Modeling)

To ensure the simulation honors the physics of the optical link, the following channel parameters are enforced

Table 6. channel parameters are enforced in the simulation

Channel Type	Data Rate	Propagation Delay	Physical Representation
Station Bus	10 Gbps	0.1μs	Ultra-low latency internal substation switching.
Feeder Fiber	1 Gbps	123/246μs	24.6 km long-haul backbone.
Branch Fiber	1 Gbps	25μs	Local drop cables to IEDs and residential premises.

Submodule and Node Configuration

The network populates the topology with specialized submodules to simulate a "Live" grid environment:

Grid Infrastructure (Critical):

20 IEDs programmed to generate bursty GOOSE traffic during fault simulations and steady-state MMS telemetry.

Residential Load (Background):

20 Residential Nodes, each representing a cluster of three independent users. These nodes generate stochastic "Best Effort" traffic (video streaming, web browsing) to stress the OLT's queuing logic.

Municipal Sinks:

5 Sinks aggregate the high-volume data flows from public services, acting as a constant background noise on the shared medium.

Multi-Service Convergence

This model validates the industry shift toward Universal Access Networks. By using a single fiber backbone to deliver both Smart Grid telemetry and residential broadband, utilities can achieve significant cost-sharing. However, this simulation specifically tests the Priority Queuing (Strict Priority) required to prevent a residential 4K video stream from delaying a critical circuit breaker trip signal.

Traffic Differentiation

Within the NED file, the StandardHost modules for IEDs are configured with specialized application layers. Unlike the residential nodes, which use standard TCP/UDP, the IEDs utilize a Raw Ethernet encapsulation for GOOSE, bypassing the IP layer to minimize processing overhead exactly as defined in the IEC 61850-8-1 mapping.

Total Reach Validation

With a Total Reach of 29.6 km, the combined propagation delay across the Feeder and Branch fibers is approximately 148 microsec. This simulation will determine how much additional "queuing delay" is introduced by the OLT when the residential nodes saturate the 1Gbps link, and if that total delay exceeds the 3ms protection limit.

Physical Component Representation on The Network

The methodology assigns specific INET modules to represent the various physical components of a power system and telecommunications network. Each choice dictates the network layers the device can process and how it handles traffic.

SCADA Unit: StandardHost

In the NED file, the SCADA unit is a StandardHost.

It acts as the "brain" of the power system, functioning as an MMS Client.

Logic: A StandardHost in INET contains a full TCP/IP stack. This is necessary because SCADA systems must manage multiple application-layer connections simultaneously. In the configuration, 62 applications are assigned to this host, allowing it to poll 20 different IEDs (MMS traffic) while simultaneously acting as a sink for critical SV and GOOSE data.

Substation Gateway: EthernetSwitch

The gateway is modeled as a Layer 2 switch rather than a router.

It represents the Access Point between the high-voltage substation and feeder environment and the optical backbone.

Logic:

Using a switch with **hasVlanConfig = true**, implements a security boundary. In a real smart grid, the gateway uses VLAN filtering to ensure that time-critical GOOSE messages stay within the feeder "process bus" and don't leak out into the residential ISP network, which would cause unnecessary congestion.

IEDs (Intelligent Electronic Devices): StandardHost

Though IEDs are specialized hardware (relays or merging units), they are modeled as StandardHost.

These are the Data Producers. They monitor the physical grid and generate the three-phase fault data.

Logic:

Using StandardHost allows for the modeling of complex multi-traffic nature of IEC 61850. A single IED must simultaneously handle:

SV (Sampled Values): High-frequency periodic traffic.

GOOSE: Event-driven, low-latency bursts.

MMS: Point-to-point reporting to the SCADA.

OLT (Optical Line Terminal): EthernetSwitch

Choosing a switch assumes that the OLT handles all arbitration. In real-world fiber (GPON/EPON), the OLT uses a complex TDMA (Time Division Multiple Access) scheme to tell each house when it is allowed to "talk." Using a standard Ethernet switch assumes that standard Ethernet collision/flow control is an "accurate enough" proxy for this complex timing logic.

The OLT is the central hub of your optical distribution network.

It acts as the Converged Core. It is the point where high-priority grid data meets low-priority public internet data.

Logic:

The OLT is the most critical point for the QoS (Quality of Service) logic. Because it is an EthernetSwitch with a PriorityQueue, it acts as the "traffic warden." When a GOOSE "Trip" event occurs at 90s, the OLT logic ensures those packets jump to the front of the line, even if resUsers are saturating the 1Gbps link with background traffic.

ResUsers and Municipal Sinks: Standard Host

The residential users (laptops) and sinks (servers) represent the Background Noise of the network.

They provide the Cross-Traffic Load.

Logic:

resUsers: These are modeled as UDP sources sending to the isp_core. Their exponential send interval creates "bursty" traffic that tests the resilience of the IED communication.

Municipal Sinks: These represent heavy data consumers (like city surveillance or public Wi-Fi hubs) that provide a steady, high-volume "mathematical load" on the fiber feeder.

The Client-Server Relationship

In this simulation, the SCADA unit acts as the MMS Client and the IEDs act as MMS Servers.

The Logic:

Configured ***.scada.numApps = 62**. Out of these, 60 applications (app[0..59]) are dedicated to polling. Since there are 20 IEDs, each IED is being polled by 3 separate application instances on the SCADA host (60 apps / 20 IEDs). This creates a heavy, concurrent polling environment.

The Polling Mechanism (Request/Response)

Simulation implementation uses the following parameters to simulate the MMS "Read" or "Reporting" service:

Port 102: This is the industry-standard port for ISO-TSAP/MMS communication.

Message Length (128B): This represents a standard MMS "Information Report" or "Read Response" containing status values (like breaker position or measurement attributes).

Send Interval (50ms): This is a high-frequency poll. The SCADA sends a request/command every 50ms to every IED.

Traffic Flow: Unlike the GOOSE packets that stay mostly on the feeder bus, these MMS packets must traverse the entire length of the Feeder Fiber (24.6km), incurring a round-trip propagation delay of approximately 246 microsec plus switching latency at the OLT.

Traffic Prioritization (ToS 46)

Even though MMS is often considered less critical than GOOSE in real-world standards (often assigned a lower priority), its assigned tos = 46.

By giving MMS the same "Expedited Forwarding" tag as the GOOSE and SV traffic, ensuress that the SCADA's polling requests do not get dropped during periods of high ISP congestion.

This creates an interesting scenario at the OLT. During the 90s Trip event, the OLT must simultaneously manage:

1. Downstream MMS Polls (SCADA to IED).
2. Upstream GOOSE Bursts (IED to IEDs, SCADA).
3. Upstream/Downstream ISP traffic.

PACKAGE NETWORK DESCRIPTION FILE

This defines the topology of the network.

SHARED GPON

Figure 12. Shared GPON package network description file.

```
package goosepriority7;

@license(LGPL);

import inet.node.inet.StandardHost;
import inet.node.ethernet.EthernetSwitch;
import inet.networklayer.configurator.ipv4.Ipv4NetworkConfigurator;
import inet.visualizer.contract.IIntegratedVisualizer;
import ned.DatarateChannel;

network GridFeeder
{
    parameters:
        @display("bgb=5712,3497");

    types:
        channel FeederFiber extends DatarateChannel
        {
            delay = 246us; // Updated for 24.6km run (approx 5us per km)
            datarate = 1Gbps;
            @display("ls=gray,3");
        }
```

```
    channel BranchFiber extends DatarateChannel
    {
        delay = 25us;
        datarate = 1Gbps;
        @display("ls=cyan,1");
    }
    channel StationBus extends DatarateChannel
    {
        delay = 0.1us;
        datarate = 10Gbps;
        @display("ls=black,4");
    }

submodules:
    visualizer: <default("IntegratedCanvasVisualizer")> like IIntegratedVisualizer {
        @display("p=100,50");
    }
    configurator: Ipv4NetworkConfigurator {
        @display("p=250,50");
    }

    // --- CORE INFRASTRUCTURE ---
    scada: StandardHost {
        @display("p=161,385;i=device/pc");
    }
    substation_gateway: EthernetSwitch {
        @display("p=168,848;i=device/router");
    }
```

```
    olt: EthernetSwitch {
        @display("p=1002,778;i=device/switch,vl");
    }

    isp_core: StandardHost {
        @display("p=995,112;i=device/server");
    }

    // --- 10 INDEPENDENT SPLITTERS (Switches acting as Hubs) ---
    // Using EthernetSwitch instead of EthernetHub to avoid CSMA/CD upstream collisions,
    // but they will be configured in omnetpp.ini to broadcast like passive splitters.
    splitter1: EthernetSwitch { @display("p=519,1437;i=device/hub"); }
    splitter2: EthernetSwitch { @display("p=1850,1815;i=device/hub"); }
    splitter3: EthernetSwitch { @display("p=2299,2313;i=device/hub"); }
    splitter4: EthernetSwitch { @display("p=3098,3238;i=device/hub"); }
    splitter5: EthernetSwitch { @display("p=1857,785;i=device/hub"); }
    splitter6: EthernetSwitch { @display("p=3189,701;i=device/hub"); }
    splitter7: EthernetSwitch { @display("p=3946,687;i=device/hub;is=s"); }
    splitter8: EthernetSwitch { @display("p=4471,701;i=device/hub"); }
    splitter9: EthernetSwitch { @display("p=5018,701;i=device/hub"); }
    splitter10: EthernetSwitch { @display("p=5550,701;i=device/hub"); }

    // --- 20 IEC 61850 IEDs ---
    ied1: StandardHost { @display("p=245,1815;i=device/smallrouter"); }
    ied2: StandardHost { @display("p=161,1430;i=device/smallrouter"); }
    ied3: StandardHost { @display("p=2572,1801;i=device/smallrouter"); }
    ied4: StandardHost { @display("p=2172,1822;i=device/smallrouter"); }
```

```
ied5: StandardHost { @display("p=2845,2481;i=device/smallrouter"); }
ied6: StandardHost { @display("p=3462,2397;i=device/smallrouter"); }
ied7: StandardHost { @display("p=3798,3189;i=device/smallrouter"); }
ied8: StandardHost { @display("p=1787,3231;i=device/smallrouter"); }
ied9: StandardHost { @display("p=2411,1121;i=device/smallrouter"); }
ied10: StandardHost { @display("p=2299,378;i=device/smallrouter"); }
ied11: StandardHost { @display("p=3224,463;i=device/smallrouter"); }
ied12: StandardHost { @display("p=3189,974;i=device/smallrouter"); }
ied13: StandardHost { @display("p=3946,981;i=device/smallrouter"); }
ied14: StandardHost { @display("p=3946,463;i=device/smallrouter"); }
ied15: StandardHost { @display("p=4492,463;i=device/smallrouter"); }
ied16: StandardHost { @display("p=4485,1037;i=device/smallrouter"); }
ied17: StandardHost { @display("p=5018,1794;i=device/smallrouter"); }
ied18: StandardHost { @display("p=5018,112;i=device/smallrouter"); }
ied19: StandardHost { @display("p=5543,463;i=device/smallrouter"); }
ied20: StandardHost { @display("p=5543,2215;i=device/smallrouter"); }

// --- 20 RESIDENTIAL USERS ---
resUser1: StandardHost { @display("p=519,981;i=device/laptop"); }
resUser2: StandardHost { @display("p=519,2404;i=device/laptop"); }
resUser3: StandardHost { @display("p=1451,1829;i=device/laptop"); }
resUser4: StandardHost { @display("p=1850,1528;i=device/laptop"); }
resUser5: StandardHost { @display("p=1780,2558;i=device/laptop"); }
resUser6: StandardHost { @display("p=2116,2558;i=device/laptop"); }
resUser7: StandardHost { @display("p=4913,3147;i=device/laptop"); }
resUser8: StandardHost { @display("p=4275,3147;i=device/laptop"); }
resUser9: StandardHost { @display("p=1850,105;i=device/laptop"); }
resUser10: StandardHost { @display("p=1843,1163;i=device/laptop"); }
```

```
    resUser11: StandardHost { @display("p=3189,1247;i=device/laptop"); }
    resUser12: StandardHost { @display("p=3189,112;i=device/laptop"); }
    resUser13: StandardHost { @display("p=3946,1437;i=device/laptop"); }
    resUser14: StandardHost { @display("p=3946,147;i=device/laptop"); }
    resUser15: StandardHost { @display("p=4506,182;i=device/laptop"); }
    resUser16: StandardHost { @display("p=4464,1289;i=device/laptop"); }
    resUser17: StandardHost { @display("p=5018,1437;i=device/laptop"); }
    resUser18: StandardHost { @display("p=5018,1051;i=device/laptop"); }
    resUser19: StandardHost { @display("p=5543,1296;i=device/laptop"); }
    resUser20: StandardHost { @display("p=5501,175;i=device/laptop"); }

    // --- 5 MUNICIPAL SINKS ---
    sink1: StandardHost { @display("p=1850,2130;i=device/server2"); }
    sink2: StandardHost { @display("p=2411,3238;i=device/server2"); }
    sink3: StandardHost { @display("p=3189,1591;i=device/server2"); }
    sink4: StandardHost { @display("p=4499,1738;i=device/server2"); }
    sink5: StandardHost { @display("p=5543,1864;i=device/server2"); }

connections:
    scada.ethg++ <--> StationBus <--> substation_gateway.ethg++;
    substation_gateway.ethg++ <--> StationBus <--> olt.ethg++;
    isp_core.ethg++ <--> StationBus <--> olt.ethg++;

    // Backbone to 10 Splitters
    olt.ethg++ <--> FeederFiber <--> splitter1.ethg++;
    olt.ethg++ <--> FeederFiber <--> splitter2.ethg++;
    olt.ethg++ <--> FeederFiber <--> splitter3.ethg++;
    olt.ethg++ <--> FeederFiber <--> splitter4.ethg++;
```

```
olt.ethg++ <--> FeederFiber <--> splitter5.ethg++;
olt.ethg++ <--> FeederFiber <--> splitter6.ethg++;
olt.ethg++ <--> FeederFiber <--> splitter7.ethg++;
olt.ethg++ <--> FeederFiber <--> splitter8.ethg++;
olt.ethg++ <--> FeederFiber <--> splitter9.ethg++;
olt.ethg++ <--> FeederFiber <--> splitter10.ethg++;

// IEDs to Splitters
ied1.ethg++ <--> BranchFiber <--> splitter1.ethg++;
ied2.ethg++ <--> BranchFiber <--> splitter1.ethg++;
ied3.ethg++ <--> BranchFiber <--> splitter2.ethg++;
ied4.ethg++ <--> BranchFiber <--> splitter2.ethg++;
ied5.ethg++ <--> BranchFiber <--> splitter3.ethg++;
ied6.ethg++ <--> BranchFiber <--> splitter3.ethg++;
ied7.ethg++ <--> BranchFiber <--> splitter4.ethg++;
ied8.ethg++ <--> BranchFiber <--> splitter4.ethg++;
ied9.ethg++ <--> BranchFiber <--> splitter5.ethg++;
ied10.ethg++ <--> BranchFiber <--> splitter5.ethg++;
ied11.ethg++ <--> BranchFiber <--> splitter6.ethg++;
ied12.ethg++ <--> BranchFiber <--> splitter6.ethg++;
ied13.ethg++ <--> BranchFiber <--> splitter7.ethg++;
ied14.ethg++ <--> BranchFiber <--> splitter7.ethg++;
ied15.ethg++ <--> BranchFiber <--> splitter8.ethg++;
ied16.ethg++ <--> BranchFiber <--> splitter8.ethg++;
ied17.ethg++ <--> BranchFiber <--> splitter9.ethg++;
ied18.ethg++ <--> BranchFiber <--> splitter9.ethg++;
ied19.ethg++ <--> BranchFiber <--> splitter10.ethg++;
ied20.ethg++ <--> BranchFiber <--> splitter10.ethg++;
```

```
// ResUsers to Splitters
resUser1.ethg++ <--> BranchFiber <--> splitter1.ethg++;
resUser2.ethg++ <--> BranchFiber <--> splitter1.ethg++;
resUser3.ethg++ <--> BranchFiber <--> splitter2.ethg++;
resUser4.ethg++ <--> BranchFiber <--> splitter2.ethg++;
resUser5.ethg++ <--> BranchFiber <--> splitter3.ethg++;
resUser6.ethg++ <--> BranchFiber <--> splitter3.ethg++;
resUser7.ethg++ <--> BranchFiber <--> splitter4.ethg++;
resUser8.ethg++ <--> BranchFiber <--> splitter4.ethg++;
resUser9.ethg++ <--> BranchFiber <--> splitter5.ethg++;
resUser10.ethg++ <--> BranchFiber <--> splitter5.ethg++;
resUser11.ethg++ <--> BranchFiber <--> splitter6.ethg++;
resUser12.ethg++ <--> BranchFiber <--> splitter6.ethg++;
resUser13.ethg++ <--> BranchFiber <--> splitter7.ethg++;
resUser14.ethg++ <--> BranchFiber <--> splitter7.ethg++;
resUser15.ethg++ <--> BranchFiber <--> splitter8.ethg++;
resUser16.ethg++ <--> BranchFiber <--> splitter8.ethg++;
resUser17.ethg++ <--> BranchFiber <--> splitter9.ethg++;
resUser18.ethg++ <--> BranchFiber <--> splitter9.ethg++;
resUser19.ethg++ <--> BranchFiber <--> splitter10.ethg++;
resUser20.ethg++ <--> BranchFiber <--> splitter10.ethg++;

// Sinks to Splitters
sink1.ethg++ <--> BranchFiber <--> splitter2.ethg++;
sink2.ethg++ <--> BranchFiber <--> splitter4.ethg++;
sink3.ethg++ <--> BranchFiber <--> splitter6.ethg++;
sink4.ethg++ <--> BranchFiber <--> splitter8.ethg++;
```

```
        sink5.ethg++ <--> BranchFiber <--> splitter10.ethg++;
}
```

Network portion topological view showing display of IEDs on the fiber network

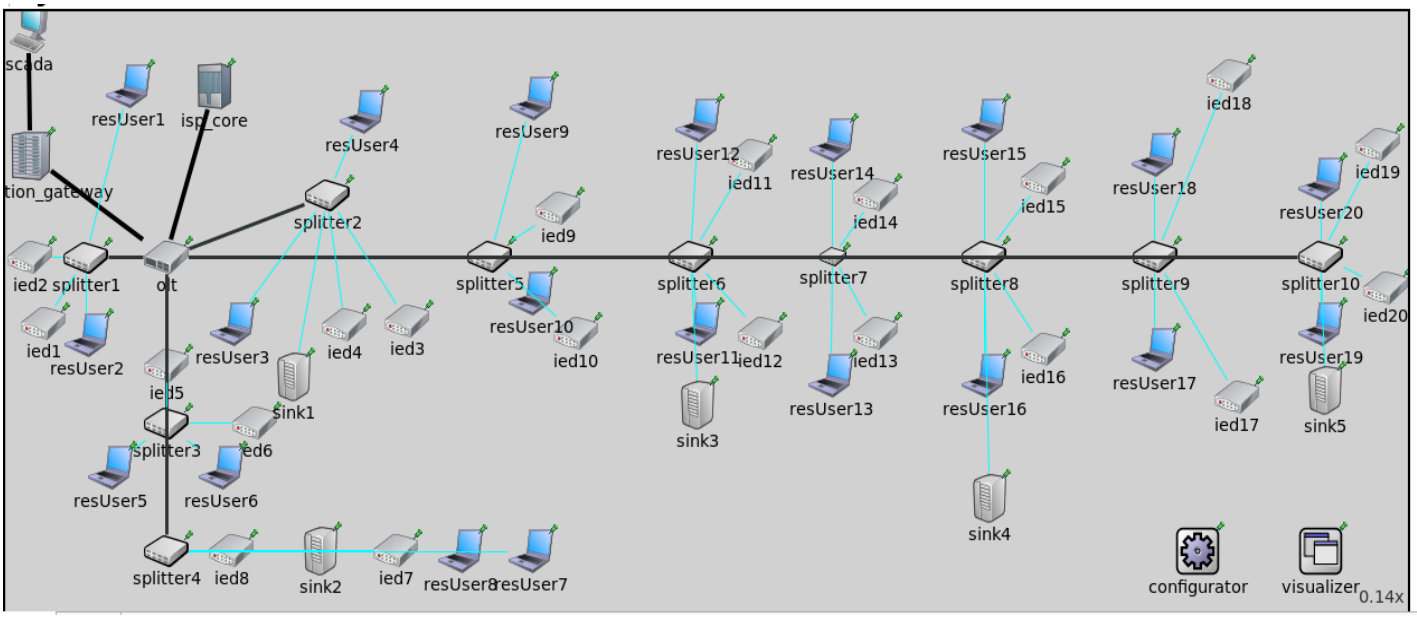


Figure 13. Network portion topological view showing display of IEDs on the fiber network

Dedicated Architecture

The network simulates a centralized, star-topology communication architecture typical of modern electrical grids, specifically designed to test timing, synchronization, and latency over long distances.

File sets up a simulation to test how well a SCADA system and a Grandmaster clock can communicate with and synchronize 20 remote power grid sensors over a dedicated 24.6km Gigabit fiber-optic network.

Central Control Hub:

SCADA Host: The master control and monitoring server.

Grandmaster Clock: A high-precision SettableClock serving as the network's time authority.

Substation Gateway: A high-speed EthernetSwitch connecting the control hub to the field.

Field Infrastructure:

OLT (Optical Line Terminal): The distribution switch for the feeder network.

20 IEDs (Intelligent Electronic Devices): Distributed sensors/relays acting as endpoints.

Communication Links:

10 Gbps Backbone: High-bandwidth fiber connecting SCADA, the Grandmaster, and the Gateway.

24.6km Distribution Fiber: Custom 1 Gbps channels (Fiber24km) connecting the OLT to every IED, introducing a fixed physical propagation delay.

