



وزارة البحث العلمي و التعليم العالي

**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET
DE LA RECHERCHE SCIENTIFIQUE**



جامعة عبد الحميد بن باديس مستغانم

Université Abdelhamid Ibn Badis Mostaganem

كلية العلوم والتكنولوجيا

Faculté des Sciences et de la Technologie

DEPARTEMENT DE GENIE ELECTRIQUE

MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN GENIE ELECTRIQUE

Spécialité : réseaux électrique

Présenté par :

DJERBOUA MUSTAPHA

ABBES IBRAHIM

**Contribution à l'analyse et à la réduction des pertes
non techniques dans le réseau électrique de
Mostaganem**

Soutenu le / /2026 Devant jury composé de

Président :

Examineur :

Encadreur : SOUAG.S

Grade MCB

Université de Mostaganem



وزارة البحث العلمي و التعليم العالي

MINISTRY OF HIGHER EDUCATION AND
SCIENTIFIC RESEARCH

جامعة عبد الحميد بن باديس مستغانم

Abdelhamid Ibn Badis Mostaganem University

كلية العلوم والتكنولوجيا

Faculty of Science and Technology

DEPARTMENT OF ELECTRICAL ENGINEERING

MEMOIRE

Presented to obtain the diploma of

MASTER'S DEGREE IN ELECTRICAL ENGINEERING

Specialty: electrical networks

Presented by:

DJERBOUA MUSTAPHA

ABBES IBRAHIM

Contribution to the analysis and reduction of non-technical losses in the Mostaganem electrical network

Defended on / /2026 Before a jury composed of

President :

Examiner:

Rapporteur: SOUAG.S

Grade MCB

Université de Mostaganem

Abstract:

Electrical distribution networks face severe operational and financial challenges due to Non-Technical Losses (NTL), which encompass electricity theft, meter tampering, and administrative anomalies. This thesis investigates the specific characteristics and impacts of NTLs within the Mostaganem electrical network in Algeria, operated by Sonelgaz. Beyond massive financial deficits and uncollected revenues, NTLs inflict uncoordinated thermal stress on distribution transformers, degrade power quality, and pose significant public safety hazards.

To address these vulnerabilities across residential and high-stakes industrial sectors, the study evaluates a multifaceted mitigation strategy. These proposed solutions range from practical physical deterrents, such as external meter relocation and the deployment of Aerial Bundled Cables (ABC), to advanced technological frameworks including Advanced Metering Infrastructure (AMI), GIS mapping, and Artificial Intelligence.

Furthermore, a dynamic electrotechnical simulation of a 30 kV Medium Voltage (HTA) network was developed using MATLAB/Simulink to model heavy industrial electricity fraud, specifically complete and asymmetric phase bypassing. The simulation successfully validates a real-time smart detection logic based on micro-energy differential balancing. By coupling this digital detection with an automated physical deterrence mechanism that instantly trips the main circuit breaker during a fraud event, the study proves that transitioning from passive, reactive billing audits to proactive, hardware-linked smart grid defenses is essential for neutralizing energy theft and securing grid stability.

Résumé :

Les réseaux de distribution électrique sont confrontés à de graves défis opérationnels et financiers en raison des pertes non techniques (PNT), qui englobent le vol d'électricité, la falsification des compteurs et les anomalies administratives. Ce mémoire étudie les caractéristiques spécifiques et les impacts des PNT au sein du réseau électrique de Mostaganem en Algérie, exploité par la Sonelgaz. Au-delà des déficits financiers massifs et des revenus non perçus, les PNT infligent des contraintes thermiques non coordonnées aux transformateurs de distribution, dégradent la qualité de l'énergie et posent des risques importants pour la sécurité publique.

Pour remédier à ces vulnérabilités dans les secteurs résidentiels et industriels à forts enjeux, l'étude évalue une stratégie d'atténuation multidimensionnelle. Ces solutions proposées vont des moyens de dissuasion physiques pratiques, tels que la relocalisation externe des compteurs et le déploiement de câbles en réseau torsadé, aux cadres technologiques avancés comprenant l'infrastructure de comptage avancée (AMI), la cartographie SIG et l'intelligence artificielle.

De plus, une simulation électrotechnique dynamique d'un réseau moyenne tension (HTA) de 30 kV a été développée à l'aide de MATLAB/Simulink pour modéliser la fraude électrique industrielle lourde, plus précisément le contournement de phase complet et asymétrique (piquage illicite). La simulation valide avec succès une logique de détection intelligente en temps réel basée sur l'équilibrage différentiel de la micro-énergie. En associant cette détection numérique à un mécanisme de dissuasion physique automatisé qui déclenche instantanément le disjoncteur principal lors d'un événement de fraude, l'étude prouve que la transition d'audits de facturation passifs et réactifs vers des défenses de réseau intelligent proactives et liées au matériel est essentielle pour neutraliser le vol d'énergie et garantir la stabilité du réseau.

ملخص

تواجه شبكات توزيع الكهرباء تحديات تشغيلية ومالية جسيمة نتيجةً للخسائر غير الفنية، والتي تشمل سرقة الكهرباء والتلاعب بالعدادات والمخالفات الإدارية. تبحث هذه الأطروحة في الخصائص والآثار المحددة للخسائر غير الفنية ضمن شبكة كهرباء مستغانم في الجزائر، التي تديرها شركة سونلغاز. فإلى جانب العجز المالي الهائل والإيرادات غير المحصلة، تُلحق الخسائر غير الفنية إجهادًا حراريًا غير منسق بمحولات التوزيع، وتؤدي إلى تدهور جودة الطاقة، وتُشكل مخاطر جسيمة على السلامة العامة. ولمعالجة هذه المخاطر في القطاعين السكني والصناعي ذي الأهمية البالغة، تُقِيم الدراسة استراتيجية تخفيف متعددة الأوجه. وتتراوح هذه الحلول المقترحة بين إجراءات ردع مادية عملية، مثل نقل العدادات الخارجية ونشر الكابلات الهوائية المجمعة، وأطر تكنولوجية متقدمة تشمل البنية التحتية المتقدمة للعدادات، ورسم الخرائط الجغرافية المكانية، والذكاء الاصطناعي. علاوة على ذلك، طُوّرت محاكاة بجهد 30 كيلو فولت باستخدام برنامج (HTA) كهروتقنية ديناميكية لشبكة جهد متوسط لنمذجة عمليات الاحتياال الكهربائي الصناعي واسعة النطاق، وتحديدًا تجاوز MATLAB/Simulink الطور الكامل وغير المتماثل. وقد نجحت المحاكاة في التحقق من صحة منطق الكشف الذكي في الوقت الفعلي القائم على موازنة الطاقة التفاضلية الدقيقة. ومن خلال ربط هذا الكشف الرقمي بآلية ردع مادية مؤتمتة تفصل قاطع الدائرة الرئيسي فورًا أثناء وقوع عملية احتياال، تُثبت الدراسة أن الانتقال من عمليات تدقيق الفواتير السلبية والتفاعلية إلى دفاعات الشبكة الذكية الاستباقية والمرتبطة بالأجهزة أمرٌ ضروري لتحديد سرقة الطاقة وضمان استقرار الشبكة.

Summary:

General Introduction.....	1
---------------------------	---

Chapter I: Overview of Electrical Distribution Networks and Energy Losses

1.1 Introduction	3
1.2 Architecture and Role of the Distribution Network.....	3
1.3 The Algerian Context and Sonelgaz.....	5
1.4 Classification of Energy Losses.....	6
1.4.1 Technical Losses (TL).....	7
1.4.2 Non-Technical Losses (NTL).....	7
1.5 Primary Causes of Non-Technical Losses.....	8
1.5.1 Direct Electricity Theft (Illegal Hooking).....	8
1.5.2 Meter Tampering and Manipulation.....	8
1.5.3 Administrative, Infrastructure, and Billing Anomalies.....	8
1.6 Factors Exacerbating Non-Technical Losses.....	9
1.7 The Impact of Non-Technical Losses.....	9
1.7.1 Economic and Financial Consequences.....	9
1.7.2 Grid Degradation and Power Quality Deterioration.....	9
1.7.3 Compounding of Technical Losses.....	10
1.7.4 Safety Hazards.....	10
1.8 Geographical, Demographic, and Economic Context of the Mostaganem Wilaya.....	12
1.8.1 Topography and Territorial Organization.....	12
1.8.2 Demographic Evolution and Urban Expansion.....	12
1.8.3 Economic Vocation and Sectoral Energy Consumption.....	13
1.9 Organizational Structure of Sonelgaz Distribution.....	13

1.9.1 The Restructuring of the Sonelgaz Group.....	13
1.9.2 The Direction of Distribution (DD) of Mostaganem.....	14
1.9.3 The Technical Division of Electricity (DTE).....	14
1.9.4 The Commercial Division (DC).....	14
1.9.5 Local Commercial Agencies (Agences Commerciales).....	15
1.10 Technical Architecture of the Electrical Grid.....	15
1.10.1 The Source Substations	15
1.10.2 The Medium Voltage Network (HT).....	16
1.10.3 The Low Voltage Network (BT).....	16
1.11 Statistical Overview of Network Customers.....	17
1.11.1 Global Electrification Rates by Commune.....	17
1.11.2 Analysis of the Low Voltage (BT) Portfolio.....	18
1.11.3 Analysis of the Medium (HTA) and High Voltage (HTB) Portfolio.....	19
1.12 Conclusion.....	21
Chapter 2: Analysis of Non-Technical Losses in Mostaganem Electrical Network	
2.1 Introduction and Transition from Network Architecture.....	22
2.2 The Energy Balance Framework and Loss Quantification.....	22
2.2.1 Operational Challenges in the Mostaganem Context.....	22
2.3 Main Sources of Non-Technical Losses	23
2.3.1 The Scale of the Debt in Mostaganem.....	23
2.3.2 Impact and Escalating Recovery Strategies.....	24
2.4 Physical Vandalism and Infrastructure Sabotage.....	25
2.4.1 The National and Local Impact of Sabotage.....	25
2.4.2 Targeted Communes and Operational Consequences.....	25
2.5 Clandestine Connections and Urban Fraud (Piquage Illicite).....	26
2.5.1 The Mechanics of Illegal Tapping.....	26
2.5.2 Safety Hazards and Grid Degradation.....	26
2.6 The Technical Anatomy of Electrical Fraud: Single-Phase vs. Three-Phase	