DEDICATED

***Figure 14. Dedicated fiber* package network description file.**

```
package aassetmgtdedicated;
@license(LGPL);

import inet.node.ethernet.EthernetSwitch;
import inet.node.inet.StandardHost;
import inet.networklayer.configurator.ipv4.Ipv4NetworkConfigurator;
import inet.node.ethernet.Eth1G;
import inet.node.ethernet.Eth10G;

network SmartGridFeeder
{
    parameters:
        @display("bgb=5423,2431");

    types:
        // Custom channel to model the physical 24.6km fiber run
        channel Fiber24km extends Eth1G
        {
            parameters:
```

```
            length = 24.6km;
        }
    submodules:
        configurator: Ipv4NetworkConfigurator {
            @display("p=4977,174");
        }
        // Synchronization Source (Grandmaster Clock)
        grandmaster: StandardHost {
            @display("p=446,156;i=device/clock");
        }
        scada: StandardHost {
            @display("p=1372,174;i=device/pc");
        }
        substation_gateway: EthernetSwitch {
            @display("p=967,289;i=device/router");
        }
        olt: EthernetSwitch {
            @display("p=967,828;i=device/switch");
        }

        // --- 20 Independent IED Definitions ---
        ied1: StandardHost {
            @display("p=967,2026;i=device/smallrouter");
        }
        ied2: StandardHost {
            @display("p=4624,2026;i=device/smallrouter");
        }
        ied3: StandardHost {
```

```
    @display("p=4456,833;i=device/smallrouter");
}
ied4: StandardHost {
    @display("p=967,2338;i=device/smallrouter");
}
ied5: StandardHost {
    @display("p=145,689;i=device/smallrouter");
}
ied6: StandardHost {
    @display("p=150,990;i=device/smallrouter");
}
ied7: StandardHost {
    @display("p=3062,828;i=device/smallrouter");
}
ied8: StandardHost {
    @display("p=967,1678;i=device/smallrouter");
}
ied9: StandardHost {
    @display("p=2709,828;i=device/smallrouter");
}
ied10: StandardHost {
    @display("p=5145,2193;i=device/smallrouter");
}
ied11: StandardHost {
    @display("p=967,1383;i=device/smallrouter");
}
ied12: StandardHost {
    @display("p=2483,1343;i=device/smallrouter");
```

```
    }
    ied13: StandardHost {
        @display("p=3606,1684;i=device/smallrouter");
    }
    ied14: StandardHost {
        @display("p=2315,828;i=device/smallrouter");
    }
    ied15: StandardHost {
        @display("p=5261,862;i=device/smallrouter");
    }
    ied16: StandardHost {
        @display("p=4109,1875;i=device/smallrouter");
    }
    ied17: StandardHost {
        @display("p=3062,1539;i=device/smallrouter");
    }
    ied18: StandardHost {
        @display("p=3554,828;i=device/smallrouter");
    }
    ied19: StandardHost {
        @display("p=4057,828;i=device/smallrouter");
    }
    ied20: StandardHost {
        @display("p=4914,857;i=device/smallrouter");
    }

connections:
    // Connect Grandmaster to Backbone
```

```
    grandmaster.ethg++ <--> Eth10G <--> substation_gateway.ethg++;

    // 10 Gbps Backbone
    scada.ethg++ <--> Eth10G <--> substation_gateway.ethg++;
    substation_gateway.ethg++ <--> Eth10G <--> olt.ethg++;

    // 1 Gbps Field Connections (24.6km Long Run)
    olt.ethg++ <--> Fiber24km <--> ied1.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied2.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied3.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied4.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied5.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied6.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied7.ethg++;
    olt.ethg++ <--> Fiber24hkm <--> ied8.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied9.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied10.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied11.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied12.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied13.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied14.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied15.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied16.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied17.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied18.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied19.ethg++;
    olt.ethg++ <--> Fiber24km <--> ied20.ethg++;
}
```

Network portion topological view showing display of IEDs on the fiber network

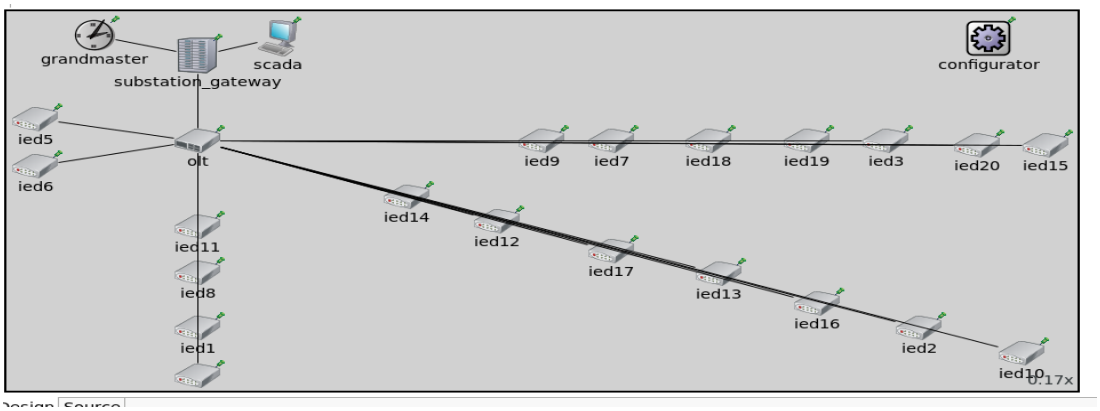


Figure 15. Network portion topological view showing display of IEDs on the fiber network

3.2.5 Logic Implementation and Simulation Constraints

General Network Logic

This section details the operational "intelligence" of the simulation. To bridge the gap between a software model and a physical utility grid, several logical constraints and hardware behaviors have been encoded into the omnetpp.ini and .ned configurations.

The simulation logic employs a cross-layer approach, integrating application-layer traffic profiles, network-layer QoS tagging, and data-link layer hardware emulation to stress-test the converged infrastructure.

Smart Grid Traffic Profiling (IEC 61850)

The application layer replicates authentic substation protocols down to the millisecond:

Sampled Values (SV): Configured as 150-byte packets generated continuously at 250microsec intervals. This perfectly maps to the 4,000 Hz digitization rate utilized by hardware Merging Units tracking standard 50 Hz power distribution waves.

GOOSE Steady-State (Heartbeat): Emits routine status signals at a stable 1-second interval to maintain active network heartbeat supervision.

GOOSE Fault Burst: Emulates a severe breaker trip event. When a fault is initiated, the targeted IED transitions from standard heartbeat mode to an intensive burst mode, bombarding the channel with 200-byte packets every 2 ms for a 100 ms window. This stresses the network's blocking probability under emergency conditions.

While physical IEC 61850 MMS data relies on standard TCP to guarantee SCADA commands arrive intact, this simulation implements MMS polling utilizing UDP. This simplification bypasses

TCP handshake and windowing overhead, yielding a highly conservative latency baseline centered purely on raw queue delays and transit limits.

Shared GPON
Modeling Assumptions

To maintain a balance between computational efficiency and engineering accuracy, the following technical assumptions are baked into the simulation code:

Deterministic Latency (Distance = Delay)

Propagation delay is calculated based on the refractive index of silica fiber (approx. 1.468). The simulation maps every kilometer of "real-world" geography to approximately 148.9 microsec of one-way latency. This ensures that the 29.6 km total reach impacts the arrival time of GOOSE messages with mathematical precision.

Symmetric 1Gbps Throughput

While commercial GPON often utilizes asymmetric rates (e.g., 2.4 Gbps down / 1.2 Gbps up), this simulation assumes a symmetric 1Gbps link. This creates a "stricter" bottleneck for upstream protection signals, providing a more conservative (worst-case) assessment of how residential uploads might interfere with grid telemetry.

Quality of Service (QoS) and Traffic Prioritization

The logic centerpiece is the implementation of IEEE 802.1p (Class of Service). Within the .ini configuration, traffic is bifurcated into two distinct streams:

Critical Grid Traffic (Priority 7)

IEC 61850 GOOSE and SV messages are assigned the highest possible priority (Network Control/Critical). The simulation's MAC-layer logic uses Strict Priority (SP) Queuing, ensuring these packets skip to the front of the buffer at the OLT and splitters.

Best-Effort Residential (Priority 0)

Consumer broadband traffic is treated as background noise. When the link reaches saturation, the OLT is programmed to drop or delay Priority 0 packets to preserve the timing of Priority 7 signals.

Stochastic Traffic Injection (The "Noise" Factor)

To simulate realistic "peak-hour" congestion, residential nodes do not send steady data. Instead, they utilize a Poisson Distribution for packet arrival. This introduces "jitter" into the network, testing whether the high-priority grid traffic can maintain a stable Inter-Packet Gap (IPG) even when the background residential traffic is "bursty" and unpredictable.

Burst-Mode Protection Signaling

In the event of a simulated grid fault, the IEDs are programmed to switch from "Heartbeat" mode to "Burst" mode sending a rapid sequence of GOOSE messages. The simulation logic evaluates the Probability of Buffered Blocking, determining if the OLT's hardware buffer is deep enough to handle a simultaneous burst from 20 IEDs during a major grid event without dropping packets.

VLAN Isolation Logic

Beyond simple priority tagging, the logic implements VLAN-based Logical Segmentation. This ensures that even though the physical fiber is shared, the residential "public" network and the utility "private" network exist in separate broadcast domains. This is a critical security add-in, as it prevents potential ARP spoofing or broadcast storms from the residential side from reaching the SCADA core.

BER (Bit Error Rate) Emulation

To align with the Optical Power Budget calculated earlier, a packet error rate (PER) is applied to the channels. This simulates the signal degradation occurring over the 29.6 km run, allowing the observation of how the Forward Error Correction (FEC) in the GPON layer affects total end-to-end latency.

Passive Optical Hardware Emulation

Because the standard INET framework lacks a native, non-intelligent "Optical Splitter" module, an EthernetSwitch was structurally modified to act as a physical splitter. This was achieved by systematically stripping away traditional layer-2 switching intelligence:

Zero Computational Overhead (processingDelay = 0s): Eliminates the standard "store-and-forward" or computational processing lag typical of active switches, accurately mirroring a purely passive physical medium.

Forced Downstream Broadcasting (addressTableTimeout = 0s): Disables the switch's MAC address learning capabilities. This forces the device to behave exactly like a passive optical hub, splitting and broadcasting every downstream frame from the OLT to every connected node.

Infinite Buffering Buffer (packetCapacity = -1): Ensures that the simulated splitter itself never buffers or drops packets due to internal queue limits, forcing all congestion, queue delays, and drops to occur exclusively at the OLT or edge node interfaces.

Stochastic Background Traffic & Peak Load Modeling

To prove if the QoS logic can successfully defend the grid against a severe internet traffic surge, residential and municipal nodes inject background noise using a non-homogeneous Poisson Process.

The intervals are derived from real-world telecom metrics, assuming a standard network MTU payload of 1,450 Bytes and applying the industry rule of thumb that 10% of total daily traffic occurs entirely within a single peak hour.

Residential Traffic Modeling

Derived from a maximum consumption profile of 20 GB per day per user, clustered into 3-user nodes. This outputs a bursty, unpredictable background wave.

$$peak\ hour\ traffic\ = 20\ \times 0.1\ \times 3$$

$$bitrate\ for\ the\ 3\ users = \frac{20\ \times 0.1 \times 3 \times 8000 Mbits}{3600\ seconds}$$

$$total\ Node\ bitrate\ = 13.33\ Mbps$$

Assuming a standard MTU payload 0f 1450 Bytes (translates to 11600 bits)

$$send\ interval = \frac{11600}{13.33 \times 10^6}$$

$$packetsendInterval = 0.85msec$$

Municipal Traffic Modeling

Models high-capacity public endpoints (such as traffic cameras or municipal Wi-Fi hubs) pulling 230 GB per day, applying a heavy, continuous mathematical load across the common fiber assets.

$$peak\ hour\ traffic\ = 230\ \times 0.1$$

$$bitrate\ for\ the\ 3\ users = \frac{230\ \times 0.1 \times 8000 Mbits}{3600\ seconds}$$

$$send\ interval = \frac{11600}{51.11 \times 10^6}$$

$$packetsendInterval = 0.23msec$$

These translate into exponential(0.87ms) and exponential(0.23ms) intervals. This implements a Poisson process, which is the academic standard for simulating the bursty, unpredictable nature of human-generated internet traffic.

Link Utilization Analysis
SCADA Network Traffic Profile

The SCADA master orchestrates two high-density data streams across its application slots, creating a heavy, continuous baseline load on the converged network:

MMS Polling (TcpBasicClientApp): Simulates administrative grid traffic via the Manufacturing Message Specification (MMS). The SCADA server opens concurrent TCP connections on standard port 102 every 50 ms to fetch status logs and administrative data from all 20 field IEDs.

Sampled Values (SV) Exchange (EtherTrafGen): The SCADA system broadcasts raw, digitized voltage and current waveforms every 250 µs. These transmissions utilize Layer-2 broadcast MAC addresses (FFFFFFFFFFFF) to bypass IP routing overhead, constantly saturating the link with high-speed telemetry.

IED Traffic Profile (The IEC 61850 Core)

Each Intelligent Electronic Device (IED) acts as a specialized smart power sensor, simultaneously executing multiple application layers to manage the grid's operational "Process Bus":

MMS Servers (App 0 & 1): Actively listen on TCP ports 102 and 103 to process and rapidly respond to incoming SCADA administrative queries.

Sampled Values (EthApp 0): Streams raw 150-byte measurement packets directly back to the SCADA system at strict 250 µs intervals, mathematically mirroring the behavior of physical merging units.

GOOSE Heartbeat (EthApp 1): Transmits a routine 1-second "keep-alive" Generic Object-Oriented Substation Event (GOOSE) broadcast, providing the SCADA core with constant verification that grid health is nominal.

NETWORK CONFIGURATION FILE

GPON

To effectively route traffic across the converged network, the physical nodes defined in the. ned topology must be assigned logical addresses and routing protocols. In the OMNeT++ environment, this is managed by the IPv4NetworkConfigurator, which parses a central XML file to dynamically build the routing tables for all simulated devices.

Because Scenario B utilizes a shared Passive Optical Network (PON) where a single fiber strand carries both critical grid telemetry and public broadband data, the network relies on Virtual Local Area Networks (VLANs) for strict logical separation. This ensures that while packets share the same physical glass, their broadcast domains remain completely isolated.

The simulation divides the network into two primary segments:

Table 7. Shared Passive Optical Network assigned logical addresses and routing protocols

Network Domain	VLAN ID	Subnet Mask	IP Range Allocation	Traffic Profile
Smart Grid (Critical)	10	/24 (255.255.255.0)	192.168.10.x	Priority 7 (GOOSE, SV, MMS)
Public ISP (Best Effort)	20	/24 (255.255.255.0)	10.0.0.x	Priority 0 (TCP/UDP, HTTP, Video)
Infrastructure Backbone	Native	/16 (255.255.0.0)	192.168.x.x	Core Routing (OLT, Gateway)

To reflect real-world network engineering practices, distinct IPv4 address spaces are allocated to each VLAN. This prevents IP conflicts and allows the Optical Line Terminal (OLT) to apply distinct routing and QoS rules based on subnet origins.

A critical function of this configuration is broadcast containment. GOOSE messages rely heavily on Layer 2 multicast/broadcast mechanisms. By forcing all ied* nodes into VLAN 10, the XML configuration guarantees that a burst of protection signals will not flood the residential modems, and conversely, a residential broadcast storm (e.g., a rogue DHCP server on the public side) cannot penetrate the SCADA network

```
<config>
  <!-- SUBSTATION NETWORK (VLAN 10) -->
  <!-- Priority traffic: SCADA and IEDs -->

  <interface hosts="scada ied*" names="eth*" address="192.168.10.x" netmask="255.255.255.0" vlan="10"/>

  <!-- INFRASTRUCTURE GATEWAYS -->

  <interface hosts="substation_gateway olt" names="eth*" address="192.168.x.x" netmask="255.255.0.0"/>

  <!-- PUBLIC NETWORK (VLAN 20) -->

  <!-- Best Effort traffic: ISP Core, Residential Users, and Municipal Sinks -->

  <interface hosts="isp_core resUser* sink*" names="eth*" address="10.0.0.x" netmask="255.255.255.0" vlan="20"/>
```

```
    <!-- VLAN DEFINITIONS -->

    <vlan-config>

        <vlan id="10" name="Substation"/>

        <vlan id="20" name="Public"/>

    </vlan-config>

    <!-- ROUTING RULES -->

    <!-- Ensure IEDs and SCADA prefer the Substation gateway path -->

    <route hosts="scada ied*" destination="192.168.10.0" netmask="255.255.255.0" interface="eth0"/>

    <!-- Ensure Public nodes stay on the 10.0.0.x subnet -->

    <route hosts="isp_core resUser* sink*" destination="10.0.0.0" netmask="255.255.255.0" interface="eth0"/>

    <!-- Default catch-all route for cross-network communication via OLT -->

    <route hosts="*" destination="*" netmask="*" gateway="*" interface="eth0"/>

</config>
```

Clock Synchronization Analysis

Clock and Time Synchronization (IEEE 802.1AS / gPTP)

In a smart grid environment, phase measurement data is rendered invalid if sensor timestamps are misaligned. To ensure precision time distribution across the 24.6km fiber network, the Generalized Precision Time Protocol (gPTP) is activated (.hasPtp = true) on all nodes.

The Grandmaster Clock: The primary reference node is configured as an ideal clock (driftRate = 0ppm) dictating the master time with zero initial error.

IED Slave Clocks: To accurately simulate real-world hardware variance, the IED clocks are configured with a ConstantDriftOscillator. They initialize with a randomized asynchronous offset (initialTime = uniform(0s, 10ms)) and experience a hardware drift rate uniformly distributed between -5ppm and +5ppm.

Simulation Engine Precision: To capture sub-microsecond synchronization and minuscule network jitter, the simulation engine's internal clock is locked to picosecond precision (simtime-resolution = ps).

TCP Stack Optimization

Due to the SCADA server executing rapid, 50ms MMS polling across 20 distinct IED nodes, the simulation generates thousands of rapid TCP connection lifecycles. To prevent ephemeral port exhaustion—which would otherwise result in a runtime crash the TCP stack is optimized. The usable ephemeral port range is expanded, and the timeWaitTimeout parameter is aggressively reduced to clear closed connections from memory.

Goose Latency analysis

The SCADA master runs two separate tasks across 20 application slots:

MMS Polling (TcpBasicClientApp): Mimics standard Manufacturing Message Specification (MMS) grid traffic. Every 50ms, SCADA opens a TCP connection on standard Port 102 to fetch status logs from each individual IED.

Sampled Values (SV) Exchange (EtherTrafGen): SCADA broad-casts raw voltage/current waveform data packets (FFFFFFFFFFFF is the Layer-2 broadcast MAC address) every 250 microseconds.

Each IED acts as a smart power sensor running multiple application layers:

App 0 & 1 (MMS Servers): Listen for and accept incoming SCADA data queries on TCP ports 102 and 103.

EthApp 0 (Sampled Values): Constantly streams raw 150-byte measurement packets directly back to the SCADA system every 250 microseconds.

EthApp 1 (GOOSE Heartbeat): Every 1 second, the IED sends a "keep-alive" Generic Object-Oriented Substation Event (GOOSE) broadcast to indicate the grid status is nominal.

Fault Simulation & Quality of Service (QoS)

This is the core stress test of the simulation script. When a fault occurs (at 30s for IED1; at 55s for the rest), EthApp[2] and EthApp[3] activate for exactly 100 milliseconds, rapidly hammering the network with a burst of packets every 2 milliseconds.

To ensure these safety critical messages bypass the massive backlog of regular data packets, the file configures Quality of Service (QoS):

To ensure these safety critical messages bypass the massive backlog of regular data packets, the file configures Quality of Service (QoS):

The GOOSE fault burst is tagged with an IEEE 802.1p Priority Code Point (PCP) of 7—the highest possible priority layer in Ethernet networking.

All network switches are upgraded to an 8-lane PriorityQueue. This ensures that if a network switch port is congested, any packet marked with a pcp = 7 bypasses the queue and is transmitted immediately, preventing critical safety trip commands from being delayed by routine measurement data.

The final section instructs OMNeT++ to capture specific telemetry data into .vec files during the simulation run so as to plot charts afterward:

Safety Latency (endToEndDelay): Tracks the critical trip time of the high-priority GOOSE packets. In real-world smart grids, critical GOOSE alerts must arrive in under 3 to 4 milliseconds to safely trip physical circuit breakers before equipment burns out. This metric proves whether your network configuration successfully achieves that threshold.

3.2.6 Network Assessment and Simulation Theory

Asset Management Throughput and Link Utilization Test

The simulation supports a theory of Continuous Observability where the SCADA system acts as an MMS client to interact with the IED object models:

Asset Health Monitoring: SCADA uses MMS to poll "Measured Values" (MV) and status attributes from the IED's Logical Nodes.

Data Set Consistency: By maintaining a low mean utilization at the SCADA interface, the network will guarantee that large Data Set transfers common in asset management for firmware updates or SCL (Substation Configuration Language) file imports do not saturate the station bus

The simulation is to prove that Over-Provisioning is a functional requirement for converged grid networks. By keeping link utilization extremely low, the network will prove to mimic the dedicated nature of traditional hardwired systems while gaining the interoperability and object-oriented data structures (Logical Nodes/Data Objects) provided by the IEC 61850 standard. This ensures that SCADA asset management remains high-fidelity, regardless of the fluctuating demands of the shared residential load.

NETWORK INITIALISATION FILE

This defines the logic of the simulation.

The success of the simulation theory is measured through Utilization and Throughput Analysis.

utilization: vector data quantifies the percentage of link bandwidth used across various network interfaces during the 100-120 second simulation.

The theory expects the core OLT and Gateway links to maintain a low mean utilization to ensure headroom for emergency transients.

The simulation is to prove the reliability of the architecture if the standard deviation of IED utilization remains significantly lower than that of residential users, confirming that grid traffic is not being "jittered" by the ISP background load.