ampering.....	27
2.6.1 Single-Phase Tampering: The Decentralized Drain (Low Voltage).....	27
2.6.2 Three-Phase Tampering: High-Stakes Industrial Fraud (Medium/Low Voltage).....	27
2.7 Administrative Weaknesses and Estimation Anomalies.....	29
2.7.1 Inaccessible Meters and "Forfaitaire" Billing.....	29
2.7.2 Database Delays and Organizational Complicity.....	29
2.8 Geographical Mapping of Non-Technical Losses.....	30
2.9 Technological Diagnostics and Advanced Current Detection Technologies.....	31
2.9.1 Hardware-Level Surveillance (ACE6000 Capabilities).....	31
2.9.2 Software Diagnostics and LCD Error Codes.....	32
2.9.3 The Shift Toward Data Mining and Profiling.....	33
2.10 Conclusion.....	35
chapter 3: Proposed Solutions for Reducing Non-Technical Losses in Mostaganem Electrical Network	
3.1 Introduction.....	36
3.2 General Technical and Practical Solutions.....	36
3.2.1 External Meter Relocation.....	36
3.2.2 Smart Meter Installation.....	37
3.2.3 Prepaid Metering Systems.....	39
3.2.4 AI and Data Analytics for Theft Detection.....	39
3.2.5 GIS-Based Monitoring and Mapping.....	40
3.2.6 Consumer Awareness and Public Campaigns.....	42
3.3 Single-Phase Targeted Solutions.....	41
3.3.1 Micro-Energy Balancing at Transformer Level	41

3.4 Three-Phase Targeted Solutions.....	41
3.4.1 Asymmetric Phase Distribution: A Physical Deterrent Strategy.....	41
3.4.2 Smart Three-Phase Meter Tampering Detection at the Terminal Level.....	42
3.4.3 Replacement of Bare Conductors with ABC Cables.....	43
3.5 Conclusion.....	44
Chapter 4: Application and Case Study in the Mostaganem Electrical Network	
4.1 Presentation of the Case Study: The Mostaganem HTA Network	45
4.2 MATLAB/Simulink Implementation and Network Parameters.....	45
4.3 Results and Discussion.....	47
4.3.1 Analysis of the Fraud Event (Active and Reactive Power)	47
4.3.2 Validation of the Smart Detection Logic	48
4.4 Advanced Scenario: Asymmetric Phase Bypassing and Physical Deterrence strategy.....	49
4.4.1 Upgraded Simulation Parameters.....	49
4.4.2 Results of the Deterrence Strategy.....	50
4.5 Comprehensive Synthesis of Simulation Outcomes and Strategic Recommendations.....	51
4.5.1 Recap of the Simulation Paradigm.....	51
4.5.2 Cross-Analysis of the Power Curves and Alarm Responses.....	51
4.5.3 Scientific Interpretation of the Physical Grid Impact.....	52
4.5.4 Comparative Literature Analysis.....	52
4.5.5 Final Conclusions and Takeaways for the Utility.....	53
4.6 Conclusion.....	53
General Conclusion.....	54

References.....56

List of figures :

Figure1.1 : high-voltage power line.....	4
Figure 1.2: Typical MV/LV Distribution Transformer configurations (Pole-mounted vs Cabin type).....	4
Figure 1.3 : power transmission system.....	5
Figure 1.4: General schematic of electrical grid hierarchy.....	6
Figure 1.5: Distribution of Subscribed Power (PMD) by Economic Sector.....	20
Figure 2.1: Front panel of the Itron ACE6000 electronic meter showing the LCD display, optical communication port, and metrological LEDs	32
Figure 2.2 : Itron ACE6000 Electricity Meter Components.....	34
Figure 3.1: Electrical Meter Box.....	36
Figure 3.2 : smart meter.....	37
Figure 3.3: Smart Meter (SM) implementation: (a) External enclosure mounted on a utility pole; (b) Internal components of the SM system.....	38
Figure 3.4: Smart card prepaid electric meter.....	39
Figure 3.5 : Data visualization process.....	40
Figure 3.6: 3-Phase 4-Wire Meter Connection Diagram (showing Terminals 1, 3, 4, 6, 7, 9 for Phases L1, L2, L3 and Terminals 10, 12 for Neutral).....	42
Figure 4.1: The complete MATLAB/Simulink model of the network and the smart detection logic.....	47
Figure 4.2: Active Power recorded by the Main Node and the Client Node showing the bypass event.....	48
Figure 4.3: Reactive Power recorded by the Main Node and the Client Node.....	48
Figure 4.4: Automated Smart Meter Alarm triggering instantaneously at the exact moment of fraud.....	49
Figure 4.5: Upgraded Simulink model featuring Asymmetric Bypass and the Automated.....	49
Figure 4.6: Smart Logic Alarm instantly detecting the asymmetric bypass and triggering the deterrence mechanism.Physical Deterrent Breaker.....	50
Figure 4.7: Active Power dropping to absolute zero due to the automated main breaker tripping.....	51

Figure 4.8: Reactive Power dropping to zero, confirming the total shutdown of the industrial facility.....5

List of tables :

Table 1.1: Situation of Electrification by selected communes in the Wilaya of Mostaganem (Source: Baseline Data 2021).....	18
Table 1.2: Distribution of Low Voltage (BT) clients by commercial agency (Source: Sonelgaz Data 2026)....	18
Table 1.3: Distribution of Large Accounts (HTA and HTB) by commercial agency in April 2026.....	19
Table 2.1: Quantitative breakdown of Sonelgaz unpaid bills (Créances) in the Wilaya of Mostaganem.....	24
Table 2.2: Comparison between Single-Phase and Three-Phase Electricity Fraud Profiles.....	28
Table 2.3: Geographical distribution and dominant typologies of non-technical losses in Mostaganem.....	30
Table 2.4: Geographical distribution and dominant typologies of non-technical losses in Mostaganem.....	31

Keywords:

Non-Technical Losses (NTL), electricity theft, electrical distribution networks, smart grid technologies, Advanced Metering Infrastructure (AMI), energy balancing, fraud detection, automated deterrence, MATLAB/Simulink modeling, Mostaganem grid.

List of Abbreviations and Symbols:

Acronyms and Abbreviations

- **ABC** — Aerial Bundled Cables (insulated overhead conductors replacing bare wires to prevent direct physical tapping)
- **AMI** — Advanced Metering Infrastructure (integrated smart meters, sensors, and two-way communication systems)
- **AMR** — Automated Meter Reading system
- **CT / PT** — Current Transformer / Potential (Voltage) Transformer
- **DSO** — Distribution System Operator (*Sonelgaz*)
- **LV** — Low Voltage distribution grid (230/400 V residential and commercial network)
- **MV** — Medium Voltage distribution grid (10/30 kV primary distribution feeders)
- **NTL** — Non-Technical Losses (unbilled energy, electricity theft, meter tampering, and billing errors)
- **PI** — Proportional-Integral Controller (utilized in automated Simulink protection and fraud-detection circuits)
- **PLC** — Power Line Communication (data transmission over physical electrical power conductors)
- **TL** — Technical Losses (Joule heating and core magnetic losses inherent to grid conductors and transformers)

Mathematical Symbols and Grid Variables

- E_{injected} — Total electrical energy injected into a distribution feeder or transformer substation (kWh / MWh)
- E_{billed} — Total electrical energy recorded and billed across all customer meter accounts (kWh / MWh)
- E_{NTL} — Quantified energy volume lost due to non-technical causes (kWh / MWh)
- E_{TL} — Calculated physical energy loss due to conductor resistance and thermal dissipation (kWh)
- $\Delta P(t)$ — Instantaneous active power differential at the transformer substation level (kW)
- P — Active power flow across a line segment (kW)
- Q — Reactive power flow across a line segment (kVAR)
- S — Apparent power capacity (kVA)
- V / U — Phase RMS voltage / Line-to-line RMS voltage (V)
- I — Line current magnitude (A)
- I_n — Neutral conductor current magnitude (A) (*Key indicator for single-phase neutral bypass fraud*)
- $\cos \phi$ — Power factor (ratio of active power to apparent power)
- R — Conductor resistance (Ω)
- X — Conductor reactance (Ω)
- Z — Complex line impedance (Ω)
- p.u. — Per-Unit system (normalized unit representation)

General Introduction

The fundamental objective of an electrical power system is to generate, transmit, and deliver electrical energy to end-users reliably, efficiently, and economically. While the generation and transmission stages operate at high voltages and are subject to stringent centralized monitoring, the distribution network represents the final, most extensive, and most vulnerable segment of the power grid. As electricity demand grows alongside rapid urbanization and industrial expansion, utility companies face profound challenges in maintaining grid efficiency and financial sustainability.

One of the most critical operational hurdles in the management of modern distribution networks is energy loss. Although technical losses are inherent to the physical properties of electrical equipment and conductors, a substantial and highly damaging fraction consists of Non-Technical Losses (NTL). Driven by unauthorized consumption, illicit hooking, sophisticated meter tampering, and administrative inefficiencies, NTLs represent a pure revenue leakage without any underlying physical justification. For distribution system operators like Sonelgaz, these commercial losses not only cripple the capacity for grid modernization and maintenance but also induce severe uncoordinated thermal stress on the existing infrastructure, thereby compromising power quality and public safety.

The mitigation of this multidimensional problem can no longer rely solely on traditional, reactive management. It requires a paradigm shift toward advanced data monitoring, physical deterrence, and intelligent detection systems. Furthermore, understanding the structural vulnerabilities that facilitate these losses demands a localized approach, adapting modern solutions to specific geographical, demographic, and socio-economic contexts.

The study conducted in this graduation thesis focuses on evaluating the contribution of non-technical losses within the Mostaganem electrical network. By bridging theoretical frameworks with concrete dynamic simulations, this research aims to diagnose the specific vulnerabilities of the local grid and validate the effectiveness of advanced smart detection strategies. This work is structured around four main chapters:

In Chapter I, a foundational overview of electrical distribution networks and energy losses is combined with the presentation of the Mostaganem network. This establishes the theoretical background and the specific socio-technical, geographical, and demographic profile of the local grid.

In Chapter II, a comprehensive analysis of the current non-technical loss situation in Mostaganem is conducted. It maps the geographical hotspots of electricity theft, evaluates the scale of structural unpaid bills, and diagnoses the administrative anomalies.

In Chapter III, various targeted solutions are proposed to reduce these losses, evaluating practical countermeasures, physical deterrents, and the implementation of Advanced Metering Infrastructure (AMI).

In Chapter IV, a practical application is demonstrated through the MATLAB/Simulink environment, simulating a high-stakes industrial meter bypass event to validate an automated smart detection logic

Chapter I: Overview of Electrical Distribution Networks and Energy Losses

1.1 Introduction :

The fundamental objective of an electrical power system is to generate, transmit, and deliver electrical energy to end-users reliably, efficiently, and economically. While the generation and transmission stages operate at high voltages and are subject to stringent centralized monitoring, the distribution network represents the final, most extensive, and most vulnerable segment of the power grid. Because this infrastructure spans vast geographical areas and interfaces directly with millions of consumers, achieving perfect observability and control remains a significant engineering challenge [1].

One of the most critical operational challenges in the management of these networks is energy loss. In any distribution grid, the total electrical energy injected from the transmission substations invariably exceeds the energy successfully billed to end consumers. This discrepancy, widely known as total energy loss, poses severe financial and operational burdens on utility companies worldwide. While a portion of these losses is naturally governed by the laws of physics, a substantial fraction is caused by unauthorized consumption, anomalous metering, and administrative inefficiencies.

This chapter establishes the foundational context for this research project. It provides a technical overview of distribution network architectures and clearly delineates the division between Technical Losses (TL) and Non-Technical Losses (NTL). Subsequently, it explores the primary mechanisms, exacerbating factors, and systemic impacts of NTLs, thereby framing the necessity for advanced analytical solutions to detect and mitigate these phenomena.

1.2 Architecture and Role of the Distribution Network

To accurately identify the origins of energy losses, it is necessary to understand the structural topology of the grid. Because electrical energy cannot be stored efficiently on a massive scale, real-time equilibrium between generation and consumption must be maintained. High-voltage transmission networks (typically 110 kV to 765 kV) transport bulk power over long distances with minimal losses. However, the scope of this project is confined strictly to the distribution network, which acts as the interface between the bulk power grid and the end-user.



Figure1.1 : high-voltage power line

The distribution system is generally categorized into two distinct operational levels [2] :

- **Primary Distribution (Medium Voltage - MV):** At the primary substation, power transformers step down the transmission voltage to medium voltage levels (typically between 10 kV and 33 kV). These feeders route power across urban and rural landscapes to localized distribution transformers.



Figure 1.2: Typical MV/LV Distribution Transformer configurations (Pole-mounted vs. Cabin type)

- **Secondary Distribution (Low Voltage - LV):** Distribution transformers further step down the voltage to utilization levels (e.g., 400 V three-phase / 230 V single-phase).

The secondary LV network is precisely where the vast majority of non-technical losses occur. Its highly decentralized nature, sprawling physical footprint, and direct physical accessibility

to the public make it exceptionally difficult to patrol and secure, rendering it the most susceptible tier of the electrical grid to illicit interventions.

In the Algerian distribution system, the grid relies on distribution transformers that step down the voltage from 10 kV to a usable 400 V. From these transformers, electricity travels through a mix of overhead lines—often using bare

or twisted cables—and underground feeders.

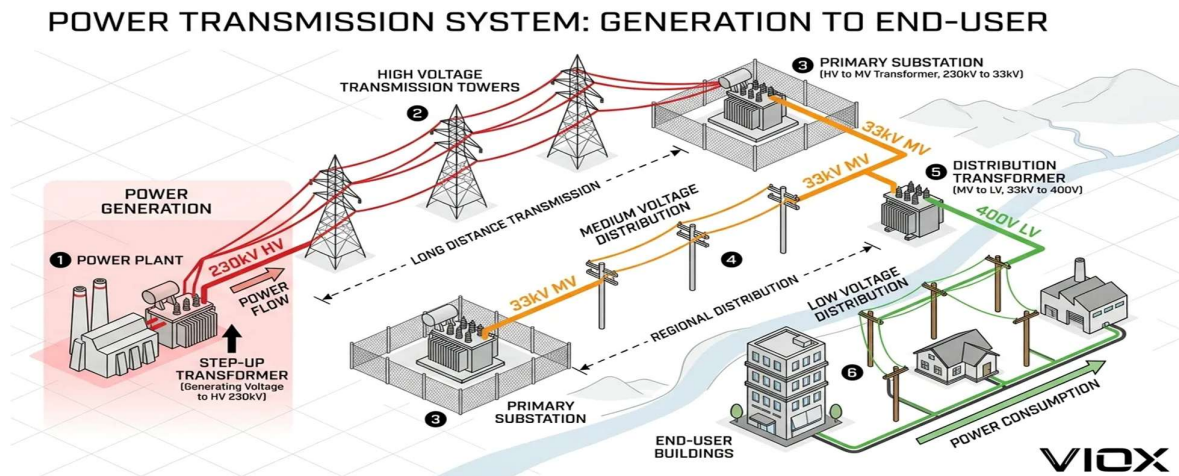


Figure 1.3 : power transmission system

1.3 The Algerian Context and Sonelgaz

In Algeria, the electricity sector is managed by the state-owned company, Sonelgaz. Over the years, the company was restructured to manage the grid more efficiently.

The Algerian electrical system is categorized into several hierarchical tiers based on voltage levels. The national transmission network (Transport) operates at high and very-high voltages, specifically 60 kV, 220 kV, and 400 kV. Below this, the sub-transmission or 'Répartition' networks interface between high and medium voltage levels, typically utilizing 30 kV and 10 kV standards to facilitate regional energy exchange. Finally, the utilization network provides low-voltage (LV) power to end consumers, ranging from 230 V to 400 V, where continuous service reliability is paramount.

Today, different tasks are handled by different branches:

- Generation is managed by SPE (Société Algérienne de Production de l'Electricité).
- High-voltage transmission is managed by GRTE (Gestionnaire du Réseau de Transport de l'Electricité).
- **Sonelgaz Distribution (SD)** is specifically responsible for the management of the medium-voltage (MV) and low-voltage (LV) infrastructures. In the Algerian technical framework, the MV distribution level is standardized at 10 kV.

Sonelgaz Distribution is the branch that deals directly with consumers. Therefore, it is the branch that faces the financial and technical burden of non-technical losses.

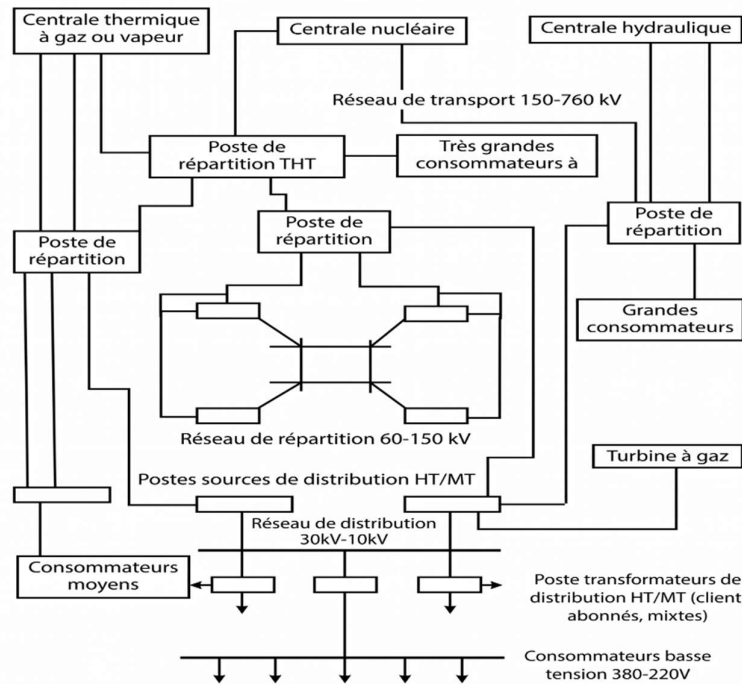


Figure 1.4: General schematic of electrical grid hierarchy

1.4 Classification of Energy Losses

Despite these national characteristics, the practical manifestation of non-technical losses varies significantly across regional distribution networks. In Mostaganem, the growing customer base, network expansion, and operational constraints create a relevant case study for analyzing these losses.

The operational efficiency of an electrical distribution network can be evaluated using a fundamental energy balance relationship. Over a defined billing or measurement period, the energy balance can be expressed as follows:

$$E_{\text{injected}} = E_{\text{billed}} + E_{\text{losses}}$$

Where:

- E_{injected} represents the total active energy supplied to the distribution network through primary substations.
- E_{billed} denotes the total active energy accurately measured by customer metering systems and billed by the utility.

- E_{losses} corresponds to the total energy that is either dissipated within the network or remains unaccounted for.

When people steal electricity, they often use heavy equipment or inductive loads that pull more reactive power than the grid is designed for. This doesn't just cause technical loss; it actually strains the network, leading to voltage drops and instability that can damage equipment and affect the quality of service for everyone nearby [4] .

For analytical and operational purposes, the total energy losses E_{losses} are further classified into two main categories [3] :

1.4.1 Technical Losses (TL)

Technical losses are inherent to the physical properties of electrical equipment and conductors. They are a direct consequence of the physical laws governing power flow and electromagnetism. TL primarily consists of:

- **Variable Losses (Load Losses):** Proportional to the square of the current flowing through the network $P_{\text{LOSS}} = I^2 \times R$. These Joule heating losses occur in overhead lines, underground cables, and transformer windings.
- **Fixed Losses (No-Load Losses):** Constant losses that occur continuously as long as the equipment is energized, regardless of the load demand. The primary contributors are hysteresis and eddy current losses within the magnetic cores of distribution transformers.

While technical losses can be optimized and minimized through network reconfiguration, reactive power compensation, or upgrading to larger conductor cross-sections, they can never be entirely eliminated.

1.4.2 Non-Technical Losses (NTL)

Non-technical losses, often referred to as commercial losses, occur when electrical energy is successfully delivered to a consumer but remains unmeasured, unbilled, or uncollected. Unlike technical losses, NTLs are completely independent of the physical parameters of the grid [4] . They are driven by socio-economic factors, deliberate human interference, and administrative inefficiencies. Because NTLs represent pure revenue leakage without any underlying physical justification, their detection and eradication are paramount for the financial sustainability of distribution system operators.