DEDICATED FIBER ARCHITECTURE

```
[General]
network = aassetmgtdedicated.SmartGridFeeder
sim-time-limit = 70s
# ============================================================
# GLOBAL PRECISION & ROUTING
# ============================================================
simtime-resolution = ps
*.configurator.typename = "Ipv4NetworkConfigurator"
*.configurator.assignAddresses = true
*.configurator.addStaticRoutes = true
*.configurator.config = xmldoc("config.xml")
```

```
# ============================================================
# CLOCK & gPTP (IEEE 802.1AS) CONFIGURATION
# ============================================================
**.clock.oscillator.nominalTickLength = 1ns
*.grandmaster.clock.typename = "SettableClock"
*.grandmaster.clock.oscillator.typename = "ConstantDriftOscillator"
*.grandmaster.clock.oscillator.driftRate = 0ppm
**.ied*.clock.typename = "SettableClock"
**.ied*.clock.oscillator.typename = "ConstantDriftOscillator"
**.ied*.clock.oscillator.driftRate = uniform(-5ppm, 5ppm)
**.ied*.clock.initialTime = uniform(0s, 10ms)

**.hasPtp = true
*.grandmaster.gptp.role = "MASTER"
*.ied*.gptp.role = "SLAVE"
*.grandmaster.eth[0].gptp.portRole = "MASTER"
*.ied*.eth[0].gptp.portRole = "SLAVE"
*.olt.eth[*].gptp.portRole = "PASSIVE"
# ============================================================
# TCP STACK & PORT EXHAUSTION FIX
# ============================================================
**.tcp.ephemeralPortMin = 1024
**.tcp.ephemeralPortMax = 65535
**.tcp.timeWaitTimeout = 5s
**.tcp.finWait2Timeout = 5s
**.tcp.msl = 2s

# ============================================================
```

```
# NEW LEAN TIMELINE (70s Total)
# 0s  - 10s : Startup & gPTP Sync
# 10s - 30s : Phase 1 - Steady State SV Exchange
# 30s - 55s : Phase 2 - IED1 Fault Event & Alert (100ms burst - Priority 7)
# 55s - 70s : Phase 3 - Global Feeder Fault (IEDs 2-20) (100ms burst - Priority 7)
# ============================================================
# ============================================================
# SCADA CONFIGURATION
# ============================================================
*.scada.numApps = 20
*.scada.numEthApps = 1
# --- MMS Polling ---
*.scada.app[*].typename = "TcpBasicClientApp"
*.scada.app[*].connectAddress = "ied" + string(int(this.index) + 1)
*.scada.app[*].connectPort = 102
*.scada.app[*].numRequestsPerSession = -1
*.scada.app[*].thinkTime = 0s
*.scada.app[*].idleInterval = 50ms
*.scada.app[*].startTime = 1s
# --- SCADA SV Exchange ---
*.scada.ethApp[0].typename = "EtherTrafGen"
*.scada.ethApp[0].destAddress = "FFFFFFFFFFFF"
*.scada.ethApp[0].sendInterval = 250us
*.scada.ethApp[0].packetLength = 150B
*.scada.ethApp[0].startTime = 10s
*.scada.ethApp[0].stopTime = -1s


# ============================================================
```

```
# IED CONFIGURATION
# ============================================================
*.ied*.numApps = 2
*.ied*.numEthApps = 4

*.ied*.app[0].typename = "TcpGenericServerApp"
*.ied*.app[0].localPort = 102
*.ied*.app[1].typename = "TcpSinkApp"
*.ied*.app[1].localPort = 103

# --- SV Exchange (IED -> SCADA) ---
*.ied*.ethApp[0].typename = "EtherTrafGen"
*.ied*.ethApp[0].destAddress = "scada"
*.ied*.ethApp[0].packetLength = 150B
*.ied*.ethApp[0].sendInterval = 250us
*.ied*.ethApp[0].startTime = 10s
*.ied*.ethApp[0].stopTime = -1s

# --- GOOSE Heartbeat ---
*.ied*.ethApp[1].typename = "EtherTrafGen"
*.ied*.ethApp[1].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[1].sendInterval = 1s
*.ied*.ethApp[1].startTime = 1s

# --- GOOSE Fault Burst (App 2) - CRITICAL PRIORITY STAGED ---
*.ied*.ethApp[2].typename = "VlanEtherApp"
*.ied*.ethApp[2].vlanId = 1
*.ied*.ethApp[2].pcp = 7                # IEEE 802.1p Highest Priority
```

```
*.ied*.ethApp[2].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[2].packetLength = 200B
*.ied*.ethApp[2].sendInterval = 2ms

# Logic: 100ms burst duration for all relevant fault phases
*.ied*.ethApp[2].startTime = 55s
*.ied*.ethApp[2].stopTime = 55.1s
*.ied1.ethApp[2].startTime = 30s
*.ied1.ethApp[2].stopTime = 30.1s

# --- Ethernet Alert Messages (App 3) ---
*.ied*.ethApp[3].typename = "EtherTrafGen"
*.ied*.ethApp[3].destAddress = "scada"
*.ied*.ethApp[3].packetLength = 100B
*.ied*.ethApp[3].sendInterval = 100ms

# Logic: Alert messages bounded within the exact 100ms window
*.ied*.ethApp[3].startTime = 55s
*.ied*.ethApp[3].stopTime = 55.1s
*.ied1.ethApp[3].startTime = 30s
*.ied1.ethApp[3].stopTime = 30.1s

# ============================================================
# QUEUES, QoS, & RECORDING
# ============================================================
# Switch to PriorityQueue to respect the PCP/CoS bits tagged by VlanEtherApp
**.eth[*].mac.queue.typename = "PriorityQueue"
**.eth[*].mac.queue.numQueues = 8       # Handles PCP 0 through 7
```

```
**.eth[*].mac.queue.packetCapacity = 500000

# METRICS, DELAY, & SYNCHRONIZATION ANALYSIS
# ============================================================
**.vector-recording = true

# Sync Accuracy Analysis (gPTP performance study)
**.ied*.clock.clockError.recordVector = true
**.ied*.clock.driftRate.recordVector = true
**.ied*.clock.timeChanged.recordVector = true

# --- Channel Utilization ---
**.eth[*].mac.rxChannelUtilization.recordVector = true
**.eth[*].mac.txChannelUtilization.recordVector = true
**.app[*].throughput.recordVector = true
**.ethApp[*].throughput.recordVector = true

# --- End-to-End Delay for Prioritized GOOSE Storms ---
**.ied*.ethApp[2].rcvdPkLifetime.recordVector = true
**.ied*.ethApp[2].endToEndDelay.recordVector = true
```

SHARED GPON ARCHITECTURE

```
[General]
network = gooselatencyshared.GridFeeder
sim-time-limit = 120s
```

```
#=============================================================
# GLOBAL STACK & INFRASTRUCTURE
#=============================================================
**.ipv4.ip.useEcn = false
**.udp.ecnMethod = "none"
**.ipv4.ip.limitedBroadcast = false
**.*gateway.hasVlanConfig = true
**.*olt.hasVlanConfig = true


**.eth[*].queue.typename = "PriorityQueue"
**.eth[*].queue.numQueues = 8
**.eth[*].queue.classifier.typename = "PriorityClassifier"


*.configurator.config = xmldoc("config.xml")
*.configurator.assignAddresses = true
*.configurator.addStaticRoutes = true


# Statistics for Latency & Link Utilization Assessment
**.app[*].endToEndDelay:vector.record = true
**.app[*].throughput:vector.record = true
*.ied*.app[25..44].endToEndDelay:vector.record = true
**.eth[*].mac.txChannel.utilization:vector.record = true
**.eth[*].queue.packetDrop:vector.record = true
```

```
#=========================================================

# APPLICATION ALLOCATIONS (Prevents OMNeT++ Array Crashes)

#=========================================================

*.scada.numApps = 43   # Expanded to accommodate Phase 4/5 MMS Polling (apps 23..42)

*.ied*.numApps = 48    # Expanded to accommodate Phase 1 response (app 46) and Phase 4/5 response (app 47)

*.isp_core.numApps = 75



# --- FILL UNUSED APP SLOTS (ALL IEDs) ---

*.ied*.app[5..24].typename = "UdpBasicApp"

*.ied*.app[5..24].destAddresses = "127.0.0.1"

*.ied*.app[5..24].destPort = 102

*.ied*.app[5..24].messageLength = 10B

*.ied*.app[5..24].sendInterval = 1s

*.ied*.app[5..24].startTime = 1000s

*.ied*.app[5..24].stopTime = -1s



# --- IED1 SPECIFIC OVERRIDES (PHASE 6) ---

*.ied1.app[5..24].typename = "UdpBasicApp"

*.ied1.app[5..24].destAddresses = "ied" + string(index - 4)

*.ied1.app[5..24].destPort = 102

*.ied1.app[5..24].messageLength = 500B
```

```
*.ied1.app[5..24].sendInterval = exponential(1ms) # Eased and randomized to prevent channel lock

*.ied1.app[5..24].startTime = 75s

*.ied1.app[5..24].stopTime = 90s




#=========================================================

# TRAFFIC PHASE CONTROLLER (0s - 120s)

#=========================================================


# --- PHASE 1: MMS (SCADA) POLLING & IED RESPONSES (0s - 15s) ---

*.scada.app[0..19].typename = "UdpBasicApp"

*.scada.app[0..19].destPort = 102

*.scada.app[0..19].messageLength = 128B

*.scada.app[0..19].sendInterval = 50ms

*.scada.app[0..19].tos = 46

*.scada.app[0..19].destAddresses = "ied" + string(index + 1)

*.scada.app[0..19].startTime = 0.5s

*.scada.app[0..19].stopTime = 15s


# IED Response to Phase 1 Polling

*.ied*.app[46].typename = "UdpBasicApp"

*.ied*.app[46].destAddresses = "scada"

*.ied*.app[46].destPort = 4000
```

```
*.ied*.app[46].messageLength = 128B

*.ied*.app[46].sendInterval = 50ms

*.ied*.app[46].tos = 46

*.ied*.app[46].startTime = 0.51s # 10ms offset processing delay

*.ied*.app[46].stopTime = 15s


# --- PHASE 2: SV ONLY (15s - 30s) ---

*.ied*.app[1].typename = "UdpBasicApp"

*.ied*.app[1].destAddresses = "scada"

*.ied*.app[1].destPort = 4000

*.ied*.app[1].messageLength = 150B

*.ied*.app[1].sendInterval = 0.25ms

*.ied*.app[1].tos = 46

*.ied*.app[1].startTime = 15s

*.ied*.app[1].stopTime = 30s


# --- PHASE 3: GOOSE ONLY (30s - 45s) ---

*.ied*.app[2].typename = "UdpBasicApp"

*.ied*.app[2].destAddresses = "scada"

*.ied*.app[2].destPort = 4001

*.ied*.app[2].messageLength = 300B

*.ied*.app[2].sendInterval = exponential(5ms)

*.ied*.app[2].tos = 46
```

```
*.ied*.app[2].startTime = 30s

*.ied*.app[2].stopTime = 45s


# --- PHASE 4 & 5: SV + GOOSE + MMS MERGED BLOCK (45s - 75s) ---

# New SCADA MMS Polling block to prevent OMNeT++ variable overwrites

*.scada.app[23..42].typename = "UdpBasicApp"

*.scada.app[23..42].destPort = 102

*.scada.app[23..42].messageLength = 128B

*.scada.app[23..42].sendInterval = 50ms

*.scada.app[23..42].tos = 46

*.scada.app[23..42].destAddresses = "ied" + string(index - 22) # Index shifting to target ied1-ied20

*.scada.app[23..42].startTime = 45s

*.scada.app[23..42].stopTime = 75s


# IED Response to Phase 4/5 Polling

*.ied*.app[47].typename = "UdpBasicApp"

*.ied*.app[47].destAddresses = "scada"

*.ied*.app[47].destPort = 4000

*.ied*.app[47].messageLength = 128B

*.ied*.app[47].sendInterval = 50ms

*.ied*.app[47].tos = 46

*.ied*.app[47].startTime = 45.01s # 10ms offset processing delay

*.ied*.app[47].stopTime = 75s
```

```
# SV Streams (Spans both Phase 4 and 5 continuously)
*.ied*.app[3].typename = "UdpBasicApp"
*.ied*.app[3].destAddresses = "scada"
*.ied*.app[3].destPort = 4000
*.ied*.app[3].messageLength = 150B
*.ied*.app[3].sendInterval = 0.25ms
*.ied*.app[3].startTime = 45s
*.ied*.app[3].stopTime = 75s

# GOOSE Streams (Starts in Phase 5)
*.ied*.app[4].typename = "UdpBasicApp"
*.ied*.app[4].destAddresses = "scada"
*.ied*.app[4].destPort = 4001
*.ied*.app[4].messageLength = 300B
*.ied*.app[4].sendInterval = exponential(5ms)
*.ied*.app[4].startTime = 60s
*.ied*.app[4].stopTime = 75s

# --- PHASE 6: PEAK PUBLIC + GOOSE FLOOD (75s - 90s) ---
# Defined above in specific overrides

# --- PHASE 7: TOTAL NETWORK CASCADE & SCADA ALERTS (90s - 120s) ---
```

```
*.ied*.app[25..44].typename = "UdpBasicApp"
*.ied*.app[25..44].destAddresses = "ied" + string(index - 24)
*.ied*.app[25..44].destPort = 102
*.ied*.app[25..44].messageLength = 500B
*.ied*.app[25..44].sendInterval = exponential(2.5ms)
*.ied*.app[25..44].tos = 46
*.ied*.app[25..44].startTime = 90s
*.ied*.app[25..44].stopTime = 120s

# SCADA Emergency Alerts
*.ied*.app[45].typename = "UdpBasicApp"
*.ied*.app[45].destAddresses = "scada"
*.ied*.app[45].destPort = 4002
*.ied*.app[45].messageLength = 1024B
*.ied*.app[45].sendInterval = exponential(10ms)
*.ied*.app[45].tos = 46
*.ied*.app[45].startTime = 90s
*.ied*.app[45].stopTime = 120s

#=========================================================
# ADVANCING RESIDENTIAL & MUNICIPAL TRAFFIC
#=========================================================
*.isp_core.numApps = 75
```

```
# Tier 1: Light Background (30s - 60s)
*.isp_core.app[0..24].typename = "UdpBasicApp"
*.isp_core.app[0..19].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[20..24].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[0..19].sendInterval = exponential(1.5ms)
*.isp_core.app[20..24].sendInterval = exponential(0.5ms)
*.isp_core.app[0..24].startTime = 30s

# Tier 2: Medium Background (60s - 75s)
*.isp_core.app[25..49].typename = "UdpBasicApp"
*.isp_core.app[25..44].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[45..49].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[25..44].sendInterval = exponential(0.8ms)
*.isp_core.app[45..49].sendInterval = exponential(0.2ms)
*.isp_core.app[25..49].startTime = 60s

# Tier 3: PEAK Background (75s - 120s)
*.isp_core.app[50..74].typename = "UdpBasicApp"
*.isp_core.app[50..69].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[70..74].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[50..69].sendInterval = exponential(0.3ms)
*.isp_core.app[70..74].sendInterval = exponential(0.08ms)
```

```
*.isp_core.app[50..74].startTime = 75s


*.isp_core.app[*].destPort = 8000

*.isp_core.app[*].messageLength = 1450B


#============================================================

# RECEIVERS & SAFETY DEFAULTS

#============================================================

# SCADA Sinks

*.scada.app[20].typename = "UdpSink"

*.scada.app[20].localPort = 4000

*.scada.app[21].typename = "UdpSink"

*.scada.app[21].localPort = 4001

*.scada.app[22].typename = "UdpSink"

*.scada.app[22].localPort = 4002


# Standard Node Sinks

*.ied*.app[0].typename = "UdpSink"

*.ied*.app[0].localPort = 102

*.resUser*.app[0].typename = "UdpSink"

*.sink*.app[0].typename = "UdpSink"

**.app[0].localPort = 8000
```

```
**.app[*].localPort = -1

**.app[*].stopTime = -1s

**.app[*].tos = 0
```

Clock Synchronization Accuracy

Simulation aimed at proving that the gPTP (IEEE 802.1AS) synchronization is robust enough to keep phase-angle errors within the limits defined by IEC 61869-9.

IEC 61850 Sampled Values (SV) over a shared network, the theory must bridge the gap between Network Calculus (how data moves) and Power System Physics (how the grid reacts).

The Core Hypothesis

The hypothesis is that IEEE 802.1AS (gPTP) creates a "Virtual Synchronous Plane" that decouples the accuracy of protection signals from the congestion of the physical network.

As long as the Residual Synchronization Error and the Network Packet Delay Variation (PDV) stay within the sampling window of the Merging Unit, the shared network behaves identically to a dedicated point-to-point fiber link.

The proposed simulation evaluates the feasibility of converged grid feeder architectures. It posits that the Time-Aware Shaper (TAS) logic within Time-Sensitive Networking (TSN), combined with IEEE 802.1AS, provides sufficient micro-second precision to satisfy the stringent phase-angle requirements of IEC 61850-9-2. By simulating stochastic background traffic against deterministic protection streams, demonstrates that the 'Synchronization Plane' remains stable regardless of the 'Data Plane' load, thereby justifying the transition from dedicated to shared fiber infrastructure.

IEC 61850-9-3 (Power Profile): This is the official IEEE 1588 (PTP) profile for power utility automation. It establishes a target accuracy where the maximum acceptable offset for a synchronized device is 1 microsec, leading to a maximum possible 2 microsec delta between any two clocks in the system.

Synchronization Sensitivity in Protection Schemes

Research emphasizes that in digital substations, synchronization directly influences how protection functions compare data.

Phase Accuracy Requirements: In modern schemes, if synchronization error exceeds a protection element's tolerance, the realignment of sampled values in the relay can cause magnitude or phase differences that result in mis operation.

Impact on Differential Protection: For critical applications like line current differential protection, microsecond accuracy is required to satisfy Kirchhoff's current law. Errors between 1

microsec and 4 microsec can lead to the blocking of all protection functions in an Intelligent Electronic Device (IED) to avoid false trips.

gPTP for OMNeT++: Specific simulation models for IEEE 802.1AS have been developed to handle propagation delay measurements and clock drift within the INET environment. These models often utilize a Constant Drift Oscillator to simulate deviating clocks and analyze the resynchronization intervals required to maintain grid stability.

Traffic Priority (QoS): To justify a shared network, research highlights the use of IEEE 802.1Q priority tagging. This reduces queuing delay by allowing SV and GOOSE messages (typically tagged with Priority 7) to bypass lower-priority background traffic, ensuring they meet the 3 ms end-to-end latency requirement mandated by IEC 61850.

Non-Preemptive Strict Priority: The theory dictates that an SV packet (Priority 7) will never wait behind an ISP packet (Priority 0) unless the ISP packet has already begun transmission.

The Blocking Probability Formula: The maximum delay (W_{max}) an SV packet will face on your 24.6km fiber run is:

Equation 1. The Blocking Probability Formula

$$Wmax = \frac{LMTU}{R} + Propagation\ Delay$$

Where LMTU is the max size of a background ISP packet and R is the link rate

The theory posits that the worst-case jitter on a shared network is bounded by the serialization time of one maximum-sized background packet, which is negligible 12 microsec for 1Gbps) compared to the protection requirements.

The Clock Synchronization Model (gPTP/802.1AS)

In the OMNeT++ environment, the accuracy of the Sampled Values (SV) depends on the Phase Offset between the Grandmaster (GM) and the Slave IED. The theory defines the slave clock time in relation to the master time as:

Equation 2. the slave clock time in relation to the master time

$$Ts(t) = Tm(t) + \theta(t) + \int_0^t \Delta f(\tau)\mathrm{d}\tau + \eta(\mathrm{t})$$

$\theta(t)$: Phase offset (the error gPTP tries to correct).

$\Delta f(\tau)$: Frequency drift of the ConstantDriftOscillator

$\eta(t)$: measurement noise (jitter from the network)

IEC 61850 Sampled Value (SV) Mapping Theory

The sampled Value stream (IEC 61850-9-2) is a time-discrete representation of a continuous analog waveform. The theory of phase Displacement states that a timing error (Δt) manifests as a vector error in the protection relay.

The sensitivity Formula

At a grid frequency of f (50Hz), the phase error Δφ in degrees is:

Equation 3. The sensitivity Formula.

$$\Delta\varphi = 360.\ f.\ \Delta t$$

NETWORK INITIALISATION FILE

DEDICATED FIBER ARCHITECTURE

```
[General]
network = aassetmgtdedicated.SmartGridFeeder
sim-time-limit = 70s
# ============================================================
# GLOBAL PRECISION & ROUTING
# ============================================================
simtime-resolution = ps
*.configurator.typename = "Ipv4NetworkConfigurator"
*.configurator.assignAddresses = true
*.configurator.addStaticRoutes = true
*.configurator.config = xmldoc("config.xml")
# ============================================================
# CLOCK & gPTP (IEEE 802.1AS) CONFIGURATION
# ============================================================
```

```
**.clock.oscillator.nominalTickLength = 1ns
*.grandmaster.clock.typename = "SettableClock"
*.grandmaster.clock.oscillator.typename = "ConstantDriftOscillator"
*.grandmaster.clock.oscillator.driftRate = 0ppm
**.ied*.clock.typename = "SettableClock"
**.ied*.clock.oscillator.typename = "ConstantDriftOscillator"
**.ied*.clock.oscillator.driftRate = uniform(-5ppm, 5ppm)
**.ied*.clock.initialTime = uniform(0s, 10ms)

**.hasPtp = true
*.grandmaster.gptp.role = "MASTER"
*.ied*.gptp.role = "SLAVE"
*.grandmaster.eth[0].gptp.portRole = "MASTER"
*.ied*.eth[0].gptp.portRole = "SLAVE"
*.olt.eth[*].gptp.portRole = "PASSIVE"
# ============================================================
# TCP STACK & PORT EXHAUSTION FIX
# ============================================================
**.tcp.ephemeralPortMin = 1024
**.tcp.ephemeralPortMax = 65535
**.tcp.timeWaitTimeout = 5s
**.tcp.finWait2Timeout = 5s
**.tcp.msl = 2s

# ============================================================
# NEW LEAN TIMELINE (70s Total)
# 0s  - 10s : Startup & gPTP Sync
# 10s - 30s : Phase 1 - Steady State SV Exchange
```

```
# 30s - 55s : Phase 2 - IED1 Fault Event & Alert (100ms burst - Priority 7)
# 55s - 70s : Phase 3 - Global Feeder Fault (IEDs 2-20) (100ms burst - Priority 7)
# ============================================================
# ============================================================
# SCADA CONFIGURATION
# ============================================================
*.scada.numApps = 20
*.scada.numEthApps = 1
# --- MMS Polling ---
*.scada.app[*].typename = "TcpBasicClientApp"
*.scada.app[*].connectAddress = "ied" + string(int(this.index) + 1)
*.scada.app[*].connectPort = 102
*.scada.app[*].numRequestsPerSession = -1
*.scada.app[*].thinkTime = 0s
*.scada.app[*].idleInterval = 50ms
*.scada.app[*].startTime = 1s
# --- SCADA SV Exchange ---
*.scada.ethApp[0].typename = "EtherTrafGen"
*.scada.ethApp[0].destAddress = "FFFFFFFFFFFF"
*.scada.ethApp[0].sendInterval = 250us
*.scada.ethApp[0].packetLength = 150B
*.scada.ethApp[0].startTime = 10s
*.scada.ethApp[0].stopTime = -1s


# ============================================================
# IED CONFIGURATION
# ============================================================
*.ied*.numApps = 2
```

```
*.ied*.numEthApps = 4

*.ied*.app[0].typename = "TcpGenericServerApp"
*.ied*.app[0].localPort = 102
*.ied*.app[1].typename = "TcpSinkApp"
*.ied*.app[1].localPort = 103

# --- SV Exchange (IED -> SCADA) ---
*.ied*.ethApp[0].typename = "EtherTrafGen"
*.ied*.ethApp[0].destAddress = "scada"
*.ied*.ethApp[0].packetLength = 150B
*.ied*.ethApp[0].sendInterval = 250us
*.ied*.ethApp[0].startTime = 10s
*.ied*.ethApp[0].stopTime = -1s

# --- GOOSE Heartbeat ---
*.ied*.ethApp[1].typename = "EtherTrafGen"
*.ied*.ethApp[1].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[1].sendInterval = 1s
*.ied*.ethApp[1].startTime = 1s

# --- GOOSE Fault Burst (App 2) - CRITICAL PRIORITY STAGED ---
*.ied*.ethApp[2].typename = "VlanEtherApp"
*.ied*.ethApp[2].vlanId = 1
*.ied*.ethApp[2].pcp = 7                # IEEE 802.1p Highest Priority
*.ied*.ethApp[2].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[2].packetLength = 200B
*.ied*.ethApp[2].sendInterval = 2ms
```

```
# Logic: 100ms burst duration for all relevant fault phases
*.ied*.ethApp[2].startTime = 55s
*.ied*.ethApp[2].stopTime = 55.1s
*.ied1.ethApp[2].startTime = 30s
*.ied1.ethApp[2].stopTime = 30.1s

# --- Ethernet Alert Messages (App 3) ---
*.ied*.ethApp[3].typename = "EtherTrafGen"
*.ied*.ethApp[3].destAddress = "scada"
*.ied*.ethApp[3].packetLength = 100B
*.ied*.ethApp[3].sendInterval = 100ms

# Logic: Alert messages bounded within the exact 100ms window
*.ied*.ethApp[3].startTime = 55s
*.ied*.ethApp[3].stopTime = 55.1s
*.ied1.ethApp[3].startTime = 30s
*.ied1.ethApp[3].stopTime = 30.1s

# ============================================================
# QUEUES, QoS, & RECORDING
# ============================================================
# Switch to PriorityQueue to respect the PCP/CoS bits tagged by VlanEtherApp
**.eth[*].mac.queue.typename = "PriorityQueue"
**.eth[*].mac.queue.numQueues = 8       # Handles PCP 0 through 7
**.eth[*].mac.queue.packetCapacity = 500000

# METRICS, DELAY, & SYNCHRONIZATION ANALYSIS
```

```
# ========================================================
**.vector-recording = true

# Sync Accuracy Analysis (gPTP performance study)
**.ied*.clock.clockError.recordVector = true
**.ied*.clock.driftRate.recordVector = true
**.ied*.clock.timeChanged.recordVector = true

# --- Channel Utilization ---
**.eth[*].mac.rxChannelUtilization.recordVector = true
**.eth[*].mac.txChannelUtilization.recordVector = true
**.app[*].throughput.recordVector = true
**.ethApp[*].throughput.recordVector = true

# --- End-to-End Delay for Prioritized GOOSE Storms ---
**.ied*.ethApp[2].rcvdPkLifetime.recordVector = true
**.ied*.ethApp[2].endToEndDelay.recordVector = true
```

SHARED GPON

Precise Time Synchronization (gPTP)

The simulation implements IEEE 802.1AS (gPTP), which is critical for IEC 61850 sampled values and synchrophasor data.