1.5 Primary Causes of Non-Technical Losses

In diverse distribution networks, non-technical losses typically manifest through three principal mechanisms. Analyzing these mechanisms is critical for developing targeted detection algorithms.

1.5.1 Direct Electricity Theft (Illegal Hooking)

The most prevalent form of NTL is direct unauthorized tapping into the grid. In regions where the LV network relies heavily on overhead bare conductors, perpetrators physically attach makeshift cables to the utility lines, entirely bypassing the service drop and the energy meter. Consequently, the user can draw unlimited load without generating any billing record. This phenomenon is frequently observed in energy-intensive applications, such as heavy agricultural irrigation pumping or unpermitted industrial workshops, where users seek to evade high operational tariffs [5] .

1.5.2 Meter Tampering and Manipulation

In this scenario, a legitimate account and physical meter exist, but the consumer deliberately manipulates the metering equipment to record only a fraction of the actual energy consumed.

- **Mechanical and Magnetic Tampering:** In traditional electromechanical induction meters, strong neodymium magnets are often placed near the casing to disrupt the magnetic braking field, slowing the rotation of the internal aluminum disk. Alternatively, physical objects are inserted to create mechanical friction.
- **Electrical Bypassing:** Consumers or illicit technicians may alter the wiring configuration at the meter terminal block. Common methods include bypassing the phase wire, reversing the polarity, or disconnecting the neutral line to prevent the current coils from registering the full load.
- **Cyber-Tampering:** As utilities transition to Advanced Metering Infrastructure (AMI) and smart meters, sophisticated consumers may attempt to hack the communication interfaces or manipulate the firmware to alter consumption data before it is transmitted to the utility's data center [4].

1.5.3 Administrative, Infrastructure, and Billing Anomalies

Not all NTLs are the result of malicious consumer behavior; a significant portion originates from internal systemic failures within the utility company itself [3] .

- **Defective Equipment:** Aging meters may drift out of calibration over time, systematically under-registering consumption. Similarly, degraded Current Transformers (CTs) or Potential Transformers (PTs) can provide inaccurate scaling factors to the metering unit.
- **Human Error in Meter Reading:** In systems lacking automated data collection, manual meter reading is prone to typographical errors. If a meter is inaccessible, utility agents may estimate consumption based on historical averages; if the estimation is too low, the unbilled difference becomes an NTL.
- **Database Asymmetries:** Discrepancies between the physical grid and the utility's Customer Information System (CIS) result in "ghost consumers"—households or businesses physically connected to the grid but inadvertently unregistered in the billing database.

1.6 Factors Exacerbating Non-Technical Losses

The complexity of identifying and resolving NTLs is heavily influenced by the operational environment of the distribution network. Several external factors make baseline analysis difficult:

- **Geographical and Topological Disparities:** Dense urban networks often feature complex, multi-layered infrastructures where unauthorized underground bypasses can be easily concealed. Conversely, sprawling rural networks feature extended overhead feeders that are inherently difficult to patrol, providing ample opportunity for illegal line hooking.
- **Seasonal Demand Fluctuations:** Sudden macro-level shifts in consumption—such as extreme peaks during summer due to air conditioning or agricultural irrigation—create "data noise." For a system operator analyzing substation data, distinguishing between a legitimate seasonal load spike and an aggregation of unmetered, stolen energy is highly complex without advanced algorithmic intervention.

1.7 The Impact of Non-Technical Losses

The ramifications of NTLs extend far beyond mere administrative discrepancies. They represent a systemic threat that compromises the utility's financial viability, the grid's physical integrity, and public safety.

1.7.1 Economic and Financial Consequences

The most immediate impact of NTL is a severe deficit in utility revenue. When a utility generates or purchases energy but fails to collect revenue for it, its capacity to reinvest in grid modernization, maintenance, and expansion is crippled. Furthermore, the financial burden of this stolen energy is ultimately socialized, leading to increased electricity tariffs for law-abiding consumers and representing a massive waste of national primary energy resources (such as natural gas or coal used in generation) [5] .

1.7.2 Grid Degradation and Power Quality Deterioration

Unauthorized connections are, by definition, unmonitored and uncoordinated. Consumers bypassing meters often draw excessive, highly inductive loads. This introduces severe power quality issues into the LV network, including significant voltage sags and phase imbalances. Because distribution transformers are sized based on documented load profiles, the hidden demand from electricity theft frequently causes transformers to operate beyond their thermal limits, leading to accelerated insulation degradation, premature equipment failure, and localized blackouts.

1.7.3 Compounding of Technical Losses

There is a parasitic relationship between NTL and TL. Because illegal consumers face no financial penalty for excess usage, their energy consumption is inherently inefficient and exceptionally high. This massive, unmetered current flow directly increases the Joule heating (I^2R) in the localized distribution cables. Therefore, an increase in non-technical losses inherently forces an artificial rise in technical losses.

1.7.4 Safety Hazards

Clandestine connections are typically executed using substandard wiring and bypass all standard utility protection devices, such as fuses and circuit breakers. These illegal setups pose severe electrocution risks to the general public, create massive fire hazards due to arcing and localized overheating, and present lethal dangers to utility line-workers conducting routine maintenance on what they falsely presume to be isolated circuits.

1.8 Geographical, Demographic, and Economic Context of the Mostaganem Wilaya

The deployment, management, and vulnerability of an electrical distribution network are heavily dictated by the characteristics of the territory it covers. The Wilaya of Mostaganem, located in the northwestern coastal region of Algeria, presents a unique geographical and demographic profile that directly influences the operational dynamics of its electrical grid. Understanding this context is a strict prerequisite for studying non-technical losses, as the physical distance between the energy source and the consumer, the density of the housing, and the economic nature of the electricity usage all represent variables in the loss equation.

1.8.1 Topography and Territorial Organization

The urban and coastal areas are densely populated and require heavy-duty infrastructure, especially to handle the massive spikes in electricity demand when tourists flood in during the summer. In stark contrast, supplying power to the rural and agricultural zones means running extremely long power lines across vast distances. Not only does this distance naturally cause energy to bleed out as heat—a technical loss—but the isolation of these areas also makes routine meter reading and surveillance incredibly difficult. This isolation creates the perfect blind spot, allowing non-technical losses like illegal power hookups to go undetected for long periods.

1.8.2 Demographic Evolution and Urban Expansion

To put this rapid growth into perspective, Mostaganem's population has been climbing steadily for decades—growing from roughly 504,000 in 1987 to over 737,000 by 2008 [6] . the number of homes connected to the power network from just 90,000 in the year 2000 to more than 218,000 by the end of 2025.

Impact on Non-Technical Losses (NTL): This massive addition of new delivery points strains the utility's commercial management. Any delay or administrative error between physically connecting a new house to the grid and activating it in the billing system results in temporary unbilled consumption, which directly increases non-technical losses.

1.8.3 Economic Vocation and Sectoral Energy Consumption

Mostaganem boasts a highly diverse economy, driven by a solid mix of agriculture, coastal tourism, manufacturing, and public services. Naturally, this economic variety directly impacts the region's power grid, creating a complex electrical load profile where different sectors pull power at varying times and in different amounts.

On a national level, everyday households are by far the biggest energy consumers, making up about 62% of Algeria's total electricity use, with the number of subscribers growing steadily at roughly 4.6% every year. In Mostaganem, residential use is what really shapes the daily power curve.

Beyond the dominant residential sector, the Wilaya has also seen a major push toward modernizing its agriculture. Since then, at least 568 farms have been officially hooked up to the grid, with another 12 major operations added in early 2024. This initiative is part of a larger

strategy to eventually power up over 90% of eligible farms in the region, aiming for a total of 1,330 connected agricultural sites.

The impact of the Agricultural and Industrial sectors on Non-Technical Losses (NTL):

- **Agricultural Sector:** Farmers need a lot of power, primarily to run heavy irrigation pumps. When you combine this high energy demand with meters that are located in remote, hard-to-monitor areas, it creates a high-risk environment for electricity theft and meter tampering, leading to severe non-technical losses.
- **Industrial & Administrative Sector (Medium Voltage):** Even though these commercial and public clients make up a much smaller portion of the customer base, their individual energy consumption is absolutely massive.
- Commercial management must be absolutely flawless, as even a tiny percentage error in billing translates into a huge financial loss for the distribution company.

1.9 Organizational Structure of Sonelgaz Distribution:

To understand how non-technical losses are managed, recorded, and ultimately fought, it is necessary to examine the corporate and administrative structure of the utility company responsible for the network. In Algeria, the monopoly for the distribution of electricity and gas is held by the Sonelgaz Group, a state-owned enterprise that manages the entire energy value chain from generation to final delivery.

1.9.1 The Restructuring of the Sonelgaz Group:

Over the past two decades, the Sonelgaz Group has undergone several major organizational restructurings to adapt to the growing energy demands of the country and to optimize its operational efficiency. Historically divided into numerous specialized subsidiaries, the group recently consolidated its structure, reducing the total number of its subsidiary companies from 26 down to 14.

Within this modernized holding structure, the core mission of delivering energy to end-users falls to the subsidiary known as Sonelgaz-Distribution (formerly SADEG). Sonelgaz-Distribution operates as the interface between the national high-voltage transmission grid (managed by the transport subsidiary) and the millions of low and medium-voltage consumers across the nation. At the national level, the distribution network spans staggering distances, with over 357,185 kilometers of electricity lines and managing a portfolio of more than 10.4 million electrical clients. The task of managing this immense infrastructure is decentralized through regional directorates and local Wilaya-level distribution directions.

1.9.2 The Direction of Distribution (DD) of Mostaganem

Locally, the electrical and gas networks of the Wilaya are operated by the Direction of Distribution (DD) of Mostaganem, which falls under the broader Regional Distribution Directorate of Oran. Located on the Route d'Oran, the DD of Mostaganem is the absolute focal point for all activities relating to network maintenance, client connection, meter reading, and revenue collection within the Wilaya.

The internal organization of the DD is structured to separate the purely technical management of the physical grid from the commercial management of the client accounts. According to the standard organizational documents of Sonelgaz-Distribution (such as Document n°07 - 2023) [7], a typical Direction of Distribution is articulated around several specialized divisions. The two most critical divisions for the scope of this thesis are the Technical Division and the Commercial Division.

1.9.3 The Technical Division of Electricity (DTE)

The Direction Technique Electricité (DTE) is the engineering and operational heart of the local company. Its primary mandate is to ensure the physical continuity and quality of the electrical supply. The DTE's responsibilities encompass the planning of network extensions, the execution of maintenance programs on medium and low-voltage lines, the management of the primary source substations, and the rapid deployment of intervention teams during power outages.

The DTE is also fundamentally responsible for minimizing physical technical losses. Through load flow studies, the DTE determines optimal conductor sizing, balances the electrical load across different phases of the network to prevent neutral currents, and strategically places capacitors or new transformers to reduce the distance electricity must travel at low voltages. While the DTE focuses heavily on the physics of the network, their work intersects with non-technical losses when their field crews discover unauthorized connections or vandalized infrastructure during routine patrols.

1.9.4 The Commercial Division (DC)

The Direction Commerciale (DC) is tasked with the financial and administrative lifecycle of the electricity consumers. This division handles the establishment of new connection contracts, the physical installation of meters, the periodic reading of those meters, the issuance of bills, and the subsequent recovery of debts.

The Commercial Division is the primary battleground against non-technical losses. A non-technical loss is essentially a failure in the commercial process: electricity flows through the DTE's physical network, but the DC fails to accurately measure or bill for it. This failure can stem from fraudulent actions by the consumer (meter manipulation, bypassing) or from internal administrative shortcomings (data entry errors, incorrect tariff application, or failure to read meters resulting in flawed estimations). The effectiveness of the DD of Mostaganem in reducing non-technical losses relies entirely on the synchronization and data integrity managed by the Commercial Division.

1.9.5 Local Commercial Agencies (Agences Commerciales)

To maintain a physical proximity to the customer base and manage the vast territory of the Wilaya, the commercial operations of the DD of Mostaganem are decentralized into eight distinct local commercial agencies. These agencies are:

1. Mosta-Est (Agency Code 631)
2. Ain Tedles (Agency Code 632)
3. Mosta-Ouest (Agency Code 633)

4. Mesra (Agency Code 634)
5. Sidi Ali (Agency Code 635)
6. Achaacha (Agency Code 636)
7. Hassi Mameche (Agency Code 637)
8. Bouguirat (Agency Code 638)

These local agencies represent the frontline of the distribution company. They house the teams of meter readers (releveurs) who physically traverse the urban streets and rural fields to record consumption indices. The performance of these local agencies in executing accurate, timely meter readings and conducting regular client audits is the most direct mechanism for controlling administrative non-technical losses.

1.10 Technical Architecture of the Electrical Grid

To appreciate how energy is lost, one must trace its path from the point of injection to the point of consumption. The electrical distribution network in Mostaganem follows a standard hierarchical architecture that is governed by the national grid code and technical reference documents utilized by Sonelgaz. The network steps down electricity from the high-voltage transmission backbone to the medium and low voltages required by end-users.

1.10.1 The Source Substations (Postes Sources HTB/HTA)

The boundary between the national transmission network and the local distribution network is defined by the primary source substations, commonly referred to as "Postes Sources HTB/HTA". These highly secure facilities receive electrical power at High Voltage type B (HTB), which in the Algerian context is typically 60 kV or 220 kV, and step it down to Medium Voltage type A (HTA), typically 30 kV or 10 kV, for regional distribution.

A source substation is a complex node housing massive power transformers (often rated at 40 MVA), automated protection relays, circuit breakers, and centralized control systems. Critically, these substations also house the primary energy metering equipment. The total electrical energy entering the Mostaganem distribution network is quantified at the output feeders of these substations. The global loss rate of the entire Wilaya is calculated by taking the sum of the energy measured at these source substations and subtracting the total sum of all the energy billed to the end consumers.

To accommodate the rapid demographic and economic growth of the region, the state continuously invests in upgrading this primary infrastructure. For example, a major project recently completed was the construction of the new 60/30 kV substation in the commune of Ain Nouissy, equipped with two 40 MVA transformers (2x40 MVA). The realization of this substation had a profound impact on the local grid. By providing a massive new injection point closer to the load centers, it alleviated the strain on existing substations, secured the power supply against localized failures, and significantly reduced the length of the medium-voltage lines required to reach the surrounding communes. From a loss perspective, shortening the length of the feeder lines drastically reduces the physical technical losses incurred during energy transit.

Other preparatory programs for the coming years involve the continuous modernization of high-voltage feeding lines and the potential planning of further primary substations to maintain optimal voltage levels across the extremities of the Wilaya.

1.10.2 The Medium Voltage Network (HTA)

Originating from the source substations, the Medium Voltage (HTA) network acts as the primary circulatory system for the Wilaya. In the Mostaganem area, the medium-voltage (HTA) network runs primarily at 30 kV, which is an ideal level for moving energy efficiently across the region. To keep up with local development, the grid is constantly expanding; by the end of 2021, the total length of the HTA network stretched to 2,679.09 kilometers, a noticeable jump from the 2,579.20 kilometers recorded the year before. Physically, this network is built using a mix of overhead lines and underground cables. In contrast, within the dense urban fabric of Mostaganem city and its immediate suburbs, the HTA network is placed underground to ensure public safety, protect against weather-induced faults, and preserve urban aesthetics. These underground HTA cables possess a much higher current-carrying capacity, often limited to 1000 Amperes, and are frequently arranged in open-loop configurations to allow for rapid service restoration by switching supply directions during a localized cable fault.

The HTA network serves two distinct purposes. Firstly, it transports energy to the hundreds of public distribution substations (Postes HTA/BT) scattered across the municipalities. Secondly, it directly supplies the "Grands Comptes" or large account customers. Major industrial factories, large agricultural complexes, and critical infrastructure such as water pumping stations are connected directly to the 30 kV grid. These large consumers own and operate their own private HTA/BT step-down transformers.

1.10.3 The Low Voltage Network (BT)

The final, and by far the most extensive, segment of the electrical chain is the Low Voltage (BT) network. Operating at standard consumer voltages of 380 V for three-phase power and 220 V for single-phase power, this network delivers electricity directly to the meters of residential households, small commercial shops, and light administrative offices.

The scale of the BT network in Mostaganem is vast. By the end of 2021, the cumulative length of the low-voltage lines had reached 4,237.68 kilometers. Because the low voltage level suffers from significant voltage drops over long distances, BT networks must be kept relatively short, radiating outwards from the local public HTA/BT distribution transformers in a radial or sometimes meshed configuration.

To support new housing developments and to rectify historic issues of severe voltage drops at the ends of existing lines, the network undergoes constant restructuring. For the horizon of 2026, the local direction has programmed the installation of 22 new electrical transformers and the extension of the BT network by nearly 50 additional kilometers. This is supported by an overall investment budget estimated at 1.779 billion Algerian Dinars, which covers the creation of new networks, the restructuring of overloaded sectors, and the replacement of aging infrastructure. This follows a similarly aggressive program in 2025 that saw the commissioning of 53 transformers and 33 kilometers of BT extensions.

Despite these massive technical investments aimed at improving service quality, the BT network remains the Achilles' heel of the distribution system regarding non-technical losses. The 4,200+ kilometers of low-voltage lines, consisting largely of overhead twisted cables running along neighborhood streets and building facades, provide endless physical opportunities for unauthorized access. The proximity of the cables to the end-user makes illegal hooking (piratage) relatively simple for malicious actors. Furthermore, the sheer volume of individual connections on the BT network makes exhaustive, continuous physical surveillance nearly impossible, cementing the BT network as the primary source of physical electricity theft.

1.11 Statistical Overview of Network Customers

The physical architecture of the grid is meaningless without an analysis of the end-users it serves. Understanding the distribution of the customer base across the Wilaya provides critical insights into the commercial pressures faced by the local agencies and highlights the geographical areas most susceptible to non-technical losses. An exhaustive review of the network's statistical data for the transition from 2025 to 2026 paints a detailed picture of the Mostaganem concession.

1.11.1 Global Electrification Rates by Commune

The sustained investments by the state and Sonelgaz have resulted in an exceptionally high global electrification rate for the Wilaya of Mostaganem, reaching 94.57% by the end of 2021. This near-universal coverage is a major achievement, yet the specific breakdown by Daïra reveals nuanced differences in network maturity.

Table 3 below details the electrification situation across the major administrative divisions as recorded in the baseline 2021 data [8] .

Daïra / Commune	Total Housing Units	Connected Households	Electrification Rate (%)
Mostaganem	45,418	45,300	99.74%
Mazagran	7,591	7,831	100%
Stidia	3,381	3,472	100%
Hassi Mameche	8,127	8,000	98.44%
Ain Tedles	9,046	8,948	98.92%
Oued El Kheir	4,281	4,166	97.31%
Sirat	4,670	4,710	100%
Sidi Ali	11,593	10,675	92.08%
Bouguirat	8,322	7,392	88.82%
Sour	5,684	2,763	48.61%

Table 1.1: Situation of Electrification by selected communes in the Wilaya of Mostaganem
(Source: Baseline Data 2021).

The data reveals that the urban core and coastal communes (Mostaganem, Mazagran, Stidia) are fully saturated, effectively reaching 100% electrification. In these saturated urban zones, the growth in energy demand comes from increased appliance usage per household rather than new geographical extensions. Conversely, rural communes such as Bouguirat (88.82%) and historically isolated areas like Sour (which recorded an abnormally low 48.61% in older datasets) represent the frontiers of ongoing network extension.

The electrification rate has a direct psychological and operational link to non-technical losses. In areas where legal electrical connection is delayed due to complex terrain, missing urban planning permits, or ongoing construction, residents sometimes resort to illegal, unmetered connections to the nearest available grid point. Thus, areas undergoing rapid transition toward full electrification often require heightened commercial vigilance.

1.11.2 Analysis of the Low Voltage (BT) Portfolio

The low voltage clientele forms the vast majority of the network's connections. According to the internal database of the Mostaganem Concession, the total number of active BT clients stood at an impressive 245,085 at the close of December 31, 2025

The network does not remain static; it is subject to a continuous influx of new connections (Apport clients). For the year 2026, the concession projected the integration of 1,140 new BT clients. The monthly tracking shows a steady climb in the portfolio, moving from 245,349 clients in January 2026, peaking at 245,883 in February, and stabilizing around 245,764 for the remainder of the year as new construction projects are delivered and energized

The management of a quarter-million individual meters is an immense logistical undertaking.