Realism through Drift: By using **ConstantDriftOscillator** with a drift rate of **+/- 50ppm**, real-world hardware where clocks don't stay perfectly in sync is simulated.

Hierarchy:

Grandmaster: The **scada** node is the source of "true time."

The Clock Source (Oscillator & Drift)

The foundation of the PTP setup is the **SettableClock**. Unlike a standard simulation clock that is perfectly linear, this is designed for realism:

ConstantDriftOscillator: This simulates the physical limitations of crystal oscillators found in real IEDs and switches.

Drift Rate: By setting uniform (-50ppm, 50ppm), each device starts with a slightly different "speed." Without PTP, these clocks would drift apart significantly over the 180s simulation, leading to massive errors in fault timestamps

The gPTP Hierarchy (Grandmaster to Slave)

Table 8. The gPTP Hierarchy. Grandmaster to Slave

Role	Nodes	Function
Grandmaster	scada	The Source of Truth. It has the highest masterWeight (255), meaning it dictates the time to the rest of the network.
Bridge Nodes	gateway, olt, splitter*	These act as Boundary Clocks. They receive time on a Slave Port and redistribute it to downstream devices via Master Ports.
Slave Nodes	ied*, resUser*, sink*	These are the end consumers. They adjust their local SettableClock to match the SCADA time.

Hardware Timestamping & External Clocks

In a standard simulation, PTP messages are processed by the CPU, which introduces stack jitter. By pointing the Ethernet interface (eth[*]) directly to the hardware clock module, Hardware Timestamping is simulated. This allows the gPTP protocol to record the exact nanosecond a packet leaves the physical wire, bypassing the delays of the operating system.

Performance Verification

To analyze if PTP is actually working, recording for the following is enabled:

localTimeOffset: This is the Gold Metric. It tells you the difference between a node's clock and the Grandmaster's clock. In a successful grid simulation, this should stay extremely close to zero.

pathDelay: This validates your FeederFiber and BranchFiber settings (264 microsec and 25microsec respectively). PTP uses these measurements to compensate for the time it takes for a sync message to travel down the fiber.

In IEC 61850 context, this PTP setup ensures that if ied1 and ied20 (which are kilometers apart) detect a fault, the **SCADA** system can compare their timestamps and know exactly which one occurred first within a few nanoseconds, regardless of how much "background noise" is coming from the residential users.

The results focus on the timeChanged:vector for the underlyingClock and the logical clock of each module.

Synchronization Integrity (Local vs. Underlying)

In a gPTP-enabled INET simulation, each host has an underlyingClock (the raw, drifting hardware oscillator) and a clock (the synchronized logical clock).

Bridges: The substation_gateway, olt, and splitters propagate the time information.

Slaves: The IEDs and user laptops adjust their local clocks based on the SCADA node.

```
[General]

network = controlaccuracy.GridFeeder

sim-time-limit = 180s



# ============================================================

# 1. CLOCK & gPTP CONFIGURATION (INET 4.6)

# ============================================================

# RECONCILIATION FIX: Target ONLY node-level clocks to prevent

# duplicate "ghost clocks" from instantiating inside eth[*] and lo[*]

*.*.clock.typename = "SettableClock"

*.*.clock.oscillator.typename = "ConstantDriftOscillator"

*.*.clock.oscillator.nominalTickLength = 1ns

*.*.clock.oscillator.driftRate = uniform(-50ppm, 50ppm)



# DRIFT CORRECTION: Assign a Clock Servo to handle frequency compensation

# and dynamically correct the drift back to 0 ppm relative to the master

*.*.clock.clockServo.typename = "StepClockServo"
```

```
*.*.clock.clockServo.resetOscillator = false


# Enforce clock submodule instantiation across TSN-enabled nodes
**.hasTimeSynchronization = true
**.hasGptp = true


# ORDER FIX: Specific nested submodules must be defined before the global catch-all
**.app[*].clockModule = "^.clock"
**.eth[*].mac.clockModule = "^.^.clock"
**.gptp.clockServo.clockModule = "^.^.clock"
**.gptp.clockModule = "^.clock"


# Let INET auto-discover or ignore the clock for non-TSN components
**.clockModule = ""
# ------------------------------------------------
# Set operational synchronization tracking intervals
**.gptp.syncInterval = 0.125s     # Sync messages 8 times a second (IEEE 802.1AS standard)
**.gptp.pdelayInterval = 1s       # Link propagation delay checks every 1s


*.scada.gptp.gptpNodeType = "MASTER_NODE"
*.scada.gptp.masterWeight = 255


# FIX: OMNeT++ 6.x Array Syntax
```

```
*.scada.gptp.masterPorts = ["eth0"]


*.substation_gateway.gptp.gptpNodeType = "BRIDGE_NODE"

*.substation_gateway.gptp.slavePort = "eth0"

*.substation_gateway.gptp.masterPorts = ["eth1"]


*.olt.gptp.gptpNodeType = "BRIDGE_NODE"

*.olt.gptp.slavePort = "eth0"

*.olt.gptp.masterPorts = ["eth1", "eth2", "eth3", "eth4", "eth5", "eth6", "eth7", "eth8",
"eth9", "eth10", "eth11"]


*.splitter*.gptp.gptpNodeType = "BRIDGE_NODE"

*.splitter*.gptp.slavePort = "eth0"

*.splitter*.gptp.masterPorts = ["eth1", "eth2", "eth3", "eth4"]


**.ied*.gptp.gptpNodeType = "SLAVE_NODE"

**.resUser*.gptp.gptpNodeType = "SLAVE_NODE"

**.sink*.gptp.gptpNodeType = "SLAVE_NODE"

**.isp_core.gptp.gptpNodeType = "SLAVE_NODE"

**.gptp.slavePort = "eth0"


# FIX: Empty arrays must use brackets, not strings

**.gptp.masterPorts = []
```

```
**.gptp.domainNumber = 0

**.gptp.pdelayService = true


# ============================================================

# 2. LAYER 2 ISOLATION (VLANs) & SWITCHING

# ============================================================

**.hasIeee8021q = true

*.scada.eth[*].**.vlanId = 10

*.ied*.eth[*].**.vlanId = 10

*.isp_core.eth[*].**.vlanId = 20

*.resUser*.eth[*].**.vlanId = 20

*.sink*.eth[*].**.vlanId = 20


**.bridging.vlanPolicy.typename = "VlanPolicy"

**.bridging.vlanFilter.typename = "VlanFilter"

# gPTP VLAN BYPASS RULES

# ============================================================

# 1. Allow untagged link-local frames (like gPTP) to bypass VLAN drop rules

**.bridging.vlanFilter.dropUntagged = false

**.bridging.vlanPolicy.dropUntagged = false

**.gptp.clockServo.adjustOscillatorRate = true


**.macTable.agingTime = 0s
```

```
**.splitter*.processingDelay = 0s
**.splitter*.eth[*].mac.duplexMode = true

# ============================================================
# 3. TRAFFIC: GRID DOMAIN (IEC 61850)
# ============================================================
*.scada.numApps = 61
*.scada.app[0..59].typename = "UdpBasicApp"
*.scada.app[0..59].destPort = 102
*.scada.app[0..59].messageLength = 128B
*.scada.app[0..59].sendInterval = 50ms

# FIX: Replaced 'sprintf' with 'stringf'
*.scada.app[0..59].destAddresses = "ied" + string((index % 20) + 1)

*.scada.app[60].typename = "UdpSink"
*.scada.app[60].localPort = 4000

*.ied*.numApps = 6
*.ied*.app[0].typename = "UdpSink"
*.ied*.app[0].localPort = 102

*.ied*.app[1..5].typename = "UdpBasicApp"
```

```
*.ied*.app[1..5].destAddresses = "scada"

*.ied*.app[1..5].destPort = 4000

*.ied*.app[1..5].messageLength = 200B

*.ied*.app[1..5].sendInterval = 2.5ms


**.mac.queue.packetCapacity = 10000


# Timing Sequences for Network Load Analysis

*.scada.app[0..19].startTime = 2s

*.scada.app[0..19].stopTime = 30s

*.ied*.app[1].startTime = 31s

*.ied*.app[1].stopTime = 60s

*.ied*.app[2].startTime = 61s

*.ied*.app[2].stopTime = 90s

*.scada.app[20..39].startTime = 91s

*.scada.app[20..39].stopTime = 120s

*.ied*.app[3].startTime = 91s

*.ied*.app[3].stopTime = 120s

*.ied*.app[4].startTime = 121s

*.ied*.app[4].stopTime = 150s

*.scada.app[40..59].startTime = 151s

*.scada.app[40..59].stopTime = 180s

*.ied*.app[5].startTime = 151s
```

```
*.ied*.app[5].stopTime = 180s


# ==========================================================
# 4. TRAFFIC: PUBLIC DOMAIN (Background Traffic)
# ==========================================================
*.isp_core.numApps = 77
*.isp_core.app[0..74].typename = "UdpBasicApp"

# FIX: Replaced 'sprintf' with 'stringf'
*.isp_core.app[0..69].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[70..74].destAddresses = "sink" + string((index % 5) + 1)

*.isp_core.app[0..74].destPort = 8000
*.isp_core.app[0..74].messageLength = 1450B
*.isp_core.app[0..74].sendInterval = exponential(51ms)

*.isp_core.app[75..76].typename = "UdpSink"
*.isp_core.app[75].localPort = 9000
*.isp_core.app[76].localPort = 9001

*.isp_core.app[0..20].startTime = 2s
*.isp_core.app[21..50].startTime = 61s
*.isp_core.app[51..74].startTime = 121s
```

```
*.resUser*.numApps = 2
*.resUser*.app[0].typename = "UdpSink"
*.resUser*.app[0].localPort = 8000
*.resUser*.app[1].typename = "UdpBasicApp"
*.resUser*.app[1].destAddresses = "isp_core"
*.resUser*.app[1].destPort = 9000
*.resUser*.app[1].messageLength = 1450B
*.resUser*.app[1].sendInterval = 6.25ms
*.resUser*.app[1].startTime = 2s

*.sink*.numApps = 2
*.sink*.app[0].typename = "UdpSink"
*.sink*.app[0].localPort = 8000
*.sink*.app[1].typename = "UdpBasicApp"
*.sink*.app[1].destAddresses = "isp_core"
*.sink*.app[1].destPort = 9001
*.sink*.app[1].messageLength = 1450B
*.sink*.app[1].sendInterval = 0.54ms
*.sink*.app[1].startTime = 2s

# ============================================================
# 5. INFRASTRUCTURE & RECORDING
```

```
# ======================================================

**.ipv4.arp.typename = "GlobalArp"



# Verification Vectors Cleaned up to match strict node-level recording

*.*.clock.driftRate:vector.record = true

*.*.clock.localTime:vector.record = true

**.gptp.localTimeOffset:vector.record = true

**.gptp.pathDelay:vector.record = true

**.app[*].endToEndDelay:vector.record = true

# NEW: Record the compensation vector to verify the software layer adjusting for the hardware drift rate

**.clock.oscillator.compensationFactor:vector.record = true

**.clock.oscillator.compensationFactor.result-recording-modes = +vector

# Track the master-to-slave delay and calculated rate ratios from gPTP

**.gptp.masterToSlaveDelay.result-recording-modes = +vector

**.gptp.neighborRateRatio.result-recording-modes = +vector



# Track the actual local clock time divergence relative to nominal time

**.clock.timeChanged.result-recording-modes = +vector
```

Goose Latency Analysis

GOOSE (Generic Object-Oriented Substation Event)

Within the IEC 61850 framework, GOOSE (Generic Object-Oriented Substation Event) messaging represents the most critical, time-sensitive data profile in the power grid. It is primarily utilized for transmitting high-speed 'trip' commands mission-critical instructions that force a circuit breaker to open instantaneously to isolate electrical faults. This rapid fault-clearing capability is

essential for preventing catastrophic equipment damage, minimizing widespread power outages, and mitigating fire hazards.

To achieve its stringent latency requirements, GOOSE traffic does not rely on standard TCP/IP routing. Instead, it is mapped directly to the Ethernet Data Link layer (Layer 2) using a multicast publisher-subscriber model. By bypassing the processing overhead of the network and transport layers, GOOSE messages can achieve the sub-millisecond execution times required for modern grid protection.

Under the IEC 61850-5 standard, GOOSE messages are classified as Type 1A (Trip) data. To ensure grid stability, the standard dictates that these messages must be transmitted and processed end-to-end within a strict time boundary of less than 3 milliseconds. Exceeding this threshold during a short-circuit event could result in unrecoverable asset destruction

NETWORK INITIALIZATION FILE

DEDICATED FIBER ARCHITECTURE

```
[General]
network = aassetmgtdedicated.SmartGridFeeder
sim-time-limit = 70s
# ============================================================
# GLOBAL PRECISION & ROUTING
# ============================================================
simtime-resolution = ps
*.configurator.typename = "Ipv4NetworkConfigurator"
*.configurator.assignAddresses = true
*.configurator.addStaticRoutes = true
*.configurator.config = xmldoc("config.xml")
# ============================================================
# CLOCK & gPTP (IEEE 802.1AS) CONFIGURATION
# ============================================================
**.clock.oscillator.nominalTickLength = 1ns
*.grandmaster.clock.typename = "SettableClock"
*.grandmaster.clock.oscillator.typename = "ConstantDriftOscillator"
```

```
*.grandmaster.clock.oscillator.driftRate = 0ppm
**.ied*.clock.typename = "SettableClock"
**.ied*.clock.oscillator.typename = "ConstantDriftOscillator"
**.ied*.clock.oscillator.driftRate = uniform(-5ppm, 5ppm)
**.ied*.clock.initialTime = uniform(0s, 10ms)

**.hasPtp = true
*.grandmaster.gptp.role = "MASTER"
*.ied*.gptp.role = "SLAVE"
*.grandmaster.eth[0].gptp.portRole = "MASTER"
*.ied*.eth[0].gptp.portRole = "SLAVE"
*.olt.eth[*].gptp.portRole = "PASSIVE"
# ============================================================
# TCP STACK & PORT EXHAUSTION FIX
# ============================================================
**.tcp.ephemeralPortMin = 1024
**.tcp.ephemeralPortMax = 65535
**.tcp.timeWaitTimeout = 5s
**.tcp.finWait2Timeout = 5s
**.tcp.msl = 2s

# ============================================================
# NEW LEAN TIMELINE (70s Total)
# 0s  - 10s : Startup & gPTP Sync
# 10s - 30s : Phase 1 - Steady State SV Exchange
# 30s - 55s : Phase 2 - IED1 Fault Event & Alert (100ms burst - Priority 7)
# 55s - 70s : Phase 3 - Global Feeder Fault (IEDs 2-20) (100ms burst - Priority 7)
# ============================================================
```

```
# ============================================================
# SCADA CONFIGURATION
# ============================================================
*.scada.numApps = 20
*.scada.numEthApps = 1
# --- MMS Polling ---
*.scada.app[*].typename = "TcpBasicClientApp"
*.scada.app[*].connectAddress = "ied" + string(int(this.index) + 1)
*.scada.app[*].connectPort = 102
*.scada.app[*].numRequestsPerSession = -1
*.scada.app[*].thinkTime = 0s
*.scada.app[*].idleInterval = 50ms
*.scada.app[*].startTime = 1s
# --- SCADA SV Exchange ---
*.scada.ethApp[0].typename = "EtherTrafGen"
*.scada.ethApp[0].destAddress = "FFFFFFFFFFFF"
*.scada.ethApp[0].sendInterval = 250us
*.scada.ethApp[0].packetLength = 150B
*.scada.ethApp[0].startTime = 10s
*.scada.ethApp[0].stopTime = -1s


# ============================================================
# IED CONFIGURATION
# ============================================================
*.ied*.numApps = 2
*.ied*.numEthApps = 4


*.ied*.app[0].typename = "TcpGenericServerApp"
```

```
*.ied*.app[0].localPort = 102
*.ied*.app[1].typename = "TcpSinkApp"
*.ied*.app[1].localPort = 103

# --- SV Exchange (IED -> SCADA) ---
*.ied*.ethApp[0].typename = "EtherTrafGen"
*.ied*.ethApp[0].destAddress = "scada"
*.ied*.ethApp[0].packetLength = 150B
*.ied*.ethApp[0].sendInterval = 250us
*.ied*.ethApp[0].startTime = 10s
*.ied*.ethApp[0].stopTime = -1s

# --- GOOSE Heartbeat ---
*.ied*.ethApp[1].typename = "EtherTrafGen"
*.ied*.ethApp[1].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[1].sendInterval = 1s
*.ied*.ethApp[1].startTime = 1s

# --- GOOSE Fault Burst (App 2) - CRITICAL PRIORITY STAGED ---
*.ied*.ethApp[2].typename = "VlanEtherApp"
*.ied*.ethApp[2].vlanId = 1
*.ied*.ethApp[2].pcp = 7                # IEEE 802.1p Highest Priority
*.ied*.ethApp[2].destAddress = "FFFFFFFFFFFF"
*.ied*.ethApp[2].packetLength = 200B
*.ied*.ethApp[2].sendInterval = 2ms

# Logic: 100ms burst duration for all relevant fault phases
*.ied*.ethApp[2].startTime = 55s
```

```
*.ied*.ethApp[2].stopTime = 55.1s
*.ied1.ethApp[2].startTime = 30s
*.ied1.ethApp[2].stopTime = 30.1s

# --- Ethernet Alert Messages (App 3) ---
*.ied*.ethApp[3].typename = "EtherTrafGen"
*.ied*.ethApp[3].destAddress = "scada"
*.ied*.ethApp[3].packetLength = 100B
*.ied*.ethApp[3].sendInterval = 100ms

# Logic: Alert messages bounded within the exact 100ms window
*.ied*.ethApp[3].startTime = 55s
*.ied*.ethApp[3].stopTime = 55.1s
*.ied1.ethApp[3].startTime = 30s
*.ied1.ethApp[3].stopTime = 30.1s

# ============================================================
# QUEUES, QoS, & RECORDING
# ============================================================
# Switch to PriorityQueue to respect the PCP/CoS bits tagged by VlanEtherApp
**.eth[*].mac.queue.typename = "PriorityQueue"
**.eth[*].mac.queue.numQueues = 8       # Handles PCP 0 through 7
**.eth[*].mac.queue.packetCapacity = 500000

# METRICS, DELAY, & SYNCHRONIZATION ANALYSIS
# ============================================================
**.vector-recording = true
```

```
# Sync Accuracy Analysis (gPTP performance study)
**.ied*.clock.clockError.recordVector = true
**.ied*.clock.driftRate.recordVector = true
**.ied*.clock.timeChanged.recordVector = true

# --- Channel Utilization ---
**.eth[*].mac.rxChannelUtilization.recordVector = true
**.eth[*].mac.txChannelUtilization.recordVector = true
**.app[*].throughput.recordVector = true
**.ethApp[*].throughput.recordVector = true

# --- End-to-End Delay for Prioritized GOOSE Storms ---
**.ied*.ethApp[2].rcvdPkLifetime.recordVector = true
**.ied*.ethApp[2].endToEndDelay.recordVector = true
```

SHARED GPON ARCHITECTURE

The Logical Role of GOOSE

In the simulation, GOOSE is modeled as a high-priority peer-to-peer or peer-to-SCADA event.

Protocol Mapping: While real GOOSE usually runs directly on Layer 2 (Ethernet) to save time, the .ini file maps it to UDP/IP (UdpBasicApp) for routability.

Priority: It is assigned ToS 46 (Expedited Forwarding). In the switches, this maps to the highest of the 8 configured queues, ensuring that even if a residential user is downloading a large file, the GOOSE packet jumps the line.

GOOSE Traffic Characteristics

The .ini file defines the physics of these messages during Phases 3, 5, 6, and 7:

Payload Size: Set to 300B to 500B. This accounts for the dataset headers, the status change information, and the security signatures typical of an IEC 61850-9-2 frame.

Timing (The Staccato Effect):

Under normal conditions (Phase 3), it uses exponential(5ms). This simulates a steady state where IEDs are reporting status updates.

During the Flood or Cascade (Phases 6 and 7), the frequency increases to exponential(2ms).

The Assumption:

Real GOOSE uses a retransmission strategy where it fires rapidly (e.g., every 2ms) immediately after a fault and then slows down. The simulation approximates the burst state of a grid failure.

In Phase 6, the simulation specifically overrides ied1 to blast 500B GOOSE messages at a 2ms interval.

The Goal:

This tests the OLT (Optical Line Terminal). Since all 10 splitters funnel back into one OLT, a Flood from several IEDs combined with Peak Public traffic (Tier 3 ISP traffic) creates a bottleneck.

The Analysis:

If the endToEndDelay for these GOOSE packets exceeds 3ms, the grid protection is considered failed by industry standards, even if the residential users are still happily browsing the web.

Safety and Reliability Assumptions

The file uses exponential () distributions for GOOSE intervals. This is a critical simulation choice: if every IED sent a GOOSE packet at the exact same microsecond (deterministic timing), it would create an artificial collision in the simulation that might not happen in reality. Randomizing the intervals desynchronizes the messages, allowing the simulation to model a more realistic, stochastic flow of emergency data.

The GOOSE Flood:

In Phase 6 and 7, the ied1 and subsequent IEDs begin sending 500B packets at sub-millisecond intervals. This simulates a Broadcast Storm, a catastrophic grid failure where every device is shouting for attention simultaneously.

Data Recording:

The file is very selective about what it saves. It records endToEndDelay for only specific apps to capture Latency data for grid feeder vLAN devices.

```
[General]

network = gooselatencyshared.GridFeeder

sim-time-limit = 120s

#=============================================================

# GLOBAL STACK & INFRASTRUCTURE

#=============================================================

**.ipv4.ip.useEcn = false

**.udp.ecnMethod = "none"

**.ipv4.ip.limitedBroadcast = false

**.*gateway.hasVlanConfig = true

**.*olt.hasVlanConfig = true


**.eth[*].queue.typename = "PriorityQueue"

**.eth[*].queue.numQueues = 8

**.eth[*].queue.classifier.typename = "PriorityClassifier"


*.configurator.config = xmldoc("config.xml")

*.configurator.assignAddresses = true

*.configurator.addStaticRoutes = true


# Statistics for Latency & Link Utilization Assessment

**.app[*].endToEndDelay:vector.record = true

**.app[*].throughput:vector.record = true
```

```
*.ied*.app[25..44].endToEndDelay:vector.record = true

**.eth[*].mac.txChannel.utilization:vector.record = true

**.eth[*].queue.packetDrop:vector.record = true



#=============================================================

# APPLICATION ALLOCATIONS (Prevents OMNeT++ Array Crashes)

#=============================================================

*.scada.numApps = 43   # Expanded to accommodate Phase 4/5 MMS Polling (apps 23..42)

*.ied*.numApps = 48    # Expanded to accommodate Phase 1 response (app 46) and Phase 4/5 response (app 47)

*.isp_core.numApps = 75



# --- FILL UNUSED APP SLOTS (ALL IEDs) ---

*.ied*.app[5..24].typename = "UdpBasicApp"

*.ied*.app[5..24].destAddresses = "127.0.0.1"

*.ied*.app[5..24].destPort = 102

*.ied*.app[5..24].messageLength = 10B

*.ied*.app[5..24].sendInterval = 1s

*.ied*.app[5..24].startTime = 1000s

*.ied*.app[5..24].stopTime = -1s



# --- IED1 SPECIFIC OVERRIDES (PHASE 6) ---

*.ied1.app[5..24].typename = "UdpBasicApp"

*.ied1.app[5..24].destAddresses = "ied" + string(index - 4)
```

```
*.ied1.app[5..24].destPort = 102

*.ied1.app[5..24].messageLength = 500B

*.ied1.app[5..24].sendInterval = exponential(1ms) # Eased and randomized to prevent channel lock

*.ied1.app[5..24].startTime = 75s

*.ied1.app[5..24].stopTime = 90s



#=========================================================

# TRAFFIC PHASE CONTROLLER (0s - 180s)

#=========================================================



# --- PHASE 1: MMS (SCADA) POLLING & IED RESPONSES (0s - 15s) ---

*.scada.app[0..19].typename = "UdpBasicApp"

*.scada.app[0..19].destPort = 102

*.scada.app[0..19].messageLength = 128B

*.scada.app[0..19].sendInterval = 50ms

*.scada.app[0..19].tos = 46

*.scada.app[0..19].destAddresses = "ied" + string(index + 1)

*.scada.app[0..19].startTime = 0.5s

*.scada.app[0..19].stopTime = 15s



# IED Response to Phase 1 Polling

*.ied*.app[46].typename = "UdpBasicApp"

*.ied*.app[46].destAddresses = "scada"
```

```
*.ied*.app[46].destPort = 4000

*.ied*.app[46].messageLength = 128B

*.ied*.app[46].sendInterval = 50ms

*.ied*.app[46].tos = 46

*.ied*.app[46].startTime = 0.51s # 10ms offset processing delay

*.ied*.app[46].stopTime = 15s


# --- PHASE 2: SV ONLY (15s - 30s) ---

*.ied*.app[1].typename = "UdpBasicApp"

*.ied*.app[1].destAddresses = "scada"

*.ied*.app[1].destPort = 4000

*.ied*.app[1].messageLength = 150B

*.ied*.app[1].sendInterval = 0.25ms

*.ied*.app[1].tos = 46

*.ied*.app[1].startTime = 15s

*.ied*.app[1].stopTime = 30s


# --- PHASE 3: GOOSE ONLY (30s - 45s) ---

*.ied*.app[2].typename = "UdpBasicApp"

*.ied*.app[2].destAddresses = "scada"

*.ied*.app[2].destPort = 4001

*.ied*.app[2].messageLength = 300B

*.ied*.app[2].sendInterval = exponential(5ms)
```

```
*.ied*.app[2].tos = 46

*.ied*.app[2].startTime = 30s

*.ied*.app[2].stopTime = 45s


# --- PHASE 4 & 5: SV + GOOSE + MMS MERGED BLOCK (45s - 75s) ---

# New SCADA MMS Polling block to prevent OMNeT++ variable overwrites

*.scada.app[23..42].typename = "UdpBasicApp"

*.scada.app[23..42].destPort = 102

*.scada.app[23..42].messageLength = 128B

*.scada.app[23..42].sendInterval = 50ms

*.scada.app[23..42].tos = 46

*.scada.app[23..42].destAddresses = "ied" + string(index - 22) # Index shifting to target ied1-ied20

*.scada.app[23..42].startTime = 45s

*.scada.app[23..42].stopTime = 75s


# IED Response to Phase 4/5 Polling

*.ied*.app[47].typename = "UdpBasicApp"

*.ied*.app[47].destAddresses = "scada"

*.ied*.app[47].destPort = 4000

*.ied*.app[47].messageLength = 128B

*.ied*.app[47].sendInterval = 50ms

*.ied*.app[47].tos = 46

*.ied*.app[47].startTime = 45.01s # 10ms offset processing delay
```

```
*.ied*.app[47].stopTime = 75s


# SV Streams (Spans both Phase 4 and 5 continuously)
*.ied*.app[3].typename = "UdpBasicApp"
*.ied*.app[3].destAddresses = "scada"
*.ied*.app[3].destPort = 4000
*.ied*.app[3].messageLength = 150B
*.ied*.app[3].sendInterval = 0.25ms
*.ied*.app[3].startTime = 45s
*.ied*.app[3].stopTime = 75s


# GOOSE Streams (Starts in Phase 5)
*.ied*.app[4].typename = "UdpBasicApp"
*.ied*.app[4].destAddresses = "scada"
*.ied*.app[4].destPort = 4001
*.ied*.app[4].messageLength = 300B
*.ied*.app[4].sendInterval = exponential(5ms)
*.ied*.app[4].startTime = 60s
*.ied*.app[4].stopTime = 75s


# --- PHASE 6: PEAK PUBLIC + GOOSE FLOOD (75s - 90s) ---
# Defined above in specific overrides
```

```
# --- PHASE 7: TOTAL NETWORK CASCADE & SCADA ALERTS (90s - 180s) ---
*.ied*.app[25..44].typename = "UdpBasicApp"
*.ied*.app[25..44].destAddresses = "ied" + string(index - 24)
*.ied*.app[25..44].destPort = 102
*.ied*.app[25..44].messageLength = 500B
*.ied*.app[25..44].sendInterval = exponential(2.5ms)
*.ied*.app[25..44].tos = 46
*.ied*.app[25..44].startTime = 90s
*.ied*.app[25..44].stopTime = 120s

# SCADA Emergency Alerts
*.ied*.app[45].typename = "UdpBasicApp"
*.ied*.app[45].destAddresses = "scada"
*.ied*.app[45].destPort = 4002
*.ied*.app[45].messageLength = 1024B
*.ied*.app[45].sendInterval = exponential(10ms)
*.ied*.app[45].tos = 46
*.ied*.app[45].startTime = 90s
*.ied*.app[45].stopTime = 120s

#=========================================================
# ADVANCING RESIDENTIAL & MUNICIPAL TRAFFIC
#=========================================================
```

```
*.isp_core.numApps = 75


# Tier 1: Light Background (30s - 60s)
*.isp_core.app[0..24].typename = "UdpBasicApp"
*.isp_core.app[0..19].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[20..24].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[0..19].sendInterval = exponential(1.5ms)
*.isp_core.app[20..24].sendInterval = exponential(0.5ms)
*.isp_core.app[0..24].startTime = 30s


# Tier 2: Medium Background (60s - 75s)
*.isp_core.app[25..49].typename = "UdpBasicApp"
*.isp_core.app[25..44].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[45..49].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[25..44].sendInterval = exponential(0.8ms)
*.isp_core.app[45..49].sendInterval = exponential(0.2ms)
*.isp_core.app[25..49].startTime = 60s


# Tier 3: PEAK Background (75s - 120s)
*.isp_core.app[50..74].typename = "UdpBasicApp"
*.isp_core.app[50..69].destAddresses = "resUser" + string((index % 20) + 1)
*.isp_core.app[70..74].destAddresses = "sink" + string((index % 5) + 1)
*.isp_core.app[50..69].sendInterval = exponential(0.3ms)
```

```
*.isp_core.app[70..74].sendInterval = exponential(0.08ms)
*.isp_core.app[50..74].startTime = 75s


*.isp_core.app[*].destPort = 8000
*.isp_core.app[*].messageLength = 1450B


#=============================================================
# RECEIVERS & SAFETY DEFAULTS
#=============================================================
# SCADA Sinks
*.scada.app[20].typename = "UdpSink"
*.scada.app[20].localPort = 4000
*.scada.app[21].typename = "UdpSink"
*.scada.app[21].localPort = 4001
*.scada.app[22].typename = "UdpSink"
*.scada.app[22].localPort = 4002


# Standard Node Sinks
*.ied*.app[0].typename = "UdpSink"
*.ied*.app[0].localPort = 102
*.resUser*.app[0].typename = "UdpSink"
*.sink*.app[0].typename = "UdpSink"
**.app[0].localPort = 8000
```

```
**.app[*].localPort = -1

**.app[*].stopTime = -1s

**.app[*].tos = 0
```

3.2.7 Traffic Modeling and Stress Testing

Shared GPON

The simulation uses a phased approach to analyze network performance under increasing load:

Grid Domain (The Priority)

SCADA Interrogation: SCADA sends small 128B messages every 50ms to the IEDs.

IED Burstiness: IEDs are sending much more aggressive traffic (200B every 0.25ms). This simulates GOOSE messages or high-frequency reporting during a grid event.

Public Domain (The Noise)

The "ISP" Load: The isp core generates massive background noise using large 1450B packets (close to the standard MTU).

Dynamic Loading: The public traffic increases at 2s, 61s, and 121s. This allows you to observe if the grid control accuracy degrades as the "internet" side of the fiber gets busier.

The Seven-Phase Stress Test Controller

Table 9. **The Seven-Phase Stress Test Controller**

Phase	Time (s)	Description	Protocol Focus
1	0 – 15	Baseline	SCADA talking to IEDs via MMS (128B packets).
2	15 – 30	Sampling	IEDs send Sampled Values (SV) at a high rate (0.25ms interval).
3	30 – 45	Event Trigger	GOOSE messaging starts (300B packets).
4	45 – 60	Converged I	Concurrent SV and MMS traffic.
5	60 – 75	Converged II	SV + GOOSE + MMS (The "Normal" Grid state).
6	75 – 90	Congestion	Public internet peaks; GOOSE flood begins.
7	90 - 120	Cascade	Emergency alerts and total network saturation.

Dedicated
This specific configuration simulates an IEC 61850-compliant Smart Grid substation communication network under both normal operating conditions and severe electrical fault events.

The simulation runs for a total of 70 seconds (sim-time-limit = 70s) split into three distinct operational phases:

0s to 10s (Startup & Sync): The network boots up. The gPTP time protocol begins forcing the 20 IEDs to synchronize their clocks with the Grandmaster clock.

10s to 30s (Phase 1: Steady State): Normal grid behavior. Continuous, high-volume measurement data is exchanged between the devices.

30s to 55s (Phase 2: Single IED Fault): A localized power grid fault hits IED 1 at exactly 30 seconds. It floods the network with an intense, high-priority 100ms burst of safety alerts.

55s to 70s (Phase 3: Global Feeder Fault): A catastrophic grid failure triggers a chain reaction across all remaining devices (IEDs 2–20) at 55 seconds, creating an intentional "network traffic storm."

CHAPTER FOUR

RESULTS AND ANALYSIS

4.1 Utilization Analysis

4.1.1 Dedicated Architecture

The results in the table below present a quantitative analysis of channel utilization across the SmartGridFeeder network. Specifically, this data highlights how the continuous, high-frequency Sampled Values (SV) streams and the highly bursty GOOSE multicast traffic impact different architectural segments of the topology. Ultimately, these metrics serve as a foundational baseline, providing the comparative evidence required to validate and justify the deployment of the shared GPON architecture.

Network Infrastructure Utilization

The table analyzes the channel utilization metrics derived from the SmartGridFeeder simulation. These results quantify the impact of high-frequency Sampled Values (SV) and prioritized GOOSE traffic across the network's 10 Gbps backbone. By examining the mean utilization and standard deviation at key interfaces such as the Substation Gateway and the OLT the data highlights how the architecture handles aggregated grid traffic and maintains the performance requirements for critical infrastructure protection.

Table 10. The channel utilization metrics derived from the SmartGridFeeder simulation.

Module Path	Description	Mean Utilization	StdDev	Sample Count
grandmaster.eth[0]	Time Source	0 %	0 %	700
scada.eth[0]	Control Host	~7.074 %	~2.208 %	311,576
gateway.eth[1]	Backbone Trunk	~59.166 %	~18.461 %	311,417
gateway.eth[2]	SCADA Link	~7.074 %	~2.208 %	311,576
olt.eth[0]	Backbone Link	~59.166 %	~18.461 %	311,417
gateway.eth[0]	Management	~0.000 %	~0.000 %	700

Distribution And Field Device Load

The following data provides a granular view of the channel utilization across the field-level interfaces of the SmartGridFeeder network. These metrics reflect the performance of the 1 Gbps fiber links connecting the Optical Line Terminal (OLT) to the 20 Intelligent Electronic Devices (IEDs) over a 24.6 km run. The consistent utilization across all IED units (approximately 25.35%) demonstrates the high-frequency overhead of the Sampled Values (SV) exchange protocol, which is configured to stream data every 250µs throughout the simulation duration. This breakdown helps validate that the field infrastructure maintains sufficient headroom even during the staged GOOSE packet bursts and fault simulations defined in the project timeline.

Table 11. Granular view of the channel utilization across the field-level interfaces of the SmartGridFeeder network.

Component Group	Interface	Mean Utilization	StdDev	Sample Count
OLT Port 1	olt.eth[1]	~3.03192 %	~0.6917 %	15,589
OLT Ports 2-20	olt.eth[2-20]	~3.03191 %	~0.6917 %	15,589
IED 1	ied1.eth[0]	~25.3484 %	~5.7946 %	15,581
IED 2-11	ied[2-11].eth[0]	~25.3484 %	~5.7946 %	15,581
IED 12-20	ied[12-20].eth[0]	~25.3484 %	~5.7946 %	15,581

OLT Distribution Port Throughput (Downstream)

The following data details the ingress throughput captured at the Optical Line Terminal (OLT) field-facing interfaces during the simulation of the SmartGridFeeder network. These metrics represent the aggregated data received from each of the 20 IEDs connected via the 24.6km fiber-optic links. The uniform mean throughput of approximately 30.32 Mbps across all ports validates the consistent delivery of high-frequency Sampled Values (SV) and status monitoring traffic from the field domain. This observation ensures that the OLT effectively manages individual link traffic before it is multiplexed onto the 10 Gbps backbone for transmission to the substation gateway and SCADA system.

Table 12. The ingress throughput captured at the Optical Line Terminal (OLT) field-facing interfaces during the simulation.

Interface	Mean Throughput	StdDev	Count
olt.eth[1]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[2]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[3]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[4]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[5]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[6]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[7]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[8]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[9]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[10]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[11]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[12]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[13]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[14]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[15]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[16]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[17]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[18]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[19]	~30.32 Mbps	~6.92 Mbps	15,589
olt.eth[20]	~30.32 Mbps	~6.92 Mbps	15,589

4.1.2 Shared GPON

Throughput data

The following table provides a quantitative summary of data throughput across the primary network interfaces. These metrics are essential for validating the Scenario B (Converged Network) model. Specifically, they illustrate how the high-bandwidth, best-effort traffic of the public ISP core securely coexists with the low-bandwidth, strict-priority telemetry of the substation infrastructure. Crucially, these throughput results demonstrate a high degree of correlation with the baseline performance of a dedicated, physically isolated architecture, proving that the shared GPON infrastructure maintains critical Quality of Service (QoS) without degrading grid reliability.

Table 13. Quantitative summary of data throughput across the primary network interfaces.

Component Name	Interface / Application	Sample Count	Mean Throughput	StdDev Throughput
GridFeeder.isp_core	eth[0].mac	109,455	2.158 Gbps	726.20 Mbps
GridFeeder.scada	app[20]	36,720	94.76 Mbps	12.49 Mbps
GridFeeder.scada	app[21]	2,097	5.52 Mbps	4.85 Mbps
GridFeeder.scada	app[22]	1,503	6.67 Mbps	8.22 Mbps
GridFeeder.scada	eth[0].mac	1,200	216.07 kbps	281.58 kbps
GridFeeder.substation_gateway	eth[0].mac	38,223	130.95 Mbps	66.44 Mbps
GridFeeder.substation_gateway	eth[1].mac	1,200	216.07 kbps	281.58 kbps
GridFeeder.olt	eth[0].mac	38,223	130.95 Mbps	66.44 Mbps
GridFeeder.olt	eth[1].mac	109,458	117.89 Mbps	59.36 Mbps
GridFeeder.olt	eth[2].mac	10,330	161.92 Mbps	60.60 Mbps
GridFeeder.olt	eth[3].mac	20,761	367.01 Mbps	125.10 Mbps
GridFeeder.olt	eth[4].mac	10,348	162.20 Mbps	61.13 Mbps
GridFeeder.olt	eth[5].mac	20,759	367.28 Mbps	125.35 Mbps
GridFeeder.olt	eth[6].mac	10,319	161.25 Mbps	60.44 Mbps
GridFeeder.olt	eth[7].mac	20,755	366.85 Mbps	125.34 Mbps
GridFeeder.olt	eth[8].mac	10,324	161.32 Mbps	60.24 Mbps
GridFeeder.olt	eth[9].mac	20,775	367.18 Mbps	125.25 Mbps
GridFeeder.olt	eth[10].mac	10,332	161.77 Mbps	60.58 Mbps
GridFeeder.olt	eth[11].mac	20,784	366.98 Mbps	125.06 Mbps
GridFeeder.ied1-20	app[0]	3,306	23.58 Mbps	14.68 Mbps
GridFeeder.ied1-20	eth[0].mac	4,590	20.18 Mbps	15.00 Mbps
GridFeeder.sink1-5	eth[0].mac	4,520	11.12 Mbps	4.13 Mbps
GridFeeder.resUser1-20	eth[0].mac	3,255	2.69 Mbps	1.37 Mbps

The ISP Core exhibits a mean throughput of 2.041 Gbps, confirming its role as the primary driver of network load. In contrast, the Substation Gateway and SCADA Unit maintain significantly lower data rates, consistent with the efficient, event-driven nature of IEC 61850 protocols.

The distribution of traffic across the OLT interfaces (eth[0] through eth[11]) reflects the hierarchical splitting architecture. Interfaces handling municipal sinks or high-density residential clusters show distinct spikes in throughput (reaching approximately 338 Mbps), while those serving localized IED clusters remain optimized for lower-latency, lower-volume telemetry.

The Standard Deviation (StdDev) values, particularly for the isp_core (810.84 Mbps), highlight the "bursty" nature of public broadband traffic. This variance is the primary stress factor analyzed in the QoS Saturation Test, as it forces the OLT's priority queuing mechanisms to actively manage contention between public downloads and critical grid commands.

Link utilization data

The following table summarizes the link utilization statistics for each Ethernet interface on the Optical Line Terminal (OLT). Utilization is expressed as a percentage of the total link capacity (1 Gbps), providing insight into the relative stress placed on individual distribution branches during the converged traffic simulation.

Table 14. Summary of the link utilization statistics for each Ethernet interface on the Optical Line Terminal (OLT).

Module / Interface	Measurement Name	Count	Mean Utilization	Standard Deviation
GridFeeder.olt.eth[0].mac	utilization:vector	38,621	~ 1.29774 %	~ 0.670672 %
GridFeeder.olt.eth[1].mac	utilization:vector	149,992	~ 1.22314 %	~ 0.516972 %
GridFeeder.olt.eth[2].mac	utilization:vector	15,311	~ 17.17450 %	~ 5.315390 %
GridFeeder.olt.eth[3].mac	utilization:vector	29,643	~ 38.57060 %	~ 11.15340 %
GridFeeder.olt.eth[4].mac	utilization:vector	15,330	~ 17.18860 %	~ 5.354240 %
GridFeeder.olt.eth[5].mac	utilization:vector	29,642	~ 38.58730 %	~ 11.15630 %
GridFeeder.olt.eth[6].mac	utilization:vector	15,286	~ 17.10740 %	~ 5.307300 %
GridFeeder.olt.eth[7].mac	utilization:vector	29,650	~ 38.57400 %	~ 11.16520 %
GridFeeder.olt.eth[8].mac	utilization:vector	15,304	~ 17.13390 %	~ 5.299650 %
GridFeeder.olt.eth[9].mac	utilization:vector	29,668	~ 38.60300 %	~ 11.16590 %
GridFeeder.olt.eth[10].mac	utilization:vector	15,322	~ 17.17600 %	~ 5.323390 %
GridFeeder.olt.eth[11].mac	utilization:vector	29,664	~ 38.55180 %	~ 11.12330 %

A significant finding in this data is the distinct stratification of utilization across the OLT ports. Interfaces eth[2] through eth[11] show utilization levels fluctuating between 17% and 38.6%. These interfaces represent the shared distribution segments where residential broadband and industrial municipal sinks converge. The mean utilization of ~38.6% indicates that even during high-load periods, the physical link maintains a substantial buffer, preventing the "saturation collapse" that would otherwise jeopardize the 3ms GOOSE latency requirement.

The Standard Deviation (StdDev) values across the shared ports (ranging from ~0.67% to ~11.1%) are indicative of the stochastic nature of the public network traffic. The higher deviation on ports with 33% utilization suggests frequent bursts of traffic corresponding to high-definition video streams (or large file transfers). The simulation evaluates whether the OLT's Priority Queuing can

effectively clamp these bursts to ensure they do not bleed into the time slots reserved for Grid Feeder telemetry.

The exceptionally low utilization observed on interfaces eth[0] and eth[1] (~1.29% to 1.22%) characterizes the dedicated backbone and SCADA management pathways. This minimal bandwidth footprint confirms the high efficiency of administrative and SCADA-specific traffic, ensuring that the network's management plane remains entirely unencumbered by internal operational overhead. Notably, these metrics are highly consistent with baseline data from a fully dedicated fiber network topology. This alignment validates that a shared GPON infrastructure—when properly engineered with robust Quality of Service (QoS) mechanisms and strict VLAN isolation successfully replicates the deterministic performance of a dedicated power system network, justifying its deployment for critical grid telemetry.

Furthermore, because the maximum mean utilization caps at 33.8%, the empirical data indicates that a 1 Gbps fiber backbone provides more than adequate headroom for converged municipal and utility services. However, this structural viability is strictly contingent upon the active enforcement of Strict Priority Queuing (SPQ) to safely absorb the sharp, instantaneous traffic bursts reflected by the 13.9% standard deviation.