Code Agence	Name of Commercial Agency	BT Clients (End of 2025)	Projected BT Intake (2026)
631	MOSTA-EST	47,991	537
635	SIDI ALI	42,239	104
632	AIN TEDLES	35,480	94
633	MOSTA-OUEST	30,948	82
637	H. MAMECHE	27,827	50
638	BOUGUIRAT	21,836	89
636	ACHAACHA	21,488	40
634	MESRA	17,276	144
Total	Mostaganem Concession	245,085	1,140

Table 1.2: Distribution of Low Voltage (BT) clients by commercial agency (Source: Sonelgaz Data 2026) [9].

1.11.3 Analysis of the Medium (HTA) and High Voltage (HTB) Portfolio

While the low-voltage clients account for the sheer volume of connections, the medium-voltage (HTA) and high-voltage (HTB) clients—referred to as "Grands Comptes" (Large Accounts)—account for a massive, concentrated share of the energy transit.

At the end of December 2025, the Mostaganem Concession managed 937 HTA contracts and 4 HTB contracts. These portfolios are highly dynamic, with factories opening, agricultural sites connecting, and temporary public works sites finishing their projects. By April 2026, the active HTA portfolio had adjusted to 953 contracts, while the HTB portfolio remained rock-steady at 4 contracts.

Code Agence	Name of Commercial Agency	Active HTA Contracts (April 2026)	Active HTB Contracts (April 2026)
631	MOSTA-EST	211	2
637	H. MAMECHE	206	1
633	MOSTA-OUEST	138	0
632	AIN TEDLES	119	1
635	SIDI ALI	95	0
638	BOUGUIRAT	74	0
634	MESRA	70	0
636	ACHAACHA	40	0
Total	Mostaganem Concession	953	4

Table 1.3: Distribution of Large Accounts (HTA and HTB) by commercial agency in April 2026.

The distribution of HTA clients is highly indicative of the economic geography of the Wilaya. Mosta-Est (211 contracts) and Hassi Mameche (206 contracts) dominate the portfolio. This concentration reflects the industrial zones and the intense, modernized agricultural corridors located within their administrative boundaries.

The management of an HTA client is fundamentally different from a BT client. Because a single medium-voltage factory or pumping station can consume more electricity in a day than a small residential neighborhood does in a month, the financial stakes are exponentially higher

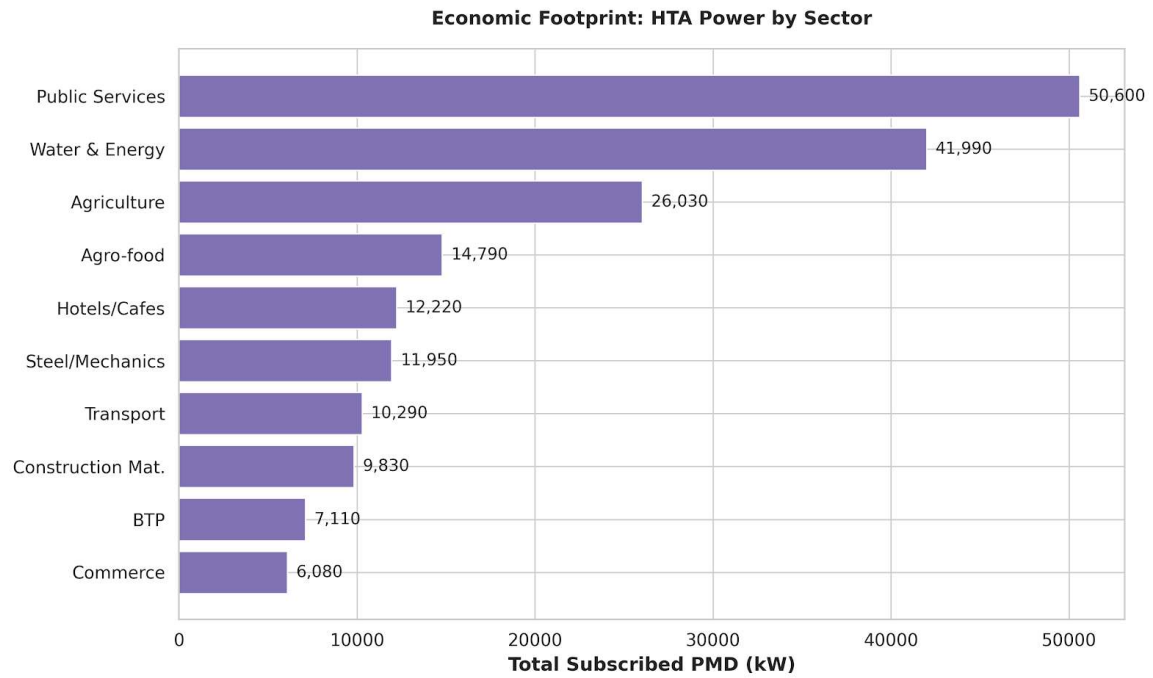


Figure 1.5: Distribution of Subscribed Power (PMD) by Economic Sector.

1.12 Conclusion

The presentation of the electrical network of Mostaganem shows that it is an important and continuously developing infrastructure that serves a growing population and different economic sectors. Managed by the local distribution branch of Sonelgaz, the network includes source substations, medium-voltage lines, low-voltage lines, and a large number of customers distributed across urban and rural areas.

The statistical data presented in this chapter highlights the continuous growth of the customer portfolio, particularly in the low-voltage sector, in addition to the presence of medium-voltage customers in industrial, agricultural, and administrative activities. This growth increases the operational responsibilities of the distribution company in terms of network expansion, maintenance, meter reading, and billing management.

This chapter also showed that the expansion of the network and the diversity of consumers can create different operational challenges that may contribute to energy losses if they are not properly managed.

Chapter 2: Analysis of Non-Technical Losses in Mostaganem Electrical Network

2.1 Introduction and Transition from Network Architecture

Following the comprehensive presentation of the Mostaganem electrical network in Chapter 2—which outlined the geographical context, the organizational structure of the Sonelgaz Distribution Directorate (SDO), the technical architecture, and customer statistics—this chapter focuses on one of the most critical operational and financial challenges facing the utility: non-technical losses. The electrical distribution network of Mostaganem is vast and highly complex, spanning approximately 6,916.78 kilometers of medium and low-voltage lines. It serves a diverse and growing customer base of 217,475 subscribers, comprising 791 Medium Voltage (MV) industrial or commercial clients and over 214,000 Low Voltage (LV) [12] residential and small-scale customers.¹ While the Wilaya of Mostaganem boasts a high overall electrification rate of 94.57%, managing this expansive infrastructure involves mitigating the inevitable dissipation of energy that occurs between the points of injection and the points of final consumption.

non-technical losses are entirely external to the physical constraints of the grid. They represent electrical energy that is successfully delivered into the distribution network by the utility but is never billed to the end consumer, or is billed but the corresponding revenue is never recovered. Nationally, the Algerian electricity distribution network recorded an overall distribution loss rate of 7.8% in the year 2024, operating against a total electricity production volume of 95,181 GWh [11]. Within this margin, non-technical losses account for a massive financial deficit. Historically, these specific losses have cost Sonelgaz between 6% and 7% of its total national turnover, translating into billions of dinars in uncollected revenue.

This chapter provides an analysis of the current situation regarding non-technical losses specifically within the Wilaya of Mostaganem. By examining quantitative operational data, field inspection reports, and the underlying socio-economic and administrative drivers, the analysis isolates the primary causes of these commercial and physical leakages. The discussion explores the multifaceted nature of the problem, encompassing direct electricity theft, sophisticated meter tampering, billing and estimation anomalies, and the severe financial burden imposed by structurally unpaid bills. Furthermore, the geographical concentration of these anomalies across the urban, suburban, and rural communes of Mostaganem is mapped out to provide a localized, context-rich understanding of the phenomenon, paving the way for the technological and organizational countermeasures that must be deployed by the utility.

3.2 The Energy Balance Framework and Loss Quantification

2.2.1 Operational Challenges in the Mostaganem Context

While the energy balance equation is straightforward in theory, its practical application across the Wilaya of Mostaganem presents profound logistical and technical challenges. The implementation of this method relies heavily on the integrity of the metering infrastructure at the High Voltage/Medium Voltage (HV/MV) source substations, such as the 60/30 kV substation situated in Ain Nouissy, which operates with a 2 x 40 MVA capacity to secure the region's supply. By recording the exact energy output of these source substations and comparing it against the aggregate consumption data collected from tens of thousands of Low Voltage

consumer meters over a corresponding billing cycle, the SDO attempts to estimate the volume of unaccounted energy.

However, several operational realities in Mostaganem skew these calculations. First, the synchronization of meter readings is highly problematic. While the HV/MV substation meters can be read instantaneously via telemetry, the LV residential meters are read manually by field agents over a staggered billing cycle. This temporal misalignment between the injection reading and the consumption reading introduces an artificial margin of error into the energy balance.

Furthermore, the integrity of the data is frequently compromised by severe weather events and subsequent network disruptions. For example, during periods of extreme meteorological instability, the Wilaya of Mostaganem frequently experiences high-velocity winds exceeding 90 km/h, which have been recorded causing over 130 simultaneous power outages and downing numerous medium-voltage electrical poles in rural areas like Sidi Ali, Sidi Lakhdar, Ain Tédèlès, and Kheireddine. These violent disruptions force the network into irregular topologies, requiring emergency load shedding and rerouting. During such events, the standard energy balance calculations become highly inaccurate, as energy is injected but dissipated through grounded faults or lost during the transient periods before protective relays trip. Consequently, differentiating between energy lost to a storm-damaged line and energy stolen by clandestine connections becomes exceedingly difficult for the utility's planning and monitoring departments.

2.3 Main Sources of Non-Technical Losses :

A critical, yet often administratively obscured, sub-component of non-technical losses is the phenomenon of unpaid bills, operationally referred to as "créances". In utility economics, energy that is successfully delivered, accurately metered by tamper-proof equipment, and correctly processed by the billing system still constitutes a functional loss if the company is completely unable to recover the associated financial revenue. This commercial deficit directly impacts the operational liquidity of the distributor, paralyzing maintenance schedules and grid expansion projects.

2.3.1 The Scale of the Debt in Mostaganem

Nationally, the volume of unpaid bills held by the Sonelgaz group is staggering, recently reaching approximately 203 billion DZD across all sectors. Within the specific administrative perimeter of the SDO of Mostaganem, the situation mirrors this national crisis and has reached a critical threshold. Recent financial audits and communications from the directorate revealed that the outstanding debt in the Wilaya exceeded 1.8 billion DZD [12]. Furthermore, this debt is not stagnant; it demonstrates a chronic upward trajectory, having grown from 1.7 billion DZD in previous operational years, indicating that existing recovery strategies are struggling to contain the deficit.

This massive volume of uncollected revenue is structurally divided among different classes of consumers, highlighting that non-payment is an institutional and municipal issue just as much as it is a consequence of household financial distress.

Customer Category	Outstanding Debt (Million DZD)	Percentage of Total Local Debt	Contextual Notes
Ordinary Subscribers (Households & Private)	852	~47.3%	Driven by chronic non-payment, economic hardship, and occasional disputes over estimated billing amounts.
Public Function (State Administrations & Enterprises)	776	~43.1%	Encompasses various state-owned facilities, public offices, and administrative buildings.
APC of Mostaganem (Local Municipality)	541	~30.0% (of total)	The single largest recalcitrant debtor in the Wilaya. This forms the bulk of the public function debt.

Table 2.1: Quantitative breakdown of Sonelgaz unpaid bills (Créances) in the Wilaya of Mostaganem.

2.3.2 Impact and Escalating Recovery Strategies

The accumulation of 1.8 billion DZD in unpaid debts severely restricts the SDO's cash flow, forcing the local treasury into what the directorate describes as the "red zone". This lack of liquidity directly hinders the directorate's ability to finance immediate grid reinforcement projects, maintain aging distribution transformers, and invest in loss-reduction technologies such as smart metering networks. The management has explicitly noted that these mounting debts stifle the development of the electrical and gas networks necessary to guarantee continuity and quality of service.

To mitigate this commercial hemorrhaging, Sonelgaz Mostaganem has historically favored dialogue, proximity, and facilitation. The utility has offered extended payment installment plans, kept commercial agencies open on weekends, and heavily promoted the diversification of payment methods, including digital transactions via the BaridiMob application, CIB cards, and the Edahabia postal network. However, faced with the persistent and year-over-year growth of the debt, the SDO has been forced to escalate its recovery procedures. After issuing multiple formal notices (mises en demeure), the directorate has increasingly resorted to the ultimate measure of disconnecting the electricity and gas supply for bad payers, and initiating judicial proceedings against the most persistent commercial and private offenders.

Despite these assertive efforts, the recovery of public sector debt remains highly complex. The 541 million DZD owed specifically by the Assemblée Populaire Communale (APC) of Mostaganem illustrates this difficulty. Disconnecting power to municipal services, public street lighting, or administrative buildings carries severe social and public safety implications, leaving the utility with limited leverage to force immediate payment from state-affiliated entities.

2.4 Physical Vandalism and Infrastructure Sabotage

While unpaid bills represent a commercial failure of revenue recovery, a far more destructive category of non-technical loss is the direct physical theft of grid infrastructure. The theft of copper and aluminum cables, alongside the vandalism of distribution transformers, transcends mere energy loss; it results in the immediate destruction of capital assets, massive service interruptions, and the creation of severe public safety hazards.

2.4.1 The National and Local Impact of Sabotage

At the national level, the Sonelgaz group reported an alarming statistic: over 80% of power outages recorded across the country are directly caused by acts of vandalism and sabotage rather than technical grid failures [11]. In a recent operational period, the utility recorded 16,496 acts of sabotage nationwide, with 12,873 incidents directly targeting electrical networks [11], resulting in a staggering financial prejudice of 5.65 billion DZD. Furthermore, 3,623 incidents targeted heavy infrastructure such as substations and transformers, adding another 400 million DZD in damages.

In the Wilaya of Mostaganem, the situation mirrors this alarming national trend and poses a persistent threat to network stability. A specific operational report from the month of November highlighted the intensity of this phenomenon: within a single month, no fewer than 11 coordinated cases of cable theft were registered on the Mostaganem electrical network. Thieves systematically stripped a total of 5,260 meters of electrical cables from the grid. This specific monthly wave of vandalism inflicted a direct financial prejudice estimated at 2,721,804 DZD on the SDO [13].

2.4.2 Targeted Communes and Operational Consequences

The geographical distribution of these thefts is highly specific. Criminal networks deliberately target rural and isolated communes where the electrical lines traverse uninhabited agricultural fields, forests, or unlit peripheral roads, providing ample cover and time to dismantle the infrastructure. In Mostaganem, the communes most heavily affected by this wave of cable theft include Bouguirat, Sidi Ali, Safsaf, Tazgait, Aïn Tatlès, and Oued El Kheir.

The consequences of this physical vandalism extend far beyond the immediate financial cost of the stolen metals. For the citizens in these rural communes, cable theft results in sudden and prolonged power outages, often occurring in the middle of the night, which disrupts economic activities, threatens the security of agricultural operations, and poses risks to sensitive household appliances. For Sonelgaz, every meter of stolen cable represents a profound setback in grid modernization. The utility is forced to divert critical resources, maintenance budgets,

and technical teams away from planned network upgrades and rural electrification programs, redirecting them instead toward emergency repairs and the repetitive replacement of stolen assets. This cycle of destruction and emergency restoration severely artificially inflates the utility's operational expenditures while simultaneously registering as a massive spike in unbilled, "lost" energy during the period the wires are cut and grounding out.

2.5 Clandestine Connections and Urban Fraud (Piquage Illicite)

Electricity theft via illegal connections—commonly referred to as "piquage illicite"—represents the most visible, dangerous, and widespread form of non-technical loss involving the direct siphoning of energy. This practice is deeply intertwined with the region's demographic shifts, socio-economic challenges, and the dynamics of urban expansion.

2.5.1 The Mechanics of Illegal Tapping

Clandestine connections occur when individuals or unlicensed electricians bypass the utility's metering infrastructure entirely, attaching makeshift wires and cables directly to the low-voltage overhead lines or community distribution pillars. Because the energy is drawn upstream of the consumer meter, it is completely invisible to the billing system, registering purely as a deficit at the local MV/LV distribution transformer during the energy balance calculation. Nationally, the energy stolen through such fraudulent means was estimated to reach 2,430.5 MWh in a single year, generating financial damages of over 11.18 billion DZD.

In Mostaganem, this phenomenon is heavily influenced by the proliferation of unauthorized housing settlements (bidonvilles) and the rapid, sometimes unregulated expansion of the urban periphery. When populations settle in areas without established grid infrastructure, or when state-sponsored housing projects are occupied before the official integration of utility networks, residents frequently resort to illegal hookups to secure basic living necessities. The SDO has actively pursued rural electrification programs to combat this, investing over 700 million DZD to legally connect 1,700 households in isolated regions, and connecting hundreds of rural families in villages like Zehahfa, Kahlala, Touatia, and Doualia [14]. Despite these massive state investments, legacy illegal connections in older slums persist.

2.5.2 Safety Hazards and Grid Degradation

Beyond the severe financial prejudice, illegal connections create extreme hazards for both the perpetrators and the surrounding community. The makeshift nature of these hookups—often utilizing undersized, uninsulated, or poorly spliced wires—leads to significant technical degradation of the local grid. These uncalibrated loads cause severe local voltage drops, phase imbalances, and thermal overloading of the distribution transformers, which can lead to catastrophic equipment failure.

Furthermore, the lack of circuit breakers or protective relays on these clandestine lines creates immense safety risks. The utility has repeatedly warned that illegal connections are a primary cause of electrocutions and urban fires. In densely populated neighborhoods, a spark from an overloaded illegal wire can easily ignite adjacent structures, making this form of non-technical loss a critical public safety issue.

2.6 The Technical Anatomy of Electrical Fraud: Single-Phase vs. Three-Phase Tampering

While clandestine hookups (piquage illicite) are highly visible and prevalent in marginalized areas, a more insidious and financially devastating form of non-technical loss operates behind closed doors: commercial meter tampering. In these scenarios, the customer is legally integrated into the grid but employs sophisticated engineering techniques to blind the utility's metering equipment to their true consumption volume.

To accurately diagnose this vulnerability, we must categorize the mechanisms of fraud based on the grid's underlying electrical architecture. The strategies used to subvert a residential single-phase connection are fundamentally different from those deployed against high-capacity, three-phase industrial loads.

2.6.1 Single-Phase Tampering: The Decentralized Drain (Low Voltage)

In the residential sector, electrical fraud is highly decentralized. While a single manipulated household represents a negligible volume of stolen energy, the cumulative financial impact across tens of thousands of low-voltage households is massive. Fraudsters continuously adapt their methods to bypass utility hardware:

Mechanical and Magnetic Interference: This technique primarily targets older, electromechanical Ferraris-disc meters. Consumers place exceptionally strong, rare-earth magnets directly against the meter's casing. The intense magnetic field violently disrupts the internal electromagnetics, creating a severe braking effect on the rotating disc. This artificially suppresses the registration of active energy, even as the household draws heavy continuous currents.

Neutral Disconnection: A more aggressive and technically dangerous manipulation involves deliberately severing the neutral wire directly at the meter's terminal block. By doing this, the internal voltage coils are starved of a return path, completely shutting down the meter's measurement circuitry. To keep the premises powered, the consumer establishes a localized, unauthorized earth ground to maintain the electrical flow, resulting in massive volumes of "invisible" consumption.

2.6.2 Three-Phase Tampering: High-Stakes Industrial Fraud (Medium/Low Voltage)

The most critical threat to the utility's energy balance does not come from residential neighborhoods, but from the large-scale commercial and industrial sectors. Because these facilities draw massive, continuous loads of three-phase power, manipulating their meters by even a few percentage points evaporates millions of dinars from Sonelgaz's revenue stream.