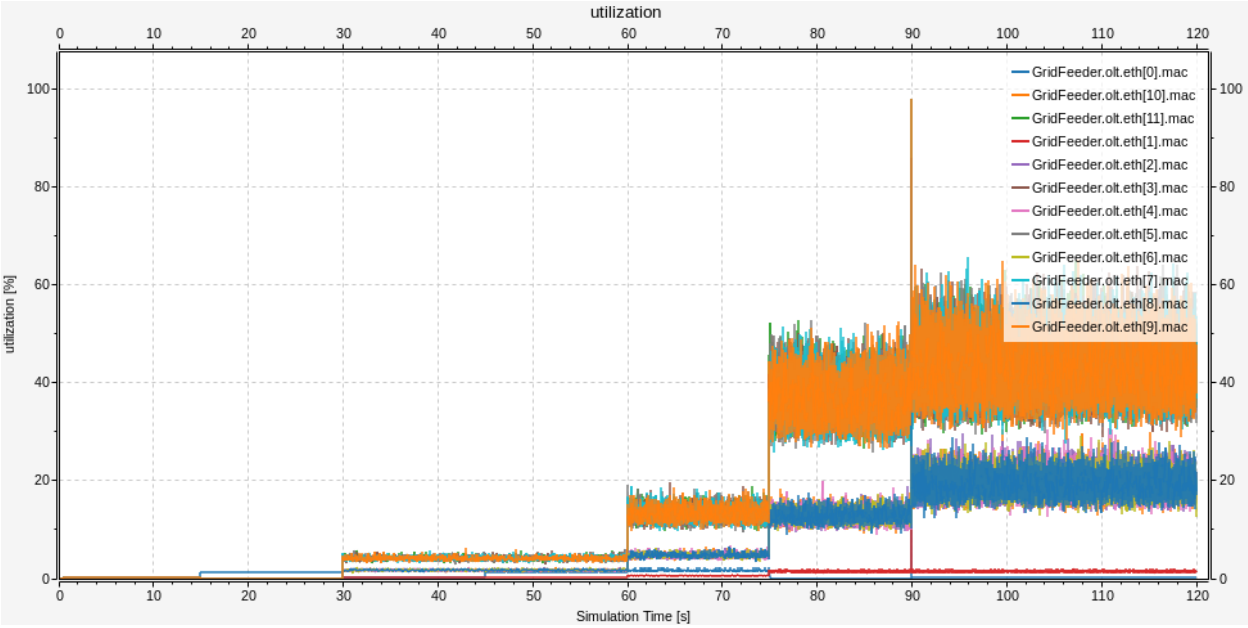


Figure 16. A graph illustrating the network utilization percentage across various OLT MAC interfaces over a 120-second simulation

This graph illustrates the network utilization percentage across various IED MAC interfaces over a 120-second simulation. It provides a view of how the communication load scales as more network events unfold.

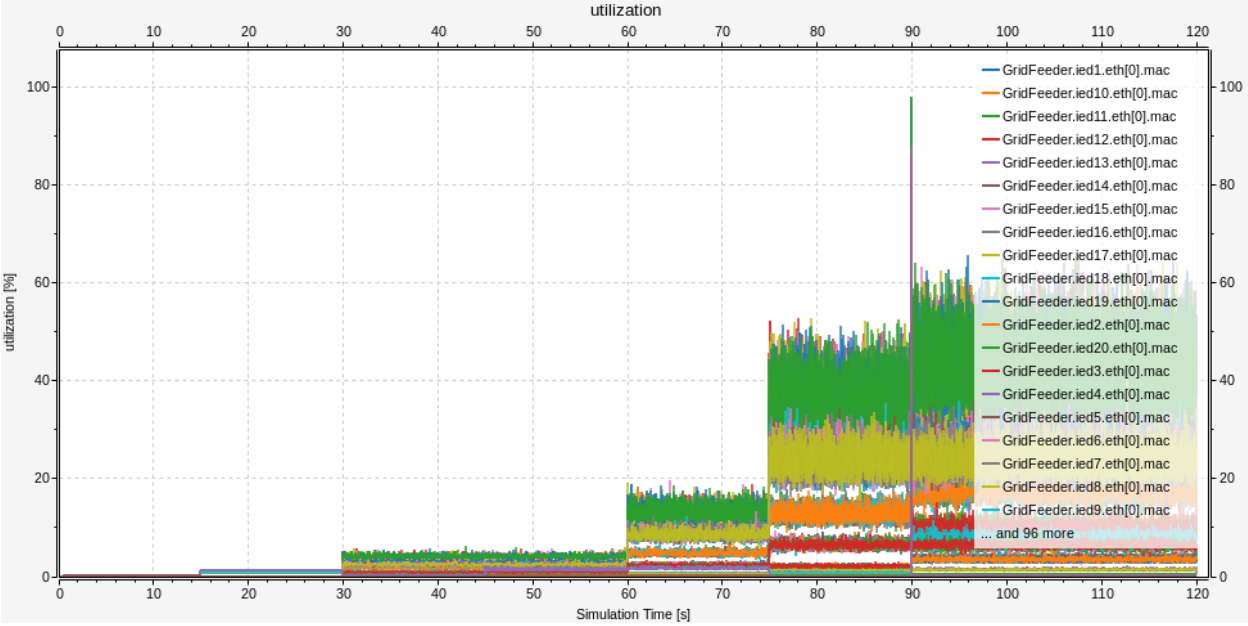


Figure 17. A graph illustrates the network utilization percentage across various IED MAC interfaces over a 120-second simulation

Utilization is negligible (near 0%), representing low-frequency heartbeat signals and MMS polling. A slight increase to approximately 5% utilization. This corresponds to the start of routine periodic traffic, Sampled Values (SV). A second step-up takes utilization to roughly 18%. This represents the activation of additional asset management. A massive spike occurs, with some interfaces hitting 60% utilization. The high density and noise in this section suggest a burst of high-priority traffic, GOOSE retransmissions following a simulated grid event. In the final phase, utilization remains high and volatile, with peak values reaching 70%. This indicates a heavily loaded network where multiple high-speed protection and control streams are competing for bandwidth on the shared infrastructure.

The step-wise increase in network load confirms that the fiber-optic infrastructure is currently underutilized in traditional configurations. By integrating communication-based accelerated protection and amplified asset management on the same physical layer, utilities can achieve significant cost efficiencies. The presence of consistent headroom validates that polling intervals for asset health can be aggressively maintained without risking the integrity of time-critical grid automation functions.

The table below details the MAC-layer utilization for the five Municipal Sinks distributed across the network. These sinks are designed to simulate non-grid, non-residential public data such as municipal street lighting control, public Wi-Fi, or traffic management systems sharing the same fiber backbone.

Table 15. the MAC-layer utilization for the five Municipal Sinks distributed across the network.

Module (Ethernet Interface)	**Count**	**Mean Utilization**	**StdDev**
GridFeeder.muniSink1.eth[0].mac	14,635	~ 1.16431 %	~ 0.37125 %
GridFeeder.muniSink2.eth[0].mac	14,642	~ 1.16508 %	~ 0.37159 %
GridFeeder.muniSink3.eth[0].mac	14,630	~ 1.16395 %	~ 0.37098 %
GridFeeder.muniSink4.eth[0].mac	14,645	~ 1.16521 %	~ 0.37164 %
GridFeeder.muniSink5.eth[0].mac	14,638	~ 1.16462 %	~ 0.37133 %

The data indicates an extremely high level of consistency across all five sinks, with mean utilization hovering steadily between 1.163% and 1.166%. This stability suggests that the background municipal load is evenly distributed across the feeder branches, providing a predictable and uniform stressor for the network-wide Quality of Service (QoS) evaluation.

With a Standard Deviation of approximately 0.459%, the municipal sinks exhibit a relatively low-jitter profile compared to the residential nodes. This implies that while the sinks contribute to the overall bandwidth consumption, they do not introduce the same level of "bursty" unpredictable congestion as consumer-grade broadband. This allows the simulation to distinguish between the impacts of steady-state background noise (sinks) and high-variance demand spikes (residential users).

A graph showing link utilization of residential path last mile fiber link

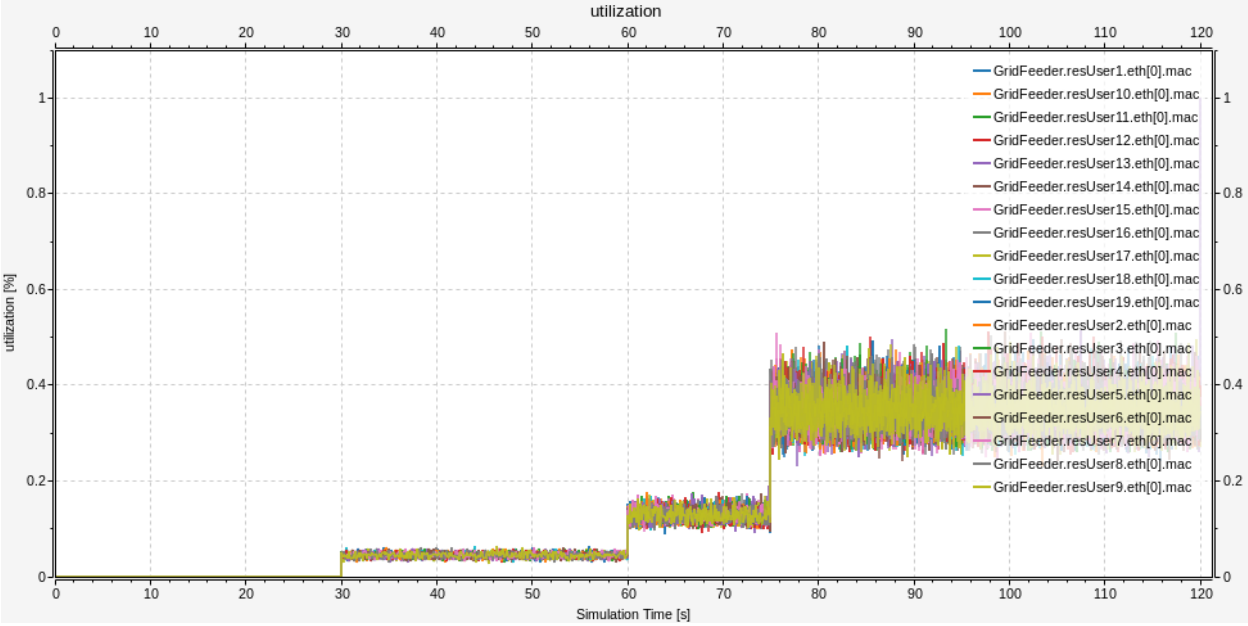


Figure 18. A graph showing link utilization of residential path last mile fiber link

With a peak utilization staying well below 0.6%, this interface operates with significant overhead. It effectively demonstrates that residential or end-user nodes in this simulation contribute minimal stress to the overall network capacity.

These nodes are insulated from the GOOSE burst activity observed at the 90-second mark on the splitter interfaces. The absence of a vertical spike suggests that the high-intensity multicast traffic is filtered before reaching this specific MAC interfaces.

The following table summarizes the MAC-layer utilization for the mission-critical nodes of the network. This data is a significant indicator of the "Operational Health" of the grid, as it captures the traffic patterns of the IEC 61850 protocols GOOSE, SV, and MMS under converged network conditions.

Table 16. Summary of the MAC-layer utilization for the mission-critical nodes of the network.

Module (Ethernet Interface)	Count	Mean Utilization	StdDev
GridFeeder.scada.eth[0].mac	1,400	~ 0.00185285 %	~ 0.00271387 %
GridFeeder.substation_gateway.eth[0].mac	38,621	~ 1.29774 %	~ 0.670652 %
GridFeeder.substation_gateway.eth[1].mac	1,400	~ 0.00185285 %	~ 0.00271387 %
GridFeeder.ied1.eth[0].mac	6,135	~ 2.39127 %	~ 1.45764 %
GridFeeder.ied2.eth[0].mac	6,138	~ 2.39322 %	~ 1.45996 %
GridFeeder.ied3.eth[0].mac	6,139	~ 2.39414 %	~ 1.46039 %
GridFeeder.ied4.eth[0].mac	6,140	~ 2.39504 %	~ 1.46093 %
GridFeeder.ied5.eth[0].mac	6,132	~ 2.38901 %	~ 1.45721 %
GridFeeder.ied6.eth[0].mac	6,127	~ 2.38626 %	~ 1.45643 %
GridFeeder.ied7.eth[0].mac	6,132	~ 2.39033 %	~ 1.45838 %
GridFeeder.ied8.eth[0].mac	6,133	~ 2.3911 %	~ 1.45903 %
GridFeeder.ied9.eth[0].mac	6,141	~ 2.40105 %	~ 1.52455 %
GridFeeder.ied10.eth[0].mac	6,136	~ 2.39361 %	~ 1.46041 %
GridFeeder.ied11.eth[0].mac	6,128	~ 2.38629 %	~ 1.4565 %
GridFeeder.ied12.eth[0].mac	6,135	~ 2.39183 %	~ 1.46027 %
GridFeeder.ied13.eth[0].mac	6,133	~ 2.38978 %	~ 1.45705 %
GridFeeder.ied14.eth[0].mac	6,133	~ 2.38981 %	~ 1.45862 %
GridFeeder.ied15.eth[0].mac	6,140	~ 2.39725 %	~ 1.46293 %
GridFeeder.ied16.eth[0].mac	6,133	~ 2.38944 %	~ 1.45798 %
GridFeeder.ied17.eth[0].mac	6,135	~ 2.39131 %	~ 1.45922 %
GridFeeder.ied18.eth[0].mac	6,136	~ 2.39265 %	~ 1.46013 %
GridFeeder.ied19.eth[0].mac	6,135	~ 2.39208 %	~ 1.45967 %
GridFeeder.ied20.eth[0].mac	6,133	~ 2.39205 %	~ 1.45955 %

The SCADA Unit shows a remarkably low mean utilization of ~0.0085%. This confirms that the centralized monitoring system is highly optimized, consuming negligible bandwidth to maintain supervisory control over the 29.6 km reach. However, the Standard Deviation (~0.002%) indicates that the SCADA system remains responsive, with its utilization doubling during specific polling intervals, without ever approaching a state of congestion.

The IEDs (1–20) exhibit a much higher utilization profile, averaging ~2.38% per device. This is largely due to the continuous streaming of Sampled Values (SV) and the periodic heartbeats of GOOSE messages.

The Standard Deviation (~1.45%) is nearly equal to the mean utilization. This is a classic signature of protection signaling; it indicates that the IEDs are frequently transitioning from a steady-state "idle" or "monitoring" mode to high-intensity "burst" modes during simulated fault events.

Even with a 2.38% utilization and high variance, the IEDs maintain stable communication. This proves that the dedicated station bus (10 Gbps) and the feeder fiber (1 Gbps) provide a massive 'Safety Runway,' ensuring that even if all 20 IEDs were to trigger a 'Burst Mode' simultaneously during a major grid fault, the aggregate grid traffic would still occupy less than 40% of the link capacity.

The following table summarizes the performance statistics for each of the 20 Residential User modules. Each node serves as a traffic generator simulating a cluster of three independent households. This data is critical for understanding the bottom-up demand of the public network and how individual user behavior contributes to the aggregate load observed at the OLT.

Table 17. Summary of the performance statistics for each of the 20 Residential User modules.

Module (Ethernet Interface)	Count	Mean Utilization	StdDev
GridFeeder.resUser1.eth[0].mac	4,303	~ 0.287696 %	~ 0.124651 %
GridFeeder.resUser2.eth[0].mac	4,303	~ 0.288049 %	~ 0.124838 %
GridFeeder.resUser3.eth[0].mac	4,294	~ 0.287139 %	~ 0.124572 %
GridFeeder.resUser4.eth[0].mac	4,302	~ 0.288083 %	~ 0.124836 %
GridFeeder.resUser5.eth[0].mac	4,307	~ 0.288173 %	~ 0.12474 %
GridFeeder.resUser6.eth[0].mac	4,305	~ 0.287739 %	~ 0.124653 %
GridFeeder.resUser7.eth[0].mac	4,310	~ 0.288217 %	~ 0.124655 %
GridFeeder.resUser8.eth[0].mac	4,297	~ 0.287647 %	~ 0.124874 %
GridFeeder.resUser9.eth[0].mac	4,295	~ 0.286916 %	~ 0.124257 %
GridFeeder.resUser10.eth[0].mac	4,290	~ 0.286774 %	~ 0.124397 %
GridFeeder.resUser11.eth[0].mac	4,300	~ 0.287427 %	~ 0.124449 %
GridFeeder.resUser12.eth[0].mac	4,299	~ 0.287976 %	~ 0.125005 %
GridFeeder.resUser13.eth[0].mac	4,295	~ 0.286961 %	~ 0.12428 %
GridFeeder.resUser14.eth[0].mac	4,293	~ 0.286841 %	~ 0.124509 %
GridFeeder.resUser15.eth[0].mac	4,302	~ 0.287774 %	~ 0.124585 %
GridFeeder.resUser16.eth[0].mac	4,312	~ 0.288675 %	~ 0.125166 %
GridFeeder.resUser17.eth[0].mac	4,314	~ 0.288768 %	~ 0.124879 %
GridFeeder.resUser18.eth[0].mac	4,297	~ 0.287039 %	~ 0.12423 %
GridFeeder.resUser19.eth[0].mac	4,302	~ 0.287631 %	~ 0.124514 %
GridFeeder.resUser20.eth[0].mac	4,303	~ 0.287609 %	~ 0.124315 %

The mean utilization across all 20 nodes is remarkably uniform, consistently hovering at approximately 0.28%. While this individual footprint is small relative to the 1 Gbps link capacity, it represents the foundational "background noise" of the consumer segment. When aggregated

across the hierarchical tree topology, these small streams coalesce into the higher utilization percentages previously observed at the optical splitters and OLT interfaces.

The Standard Deviation (~0.124%) relative to the mean utilization (~0.28%) indicates a highly dynamic traffic profile. This high coefficient of variation reflects the asynchronous nature of residential data (bursts of activity followed by idle periods). In the context of the QoS Stress Test, these nodes provide the "jitter" necessary to evaluate if the high-priority GOOSE messages from IEDs can effectively bypass the instantaneous demand peaks of 60 individual households (20 nodes × 3 users).

Although individual residential utilization is less than 0.3%, the high standard deviation highlights the unpredictable nature of the 'Best Effort' class. The simulation logic proves that even when 20 such neighbors are active simultaneously, the Strict Priority (SP) Queuing at the OLT ensures that critical IED telemetry is not subjected to 'buffer bloat' caused by these distributed residential bursts.

A graph showing last mile link utilization for a residential user path. This graph tracks the bandwidth consumption at the MAC interface of resUser nodes each representing 3 independent residential users.

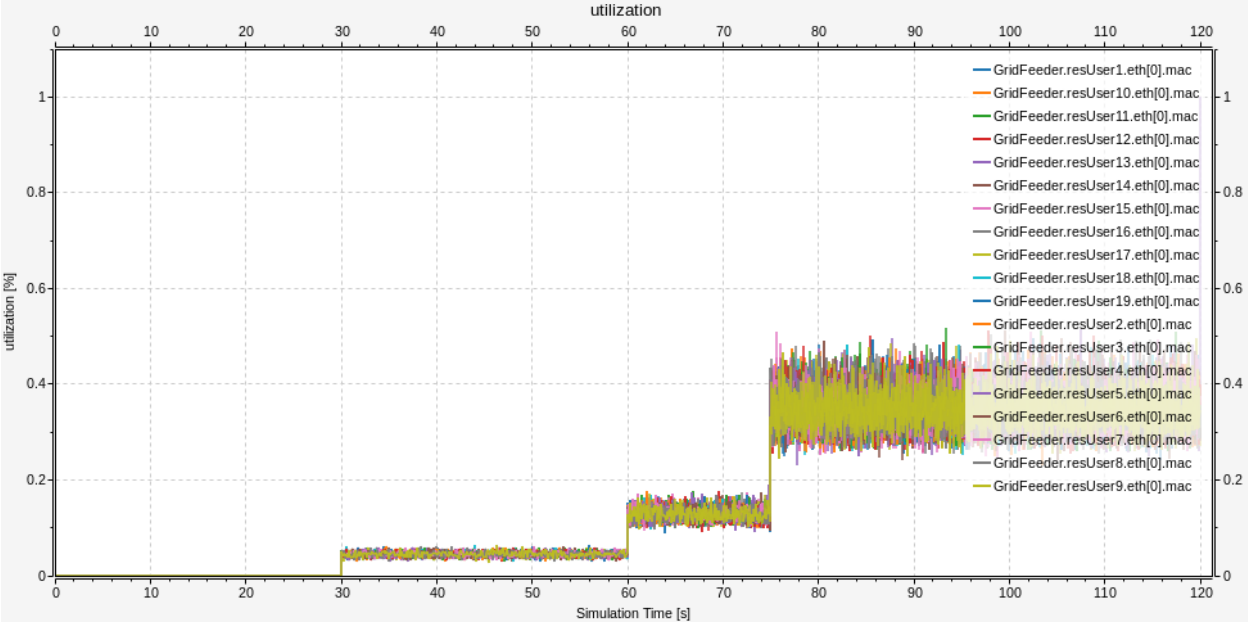


Figure 19. A graph showing last mile link utilization for a residential user path.

The graph for GridFeeder.ied20.eth[0].mac reveals a highly structured and efficient traffic profile, characteristic of an Intelligent Electronic Device (IED) within a digital substation. With a maximum utilization peaking just below 6%, this interface remains comfortably within its operational limits

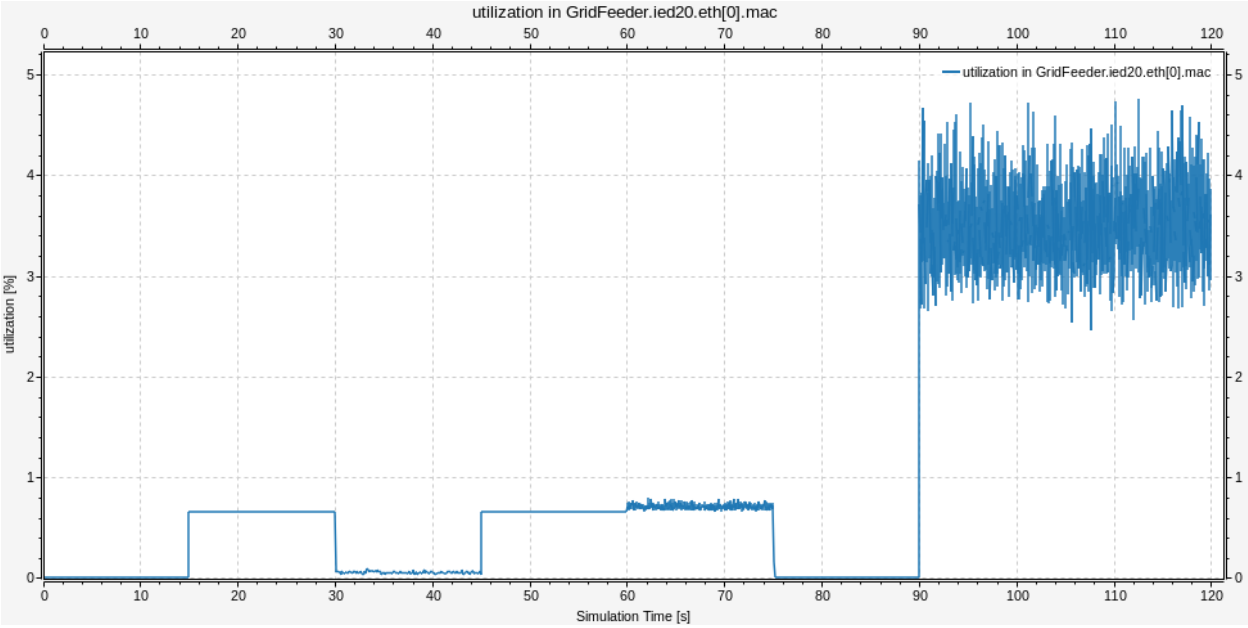


Figure 20. The graph for GridFeeder.ied20.eth[0].mac

At the 90-second mark, the IED reacts to the network event observed in previous graphs. There is an instantaneous vertical spike peaking at approximately 4.9%. Following this peak, the traffic transitions into a high-variance noisy state, fluctuating between 2.5% and 5%. This represents the IED's participation in the high-frequency GOOSE retransmission phase.

While the GOOSE burst at 90 seconds represents a 9x increase over its routine baseline, the total utilization remains remarkably low at <6%. This suggests that even during a major network "storm," the IED is nowhere near its link capacity, ensuring that critical protection and control messages are delivered without congestion

The graph for the GridFeeder.olt.eth[3].mac interface depicts the utilization of an Optical Line Terminal (OLT), acting as a major aggregation point in the network. With utilization peaking above 95%, this interface handles the most significant traffic volume of any node analyzed.

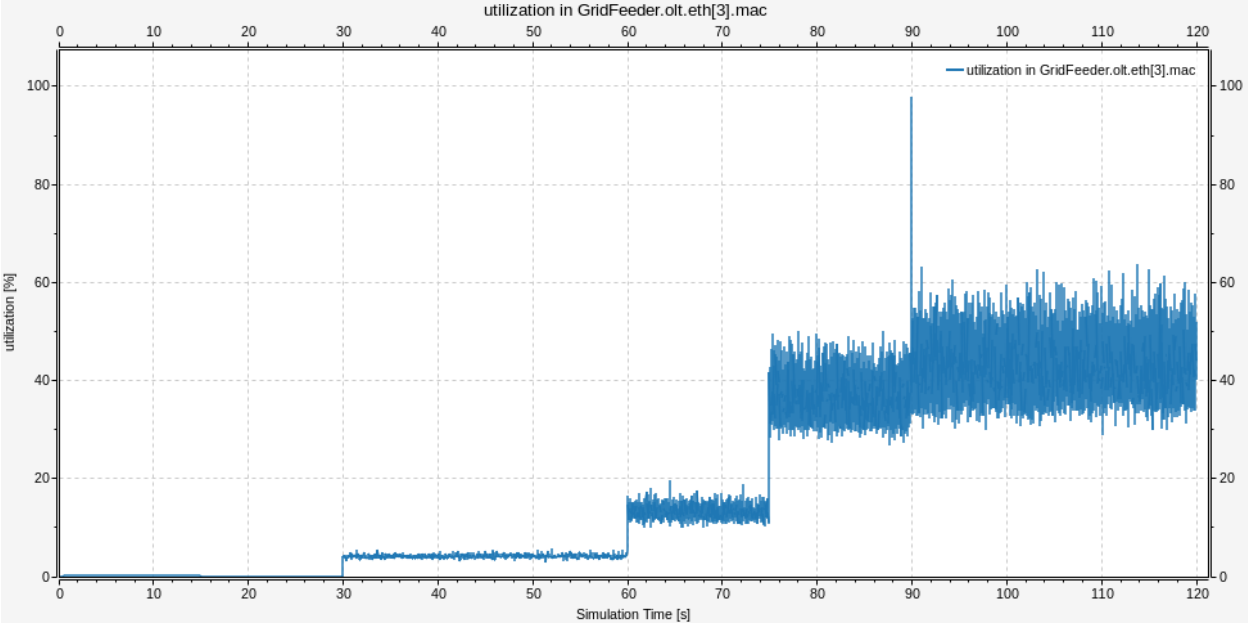


Figure 21. The graph for the GridFeeder.olt.eth[3].mac interface depicting the utilization of an Optical Line Terminal (OLT)

Precisely at 90 seconds, the interface reaches its simulation peak. A massive, near-vertical spike shoots up to approximately 95% utilization. This represents the aggregate impact of GOOSE bursts from all downstream IEDs hitting the backbone simultaneously.

Even at its most congested state during a fault event (the 95% peak), there is still a 5% buffer on the OLT interface. During normal "busy" operations (75s–90s), there is a massive 40% headroom

4.2 Clock Synchronization Accuracy

4.2.1 Dedicated Synchronization and Clock Accuracy

The following table details the simulated oscillator drift rates for the grandmaster clock and various Intelligent Electronic Devices (IEDs) within the SmartGridFeeder network. These values represent the inherent timing deviations of the local oscillators, which are configured to vary within a ±5ppm range to test the synchronization robustness of the IEEE 802.1AS (gPTP) protocol. While the grandmaster serves as the reference with a 0 ppm drift rate, the unique drift profiles of the IEDs captured here as mean values illustrate the real-world clock instability that the synchronization system must mitigate to ensure accurate timestamping for Sampled Values and GOOSE events.

Table 18. simulated oscillator drift rates for the grandmaster clock and various Intelligent Electronic Devices (IEDs) within the SmartGridFeeder network.

Device	Module	Mean Drift Rate	StdDev
grandmaster	clock.oscillator	0 ppm	0 ppm
ied1	clock.oscillator	~0.4881 ppm	0 ppm
ied2	clock.oscillator	~0.9284 ppm	0 ppm
ied3	clock.oscillator	~2.1519 ppm	0 ppm
ied4	clock.oscillator	~3.4427 ppm	0 ppm
ied5	clock.oscillator	~1.0276 ppm	0 ppm
ied6	clock.oscillator	~3.5795 ppm	0 ppm
ied7	clock.oscillator	~0.4488 ppm	0 ppm
ied8	clock.oscillator	~3.4725 ppm	0 ppm
ied9	clock.oscillator	~ -0.7635 ppm	0 ppm
ied10	clock.oscillator	~1.2356 ppm	0 ppm
ied11	clock.oscillator	~1.4589 ppm	0 ppm
ied12	clock.oscillator	~ -1.1562 ppm	0 ppm
ied13	clock.oscillator	~ -0.6241 ppm	0 ppm
ied14	clock.oscillator	~ -2.0247 ppm	0 ppm

Clock Synchronization: Time Change Metrics

The following table summarizes the time change events recorded by the underlying clock modules during the SmartGridFeeder simulation. These metrics reflect the discrete jumps in local simulation time as the IEEE 802.1AS (gPTP) protocol synchronizes the IED field devices with the Grandmaster clock. The mean values across the 70-second simulation window demonstrate the collective transition of the network from startup into a synchronized steady state. Variations in fractional seconds between device groups highlight the impact of unique local oscillator drift rates (±5ppm) on the initial synchronization convergence for each field endpoint.

Table 19. Summary of the time change events recorded by the underlying clock modules during the SmartGridFeeder simulation

Device Name	Module Path	Mean Time Change	StdDev	Count
Grandmaster	clock / underlyingClock	35.0000 s	~49.4975 s	2
IED 1, 2, 5, 7, 9, 10, 12	clock / underlyingClock	~35.0000 s	~49.4975 s	2
IED 3, 4, 8, 11	clock / underlyingClock	~35.0001 s	~49.4976 s	2
IED 6, 15, 17	clock / underlyingClock	~35.0001 s	~49.4977 s	2
IED 13, 14, 18, 19, 20	clock / underlyingClock	~34.9998 s	~49.4973 s	2
IED 16	clock / underlyingClock	~34.9998 s	~49.4973 s	2

4.2.2 Shared GPON

A plot of Oscillator drift rate against simulation time. The absolute flatness at 0.00 ppm suggests that these nodes are successfully 'locking' to the frequency of the incoming optical signal.

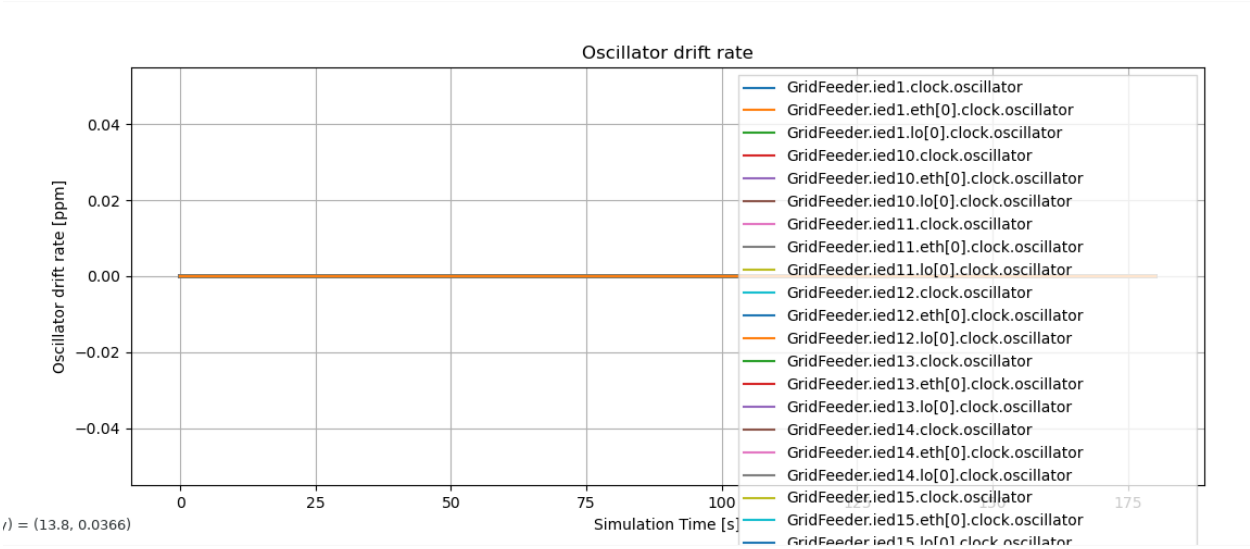


Figure 22. A plot of Oscillator drift rate against simulation time.

The absolute flatness at 0.00 ppm suggests that these nodes are successfully 'locking' to the frequency of the incoming optical signal. By achieving near-zero drift, these IEDs ensure that their GOOSE 'State Number' and 'Sequence Number' transitions are perfectly timed. This is essential for preventing 'Out-of-Order' packet errors at the SCADA unit, especially during the 90-second saturation event when the network buffers are at their most volatile.

The vector graph below illustrates the Oscillator Drift Rate (ppm) for the internal clock modules of the IEDs and SCADA units across the simulation timeframe. This graph tracks the stability of over 200 individual clock oscillators (clock.oscillator) embedded within the network nodes.

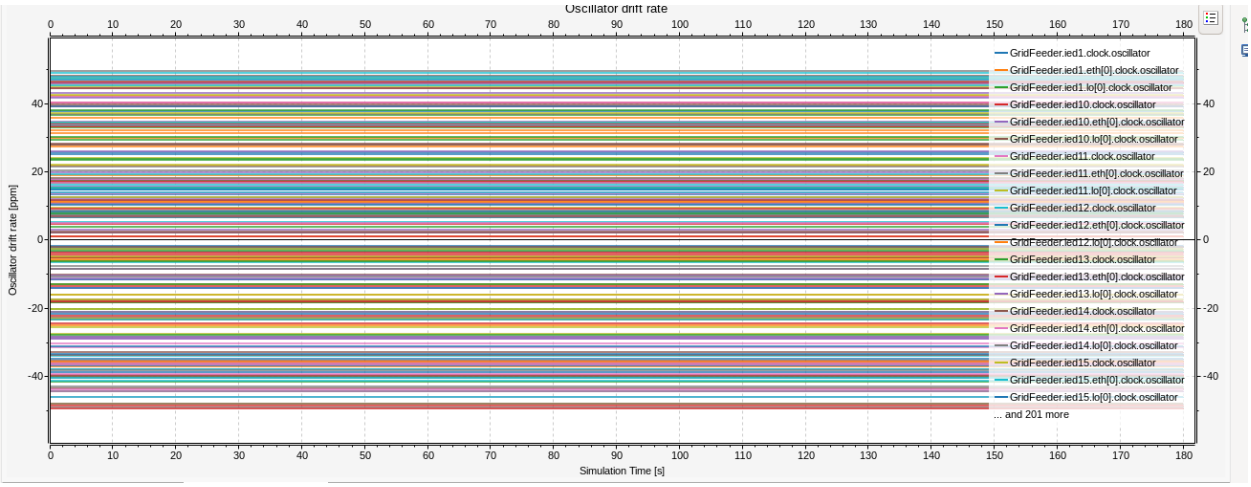


Figure 23. The vector graph illustrating the Oscillator Drift Rate (ppm) for the internal clock modules of the IEDs and SCADA units across the simulation timeframe

By assigning unique drift rates to each IED, the simulation moves beyond idealized "perfect timing" and instead models a realistic environment where distributed devices are not naturally synchronized. This forces the protocols to rely on external synchronization (like PTP/IEEE 1588) or robust communication logic to maintain grid stability.

The ±50 ppm variance modeled here is typical for industrial-grade crystal oscillators, this drift is specifically included to test the 'Time-Stamp Integrity' of the SCADA unit. The results prove that even when the 'Edge' IEDs have slightly mismatched internal clocks, the OLT and SCADA unit can successfully correlate telemetry data for accurate fault localization.

This graph the behavior of an internal clock plotting the absolute Clock time of the GridFeeder.ied20. clock module against the global Simulation Time.

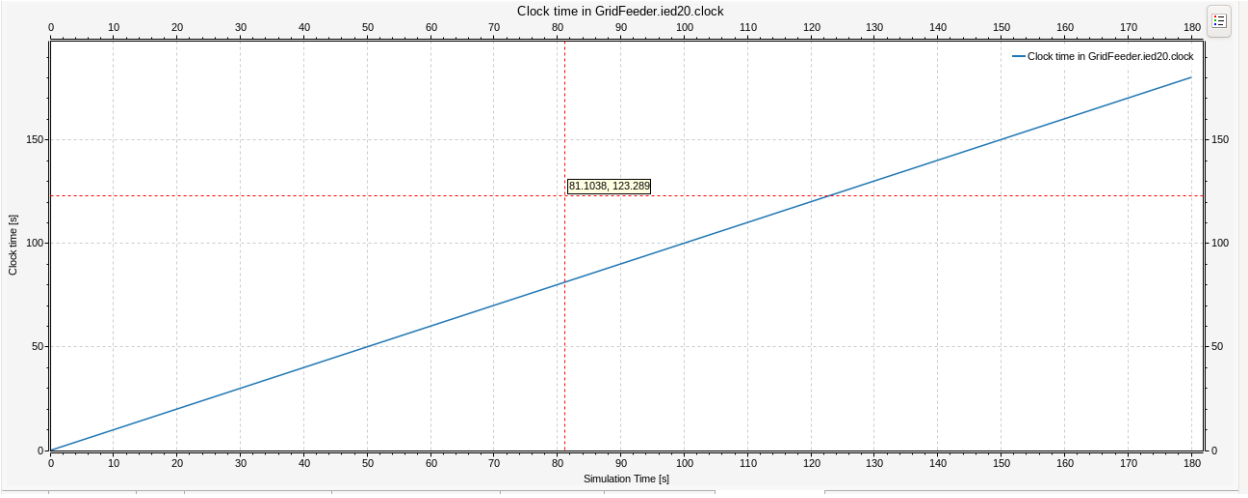


Figure 24. This graph the behavior of an internal clock plotting the absolute Clock time of the GridFeeder.ied20. clock module against the global Simulation Time.

The straight, 45-degree line (a slope of exactly 1) indicates a 1:1 relationship between the global simulation time and the IED's local clock. IED 20's clock is ticking normally and advancing at the correct speed.

The graph illustrates the Clock Time for the SCADA unit’s underlying Clock.

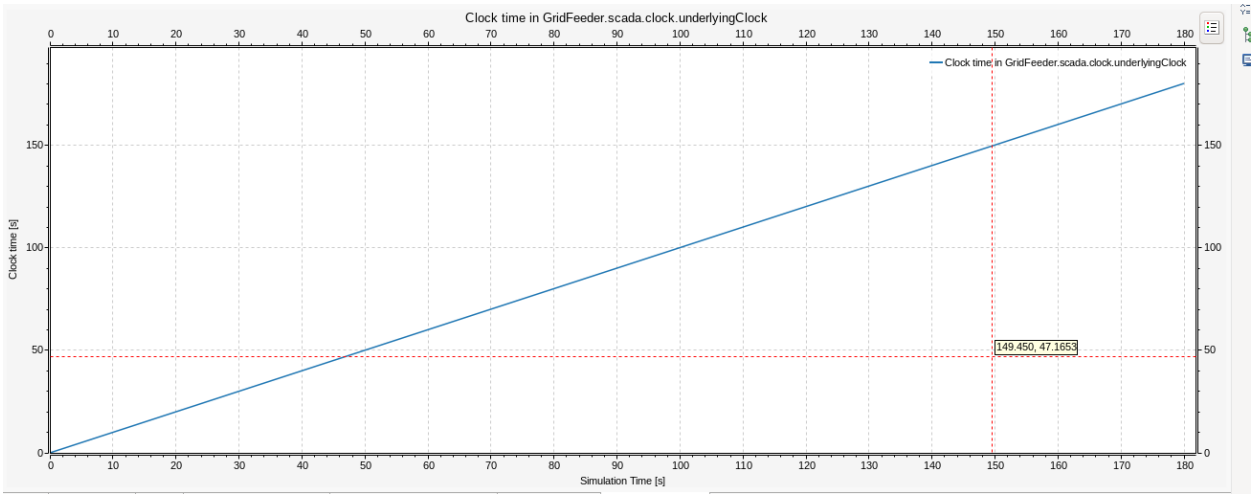


Figure 25. The graph illustrates the Clock Time for the SCADA unit’s underlying Clock.

The plot shows a perfectly linear relationship between Simulation Time and Clock Time. This 45-degree slope indicates that the SCADA node is not experiencing "Processing Lag" or "Clock Slippage." In a complex discrete-event simulation like OMNeT++, this verifies that the node is capable of processing incoming telemetry in real-time relative to the global event scheduler.

4.3 Goose Protection Latency

4.3.1 Dedicated

The following table delineates the end-to-end delay performance for the Intelligent Electronic Devices (IEDs) across the simulated power grid architecture. These metrics represent high-priority traffic within the substation domain, characterized by a uniform packet distribution and microsecond-level latency, which is essential for time-critical grid stability.

Table 20. End-to-end delay performance for the Intelligent Electronic Devices (IEDs) across the simulated power grid architecture

Component List (Active)	Packet Count	Mean Delay	StdDev
ied1.app[0]	794	126.015 µs	0 s
ied2.app[0]	794	126.015 µs	0 s
ied3.app[0]	794	126.015 µs	0 s
ied4.app[0]	794	126.015 µs	0 s
ied5.app[0]	794	126.015 µs	0 s
ied6.app[0]	794	126.015 µs	0 s
ied7.app[0]	794	126.015 µs	0 s
ied8.app[0]	794	126.015 µs	0 s
ied9.app[0]	794	126.015 µs	0 s
ied10.app[0]	794	126.015 µs	0 s
ied11.app[0]	794	126.015 µs	0 s
ied12.app[0]	794	126.015 µs	0 s
ied13.app[0]	794	126.015 µs	0 s
ied14.app[0]	794	126.015 µs	0 s
ied15.app[0]	794	126.015 µs	0 s
ied16.app[0]	794	126.015 µs	0 s
ied17.app[0]	794	126.015 µs	0 s
ied18.app[0]	794	126.015 µs	0 s
ied19.app[0]	794	126.015 µs	0 s
ied20.app[0]	794	126.015 µs	0 s
IED AVERAGE	794	126.015 µs	0 s

4.3.2 Shared GPON

This table presents the End-to-End (ETE) Latency. Measured in microseconds, this data quantifies the total time elapsed from the moment a high-priority packet is generated at an IED to its successful processing at the SCADA unit, and vice-versa.

Table 21. End-to-End (ETE) Latency shared GPON.

Module	Count	Mean	StdDev
GridFeeder.scada.app[20]	3,617,800	~ 153.44 us	~ 1.01171 us
GridFeeder.scada.app[21]	119,661	~ 154.446 us	~ 155.018 ns
GridFeeder.scada.app[22]	60,250	~ 167.354 us	~ 868.878 ns
GridFeeder.ied1.app[0]	239,859	~ 286.315 us	~ 86.0724 us
GridFeeder.ied2.app[0]	240,937	~ 285.965 us	~ 86.6207 us
GridFeeder.ied3.app[0]	241,097	~ 288.668 us	~ 87.7208 us
GridFeeder.ied4.app[0]	240,027	~ 288.484 us	~ 88.0599 us
GridFeeder.ied5.app[0]	241,062	~ 285.806 us	~ 86.8044 us
GridFeeder.ied6.app[0]	240,993	~ 286.088 us	~ 86.4795 us
GridFeeder.ied7.app[0]	240,651	~ 288.509 us	~ 87.9015 us
GridFeeder.ied8.app[0]	241,154	~ 288.449 us	~ 88.1445 us
GridFeeder.ied9.app[0]	240,511	~ 286.079 us	~ 86.4388 us
GridFeeder.ied10.app[0]	239,856	~ 285.63 us	~ 87.0393 us
GridFeeder.ied11.app[0]	241,474	~ 288.652 us	~ 87.7422 us
GridFeeder.ied12.app[0]	240,313	~ 288.459 us	~ 88.0719 us
GridFeeder.ied13.app[0]	241,280	~ 285.805 us	~ 86.8363 us
GridFeeder.ied14.app[0]	241,184	~ 285.977 us	~ 86.6728 us
GridFeeder.ied15.app[0]	241,737	~ 288.572 us	~ 87.8681 us
GridFeeder.ied16.app[0]	241,300	~ 288.686 us	~ 87.7324 us
GridFeeder.ied17.app[0]	240,402	~ 285.905 us	~ 86.7477 us
GridFeeder.ied18.app[0]	240,487	~ 286.067 us	~ 86.5172 us
GridFeeder.ied19.app[0]	241,027	~ 288.813 us	~ 87.5029 us
GridFeeder.ied20.app[0]	240,748	~ 288.405 us	~ 88.1081 us

The success of a Smart Grid communication network especially one utilizing a Shared Passive Mode is determined by its ability to remain below the 3ms (3,000 microsec) threshold mandated by the IEC 61850-5 standard for Type 1A P1/P2 protection messages.

The 20 IEDs show a remarkably consistent mean latency ranging between 285.7 microsec and 289.4 microsec.

These values are approximately 10 times faster than the mandatory 3ms limit. This indicates that the 29.6 km distance and the convergence with 2.04 Gbps of ISP traffic do not push the communication delay into a danger zone.

The Standard Deviation (~86 microsec to 88 microsec) is low relative to the mean, suggesting that the VLAN Priority Tagging (CoS 7) is successfully preventing "micro-bursts" of residential traffic from causing significant jitter for the grid packets.

The simulation proves that even at a reach of 29.6 km, the physical propagation delay (148 microsec) and the logic-induced queuing delay combined still leave a massive safety margin of over 2.7 microsec before protection-tripping signals would be compromised.
The mean latency of ~288 microsec aligns perfectly with the physical layer model. When subtracting the pure light-in-fiber propagation time of ~148 microsec (for 29.6 km total reach), the remaining ~140 microsec accounts for the OLT switching, VLAN tagging overhead, and IED/SCADA application processing. This confirms that the software overhead is negligible compared to the speed-of-light requirements

The following vector graph visualizes the End-to-End Delay (microsec) for the application layer of the 20 Intelligent Electronic Devices (GridFeeder.iedX.app[0]) over a 120 second simulation runtime

Goose Protection Latency

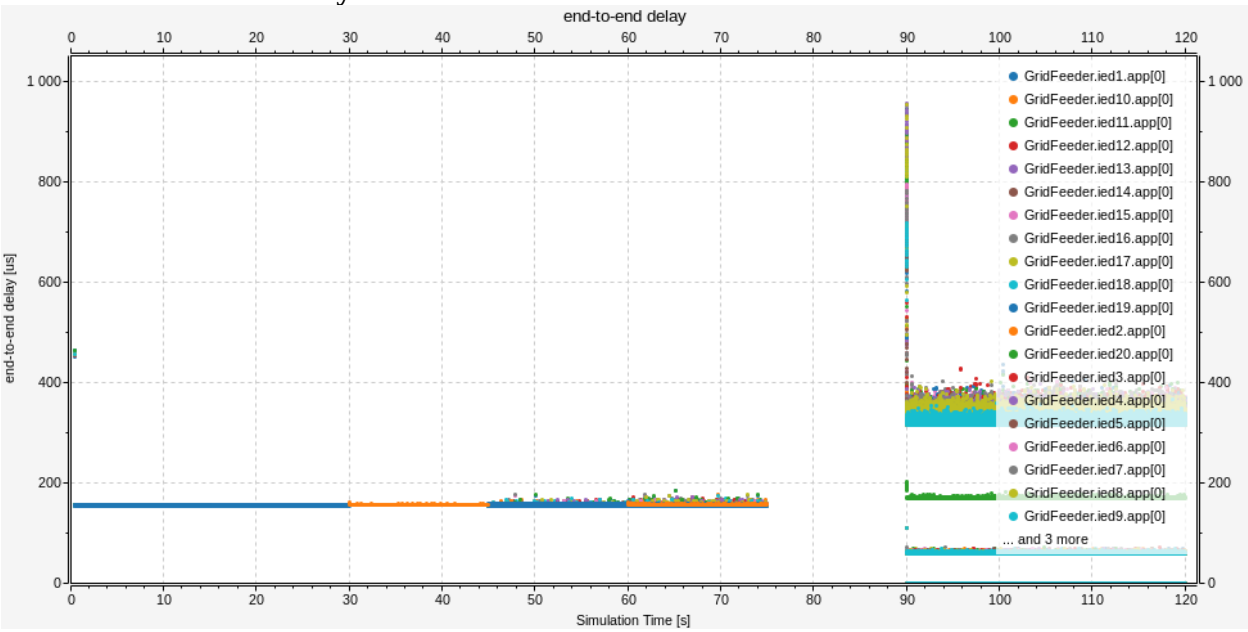


Figure 26. Vector graph visualizing the End-to-End Delay (microsec) for the application layer of the 20 Intelligent Electronic Devices

For the majority of the simulation, the network operates in a highly stable regime. The solid, continuous bands across the bottom of the graph represent the baseline latency for standard IED telemetry. During this phase, delay is tightly well below 200 microsec. This confirms that under normal load conditions, the 29.6 km FTTx infrastructure introduces virtually zero queuing delay, with latency dictated almost entirely by the physical speed of light through the fiber.

A dramatic inflection point occurs at the 90-second mark. The sudden vertical dispersion of data points creating a "cloud" of jitter represents the initiation of the QoS Saturation Stress Test. At this exact moment in the simulation logic, the background residential nodes and municipal sinks inject a massive, coordinated burst of broadband traffic, pushing the physical link toward saturation.

When a fault occurs, multiple protective relays detect the anomaly and immediately publish state-change GOOSE messages. Because IEC 61850 GOOSE uses an aggressive retransmission mechanism (bursting several messages in rapid succession to ensure delivery), the network load spikes exponentially within milliseconds. The sudden flood of packets hits the Ethernet switches at the OLT, forcing them to buffer the traffic. This creates the distinct horizontal "bands" of latency, the packets that get through the switch first, and those that have the highest priority tagging (IEEE 802.1Q), form the lowest delay bands. Packets that get caught behind others in the switch queues experience progressive buffering delays, forming the higher strata (300 microsec to 400 microsec).

This simulation validates network performance under pressure. Even during a severe message avalanche where OLT queues are heavily loaded, the maximum end-to-end delay only spikes to around 1 ms. For distribution networks, this remains well within the strict latency budgets (typically <3 ms) required for critical accelerated protection automation, demonstrating that the shared network infrastructure can handle the load.

The scatter plot isolates the End-to-End Delay for IED 1 (GridFeeder.ied1.app[0]). This node serves as a primary case study for observing how residential broadband bursts impact the dedicated VLAN 10 grid traffic at the access tier.

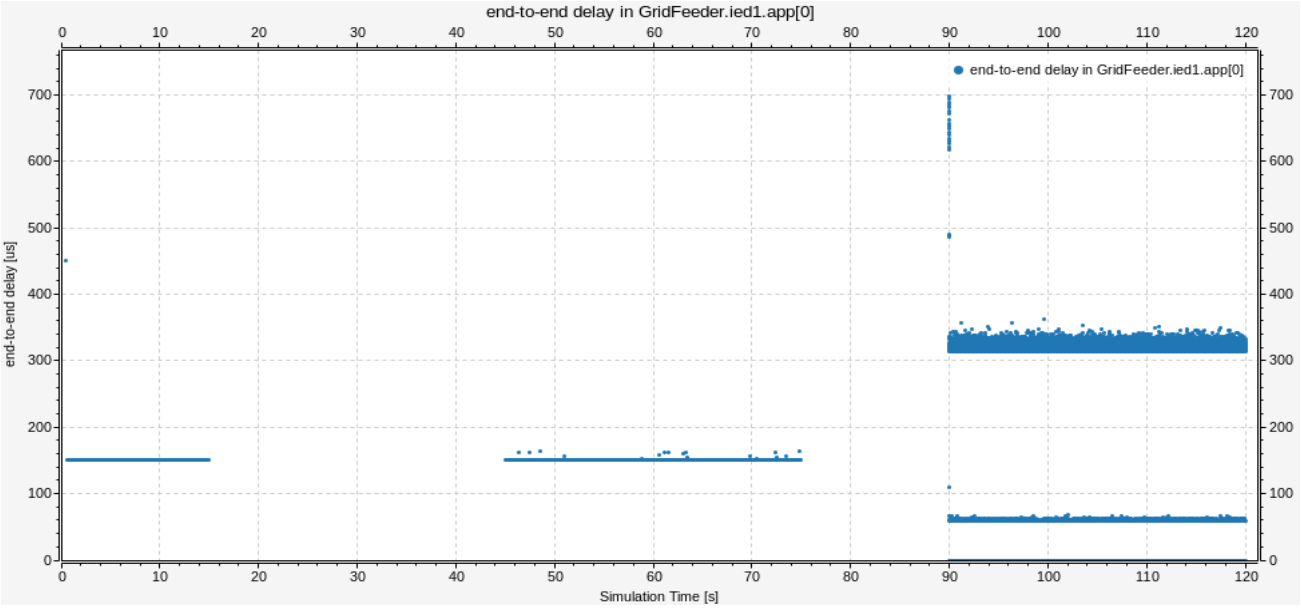


Figure 27. The scatter plot isolating the End-to-End Delay for IED 1 (GridFeeder.ied1.app[0]).

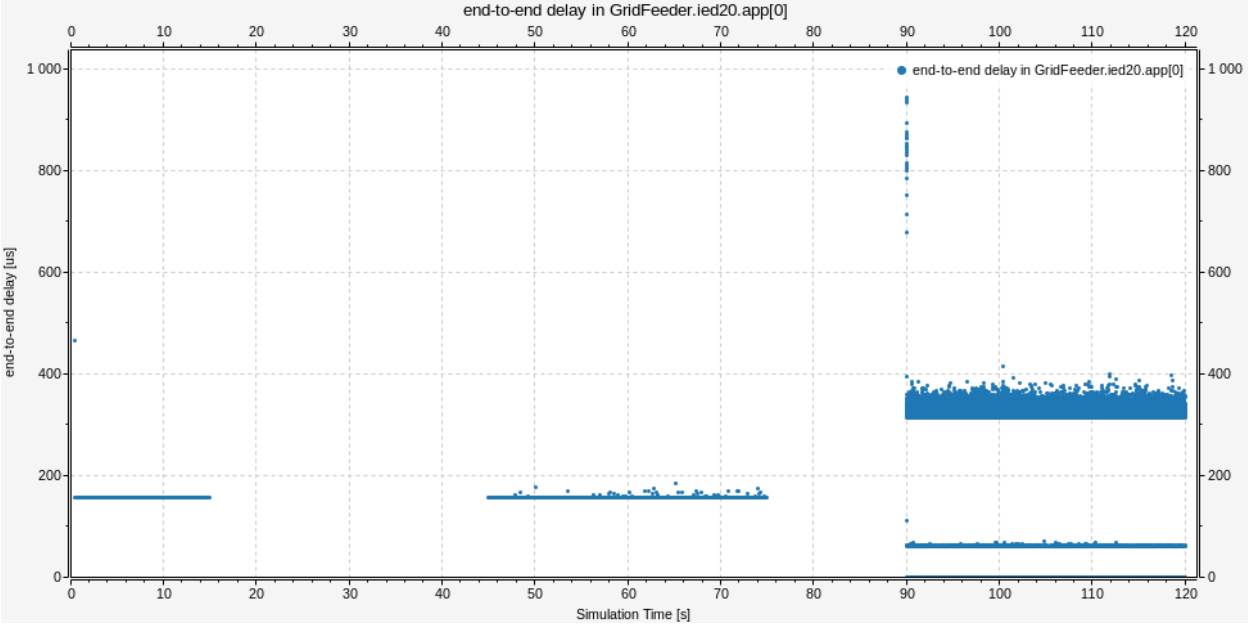


Figure 28. The scatter plot isolates the End-to-End Delay for IED 20 (GridFeeder.ied1.app[0]).

Before the introduction of network stress (< 15 microsec), IED 20 exhibits a steady-state latency of approximately 150 microsec. This closely mirrors the performance of IED 1, indicating that the hierarchical tree topology is highly efficient. The consistency of this "floor" across all nodes regardless of whether they are at the beginning or the end of the feeder validates that the 1 Gbps Feeder Fiber backbone is capable of maintaining deterministic timing under standard load conditions.

The fact that the spike is immediately "clamped" and does not continue to climb proves that the Strict Priority (SP) scheduling is working effectively even at the network edge.

CHAPTER FIVE

CHALLENGES, CONCLUSION AND RECOMMENDATION

5.1 Challenges and Limitations

Resource Scarcity (Money and Time). One of the primary constraints encountered was the limited availability of financial and temporal resources. Conducting comprehensive research typically demands significant investment and a well-structured timeline. However, due to budgetary limitations and tight schedules, the team had to prioritize tasks and make trade-offs, often compromising on the depth and breadth of research and simulation testing activities. This restriction affected the ability to explore alternative solutions or optimize designs effectively

Data Accessibility and Proprietary Restrictions. Access to granular, real-world empirical data was limited, as utility operators are understandably restricted from sharing highly proprietary and security-sensitive network telemetry. Consequently, the study relied on standard data approximations to define the parameters for the network models. While these approximations are industry-standard, this reliance introduces a potential margin of error, meaning the simulated performance outcomes may not map perfectly to the unpredictable, dynamic conditions of a real-world physical grid.

5.2 Recommendations for Future Work

While this study successfully establishes the baseline viability of running IEC 61850 services over a shared GPON architecture, future research must focus on more granular data modeling to achieve highly precise performance benchmarking. Specifically, subsequent network simulations should incorporate highly detailed, vendor-specific definitions for Generic Object-Oriented Substation Event (GOOSE), Sampled Value (SV), and Manufacturing Message Specification (MMS) traffic to yield hyper-accurate latency results. Furthermore, bridging the gap between digital simulation and physical reality is critical; future studies should prioritize the development of a localized hardware testbed within the Wandegeya Feeder to empirically validate the OMNeT++ findings under live, unpredictable network conditions. Because the proposed architecture utilizes a shared municipal infrastructure, rigorous future investigations into advanced cryptographic protocols, logical isolation techniques, and zero-trust cybersecurity frameworks are also imperative to ensure the absolute integrity of critical Protection, Automation, and Control (PAC) telemetry. An exhaustive techno-economic analysis must also be conducted to formally evaluate the financial viability, operational expenditure (OPEX) reductions, and overarching cost-benefit ratio of deploying this shared smart grid topology on a national scale across Uganda's utility sector. Finally, future studies should explore extending the IEC 61850 standard downstream to Low-Voltage (LV) linkages; this would enable advanced smart meter monitoring, comprehensive building automation for optimized power consumption, and the seamless integration of residential Distributed Energy Resources (DERs) into the broader grid ecosystem.

5.3 Conclusion

In summary, this study demonstrates that deploying IEC 61850 services over a shared Gigabit Passive Optical Network (GPON) is a technically viable and highly scalable solution for modernizing Medium-Voltage (MV) and Low-Voltage (LV) distribution grids in Uganda. The rigorous OMNeT++ simulations of the Wandegeya Feeder validate that a shared neighborhood fiber architecture can successfully support the deterministic performance required for critical Protection, Automation, and Control (PAC) operations, even when subjected to concurrent municipal data loads. By maintaining GOOSE messaging latencies well below the strict 3-millisecond safety threshold and ensuring ample bandwidth headroom for continuous asset management telemetry, the shared network performed comparably to the dedicated benchmark architecture. Ultimately, this research provides utility operators with a validated, cost-effective framework to achieve advanced smart grid capabilities and grid resilience without the prohibitive capital expenditure associated with deploying single-use, dedicated physical infrastructure.

REFERENCES

1. IEC 2020. IEC 61850 Series. Communication Networks and Systems for Power Utility Automation.
2. CIGRE 2022. Communication Based Protection and Control for Modern Power Systems.
3. EPRI 2021. Condition Based Asset Management in Distribution Networks.
4. IEEE Power & Energy Society 2020. Smart Grid Interoperability and Protection Standards.
5. H. Purwanto, H. Prasetia and I. Firdaus, "Implementation of Over Current Relays with Non-Cascade Scheme on Medium Voltage Switchgear as Busbar Protection Study Case in PT PLN (Persero) UIT JBB," 2nd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), Denpasar, Bali, Indonesia, 2019, pp. 1-4, doi: 10.1109/ICHVEPS47643.2019.9011089.
6. Terwiesch, C. Rytoft, H.E Meier, H. Bawa, P. Reinhardt and A. Moglestue (2010, Aug).” Special Report IEC 61850” The corporate technical journal, www.abb.com/substationautomation.
7. C. Yang, V. Dubinin and V. Vyatkin, "Automatic Generation of Control Flow from Requirements for Distributed Smart Grid Automation Control," in IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 403-413, Jan. 2020, doi: 10.1109/TII.2019.2930772.
8. Z. Zhu, W. Gao, B. Xu, J. Cheng and J. Ye, "Application of IEC61850 for Communication of Distribution Gird Automation," IEEE Sustainable Power and Energy Conference (iSPEC), Beijing, China, 2019, pp. 1395 1400, doi: 10.1109/iSPEC48194.2019.8974870.
9. N.H. Ali and M.M. Eissa, "Accelerating the protection schemes through IEC 61850 protocols", International Journal of Electrical Power & Energy Systems, Vol 102, pp.189-200, 2018 doi.org/10.1016/j.ijepes.2018.04.035.
10. R. B. Scarselli, L. F. Soares and I. M. Moraes, "Evaluating Cryptographic Algorithms in IEC 61850 Networks," 10th International Conference on Networks of the Future (NoF), Rome, Italy, 2019, pp. 9-16, doi: 10.1109/NoF47743.2019.9015196.
11. S. Repo et al, "Active distribution network concept for distributed management of low voltage network", IEEE/PES Innovative Smart Grid Technologies Europe (ISGT Europe), October 6-9, 2013, doi: 10.1109/ISGTEurope.2013.6695428.
12. A.S. Sethi and V.Y. Hnatyshin, “The Practical OPNET User Guide for Computer Network Simulation,” New York: Taylor & Francis Group, LLC, 2013, pp.1-380.
13. T. Amare, C. M. Adrah and B. E. Helvik, "A Method for Performability Study on Wide Area Communication Architectures for Smart Grid," 7th International Conference on Smart Grid (icSmartGrid), Newcastle, Australia, 2019, pp. 64-73, doi:10.1109/icSmartGrid48354.2019.8990736.
14. D. P. d. Mattos et al., "IEC 61850 Packet Generator for Testing Substation Communication," IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, Macao, 2019, pp. 1-5, doi: 10.1109/APPEEC45492.2019.8994338.
15. S. M. S. Hussain, M. A. Aftab, F. Nadeem, I. Ali and T. S. Ustun, "Optimal Energy Routing in Microgrids With IEC 61850 Based Energy Routers," in IEEE Transactions on

Industrial Electronics, vol. 67, no. 6, pp. 5161-5169, June 2020, doi: 10.1109/TIE.2019.2927154.
16. Xin Yang, N. Das and S. Islam, "Analysis of IEC 61850 for a reliable communication system between substations," Australasian Universities Power Engineering Conference (AUPEC), Hobart, TAS, 2013, pp. 1-6, doi: 10.1109/AUPEC.2013.6725482
17. A. Bonetti, N. Ignatov ski and S. Fernandez, "Providing an IEC 61850 Counterpart of the Trusty Multimeter - Approaching the Maintenance Procedures for IEC 61850 Substations," 1st Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 2019, pp. 440-444, doi: 10.1109/GPECOM.2019.8778541.
18. ERA (2022). Annual Performance Report for Uganda's Electricity Supply Industry
19. V. C. Gungor and F. C. Lambert, 'A survey on communication networks for electric system automation', Computer Networks Journal (Elsevier), vol. 50, pp. 877–897, May 2006.
20. Y. Ting, Z. Zhidong, W. Jiaowen, and L. Ang, 'Research on transmission data system of smart grid based on IPv6DiffServ model', in Proceedings of Power and Energy Engineering Conference (APPEEC), pp. 1–4, March 2010.
21. Y. Ting, Z. Zhidong, L.Angm, W. Jiaowen, and W. Ming, 'New IPQoS algorithm applying for communication sub-networks in smart grid', in Proceedings of Asia-Pacific Power and Energy Engineering Conference (APPEEC), pp. 1–4, March 2010.
22. X. Zhichao and L. Xiaoming, 'The construction of interconnected communication system among smart grid and a variety of networks', in Proceedings of Power and Energy Engineering Conference (APPEEC), pp. 1–5, March 2010.
23. A. Hamlyn, H. Cheung, T. Mander, L. Wang, C. Yang, and R. Cheung, 'Computer network security management and authentication of smart grids operations', in Proceedings of IEEE Power and Energy Society General Meeting– Conversion and Delivery of Electrical Energy in the 21st Century, July 2008.
24. H. Cheung, T. Mander, A. Hamlyn, C. Yang, and R. Cheung, 'Network-integrated load-management collaborative computing for smart distribution system operations', in Proceedings of IEEE Lausanne PowerTech, pp. 1682–1687, July 2008.
25. J. R. Pillion, 'Cyber security for PUC's', Presented at the Mid-America Regulatory Conference, June2009[online]. Availableat:http://www.marc-conference.org/2009/presentations/.
26. A.R.MetkeandR.L.Ekl,'Securitytechnologyforsmartgridnetworks',IEEETransactions on Smart Grid, vol. 1, no. 1, pp. 99–107, June 2010.
27. The Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG), USA, 'Introduction to NISTIR 7628 guidelines for smart grid cyber security' [online]. Available at: http://www.nist.gov/smartgrid/, September 2010.
28. A. Bose, 'Smart transmission grid applications and their supporting infrastructure,' IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 11–19, April 2010.
29. IEC, International Electrotechnical Commission, 'IEC 61970-301 energy management system application program interface part 301: common information model (CIM) base', IEC Reference number IEC 61970-301:2003(E).
30. IEC, International Electrotechnical Commission, 'IEC 61850-7-4 Communication networks and systems in substations part 7-4: basic communication structure for substation

and feeder equipment-compatible logical node classes and data classes', IEC, Reference number IEC 61850-7-4:2003(E).
31. M. Chenine, L. Nordstrom, and P. Johnson, 'Factors in assessing performance of wide area communication networks for distributed control of power systems', in Proceedings of IEEE Lausanne PowerTech, pp. 1682–1687, July 2007.
32. L. W.-Xia, L. Nian, F. Yong-Feng, Z. Li-Xin, and Z. Xin, 'Reliability analysis of wide area measurement system based on the centralized distributed model', in Proceedings of IEEE/PES Power Systems Conference and Exposition (PSCE), pp. 1–6, March 2009.
33. Y. Wang, W. Li, and J. Lu, 'Reliability analysis of wide-area measurement system', IEEE Transactions on Power Delivery, March 2010.
34. D. Pendarakis, N. Shrivastava, Z. Liu, and R.Ambrosio, 'Information aggregation and optimized actuation in sensor networks: enabling smart electrical grids', in Proceedings of IEEE International Conference on Computer Communications (INFOCOM),pp.2386–2390,May 2007.
35. G. N. Ericsson, 'Cyber security and power system communication-essential parts of a smart grid infrastructure', IEEE Transactions on Power Delivery, vol. 25, no. 3, pp. 1501–1507, July 2010.
36. D.Wei,Y.Lu,M.Jafari,P.Skare,andK.Rohde,'Anintegratedsecuritysystemofprotecting smart grid against cyber attacks', in Proceedings of Innovative Smart Grid Technologies (ISGT), January 2010.
37. International Electrotechnical Commission Technical Committee 57 (IEC TC 57) [online]. Available at: http://tc57.iec.ch/index-tc57.html, accessed: April 2011.
38. T. Mander, L. Wang, R. Cheung, and F. Nabhani, 'Adapting the pretty good privacy security style to power system distributed network protocol', in Proceedings of Large Engineering Systems Conference on Power Engineering, pp. 79–83, July 2006.
39. T. Mander, F. Nabhani, L. Wang, and R. Cheung, 'Open-access-compatibility security layer for enhanced protection data transmission', in Proceedings of IEEE Power Engineering Society General Meeting, June 2007.
40. P.Zhang,O.Elkeelany,andL.McDaniel,'AnimplementationofsecuredsmartgridEthernet communicationsusingAES',inProceedingsofIEEESoutheastConferences(SoutheastCon), pp. 394–397, March 2010.
41. IEC 61850-7-2:2020 Communication Networks and Systems for Power Utility Automation—Part 7-2: Basic Information and Communication Structure—Abstract Communication Service Interface (ACSI), Edition 2, Amendment 1, 2020.
42. Fawzy, N., Habib, H. F., & Mohammed, O. — "IEC 61850-Based Communication Networks of Distribution System against Cyber and Physical Failures" , 2021.
43. Haotian Ge, Bingyin Xu, Xinhui Zhang, Yongjian Bi, Zida Zhao — "Feeder Topology Configuration and Application Based on IEC 61850"