In these high-capacity environments, standard meters cannot handle the main current directly. Instead, they rely on Current Transformers (CT) and Voltage Transformers (VT) to step the high currents down to safe, measurable parameters. This indirect measurement architecture creates highly lucrative vulnerabilities:

Current Bypassing and Phase Reversal: Sophisticated perpetrators actively manipulate the incoming and outgoing phase wires to run the meter backward. Alternatively, they engineer parallel shunt circuits that route the bulk of the electrical load entirely around the CT sensors, allowing the meter to register only a fraction of the actual current.

Multiplier Ratio Manipulation: If corrupt technicians compromise the meter's digital configuration, they can maliciously reprogram the internal CT/VT multiplier ratios. This algorithmic tampering artificially scales down the registered data, allowing a heavy manufacturing plant to consume massive power while mathematically appearing to the billing system as a moderate user.

Analytical Highlight: The Cold Storage Anomaly

The severity of three-phase tampering is perfectly illustrated by the industrial cold storage sector (*chambres froides*) in Mostaganem. These facilities require immense, uninterrupted energy to maintain three-phase refrigeration cycles.

Recent regulatory audits exposed blatant operational discrepancies. In one documented case, a Mostaganem facility officially declared an active storage capacity of 18,250 quintals to the utility. However, physical field inspections revealed the facility was actively holding and refrigerating 25,000 quintals [15] . This massive gap between the declared capacity and the actual power required points directly to high-level, sophisticated industrial fraud that severely distorts the energy balance of the entire local feeder.

Summary Analysis: Single-Phase vs. Three-Phase Vulnerabilities

To synthesize these findings, the following table contrasts the operational profiles of single-phase and three-phase non-technical losses:

Analytical Parameter	Single-Phase Fraud (Residential)	Three-Phase Fraud (Commercial/Industrial)
Grid Sector	Low Voltage (LV) households.	Medium/Low Voltage (MV/LV) factories, cold storage, hotels.
Financial Impact Model	"Death by a thousand cuts" – Individual losses are small, but cumulative damage is high due to sheer volume.	High-stakes – A single compromised node causes massive, localized revenue hemorrhage.
Technical Complexity	Low to Moderate. Relies on crude physical tampering (magnets, physical disconnections).	High. Requires advanced knowledge of network architecture, CT/VT configurations, and bypass engineering.

Analytical Parameter	Single-Phase Fraud (Residential)	Three-Phase Fraud (Commercial/Industrial)
Primary Tampering Mechanisms	Magnetic braking of electromechanical discs; Neutral wire disconnection.	Phase reversal; CT sensor bypassing; Software manipulation of multiplier ratios.
Utility Countermeasures	Widespread meter modernization; visual field inspections.	Software diagnostics (e.g., <i>ACE Pilote</i>); automated load profile analysis; algorithmic anomaly detection.

Table 2.2: Comparison between Single-Phase and Three-Phase Electricity Fraud Profiles

2.7 Administrative Weaknesses and Estimation Anomalies

It is crucial to recognize that a significant portion of non-technical losses stems not from malicious theft, but from logistical failures, administrative bottlenecks, and estimation errors inherent to the utility's billing cycle.

2.7.1 Inaccessible Meters and "Forfaitaire" Billing

In many traditional residential buildings and historic neighborhoods in Mostaganem, electricity meters are physically located inside the private premises rather than in accessible external technical cabinets. When a Sonelgaz reading agent is unable to access the property during the scheduled reading cycle—due to the absence of the homeowner—the utility is forced to issue an estimated bill (facturation au forfait) based on historical consumption averages.

While estimation is a standard utility practice, it frequently generates artificial non-technical losses. If the customer's actual consumption has surged—for instance, due to the installation of new air conditioning units during the intense summer heat—the estimated bill will fall significantly short of the true energy delivered. Although this discrepancy is theoretically self-correcting once a physical reading is eventually obtained, chronic inaccessibility leads to prolonged periods where consumed energy is effectively "lost" from the utility's immediate revenue stream. Furthermore, when corrections are finally applied, the resulting massive adjustment bills frequently trigger customer disputes, leading to prolonged non-payment and adding to the aforementioned burden of "créances".

2.7.2 Database Delays and Organizational Complicity

Errors in the centralized billing system also generate non-technical losses. Technical glitches during the manual transcription of meter indices by reading agents, or failures in the prompt integration of new customers into the IT database, create blind spots in the network. If a newly electrified neighborhood is not immediately activated in the commercial software, the energy consumed by those households registers as a total loss at the substation level until the administrative bottleneck is resolved.

Moreover, the integrity of the billing cycle is occasionally compromised by internal organizational weaknesses. Previous regional analyses have highlighted the issue of excessive centralization in customer management and the severe consequences of complicity among field personnel. When field agents are tasked with overseeing vast, difficult-to-monitor geographical areas, the supervision of their work becomes strained. Collusion between utility personnel and consumers—where agents are bribed to overlook tampered meters, ignore clandestine connections, or deliberately record artificially low index values—represents a profound breach of organizational integrity. The lack of strict, randomized internal audits allows these fraudulent behaviors to persist for extended periods, compounding the financial deficit.

2.8 Geographical Mapping of Non-Technical Losses

By combining the various typologies of fraud and administrative errors, a distinct geographical mapping of non-technical losses emerges across the Wilaya of Mostaganem. The nature of the loss is heavily dictated by the local socio-economic context, urban density, and the age of the infrastructure.

Zone Typology	Key Communes / Neighborhoods	Primary Characteristics of Non-Technical Loss
Historic and Dense Urban Centers	Tidjdit, Derb, Kharouba, Hai Salam	Characterized by highly complex, aging urban fabrics with narrow alleys. The proximity of housing units facilitates clandestine hookups that are difficult for inspectors to visually trace. High prevalence of meter tampering and commercial fraud.
High-Consumption Suburban & Coastal Zones	Hassi Mameche, Fornaka, Mazagran	These areas experience massive surges in energy demand during the summer months due to intensive air conditioning usage. As consumption peaks, the financial incentive to bypass the meter increases proportionately, leading to seasonal spikes in non-technical losses.
Rural and Agricultural Expanses	Bouguirat, Sidi Ali, Safsaf, Aïn Tatlès, Oued El Kheir	Characterized by long stretches of isolated overhead lines. These zones are the primary hotspots for destructive cable theft and vandalism.

		Historically, unauthorized agricultural extensions also occurred here, though recent programs connecting 568 farms without upfront fees aim to formalize these draws.
--	--	---

Table 2.3: Geographical distribution and dominant typologies of non-technical losses in Mostaganem.

2.9 Technological Diagnostics and Advanced Current Detection Technologies

To transition from a reactive to a proactive posture regarding non-technical losses, Sonelgaz is increasingly relying on advanced metering infrastructure, intelligent software platforms, and data analytics. In the industrial and high-consumption commercial sectors of Mostaganem, the deployment of sophisticated electronic meters, such as the Itron ACE6000 series, provides the SDO with powerful, automated diagnostic tools [10] .

2.9.1 Hardware-Level Surveillance (ACE6000 Capabilities)

Modern electronic meters are no longer simple recording devices; they are equipped with internal event managers and active surveillance functions designed specifically to detect physical tampering and fraud. By interrogating the internal logs of these meters via optical interfaces or remote communication protocols using specialized management software like *ACE Pilote*, utility inspectors can pinpoint the exact timestamps of fraudulent activities [16].

Function	Description
Anti-fraud measurement method	The meter can be configured to record energy with an anti-fraud algorithm
Sealing of the meter and terminals	The meter body and terminal cover can be sealed separately using traditional lead seals or plastic covers.
Protection of electrical connections	Access to the connections requires the removal of the sealed terminal cover.
Monitoring	Anti-fraud events, for example: current reversal or phase reversal Neutral voltage and current sequence Time without internal consumption above a threshold Overcurrent These are recorded in time-stamped events, which can be read on the meter.
Reversed energy	It is recorded in the time-stamped events, which can be read on the counter. Indication provided by a warning on the LCD screen.
Configurations	When one of the meter's aspects is

	programmed, the meter records the number of configured objects as a time-stamped event. Parameters typically associated with fraud include: - reprogramming the calendar (seasons, daily profiles, index) - reprogramming the current transformer (CT)/voltage transformer (VT) ratio
Indication for removing the cover of the meter and/or the terminal cover	Recorded in time-stamped events: - start date of lid opening - duration - number of lid openings Detection remains active during power outages (one opening is counted, regardless of the number of incidents)

Table 2.3: Geographical distribution and dominant typologies of non-technical losses in Mostaganem.



Figure 2.1: Front panel of the Itron ACE6000 electronic meter showing the LCD display, optical communication port, and metrological LEDs

2.9.2 Software Diagnostics and LCD Error Codes

During routine field inspections in Mostaganem, agents can rapidly assess the integrity of an installation without requiring complex software interfaces by reading the hexadecimal error codes directly displayed on the meter's LCD screen. According to the diagnostic protocols for these devices, system alarms are structured in quartets (demi-octets), providing highly specific information regarding the type of fault or fraud detected.

Table 3.3 illustrates the specific diagnostic codes related to fraud and network anomalies that Sonelgaz agents utilize to identify tampered installations:

2.9.3 The Shift Toward Data Mining and Profiling

Beyond physical hardware alarms, the analysis of non-technical losses is fundamentally evolving toward data-driven, macroscopic approaches. By extracting continuous load profiles (courbes de charge) from digital meters, analysts can utilize advanced pattern recognition algorithms and artificial intelligence techniques—such as Support Vector Machines (SVM)—to flag suspicious consumption behaviors across the network

For example, a sudden, unexplained drop in a commercial client's load profile that is entirely unaligned with seasonal temperature variations or standard business operating hours serves as a high-probability statistical indicator of newly installed bypasses or meter tampering. Integrating these IT-driven diagnostic models is crucial for the Mostaganem directorate. It allows the administration to shift from a random inspection strategy to a highly targeted approach, efficiently allocating its limited field inspection teams to the specific substations and individual clients presenting the highest statistical probability of fraud.

Using the ACE Pilote software interface, inspectors have the ability to precisely extract and select specific datasets for offline analysis. According to the software's user guide, these include

- Date, time, and meter ID
- Meter status
- Log
- Network history
- Fraud data
- Meter history
- Voltage quality data
- Instantaneous data
- Total energy records
- Power records
- Peak power records
- Partial load curve reading 1

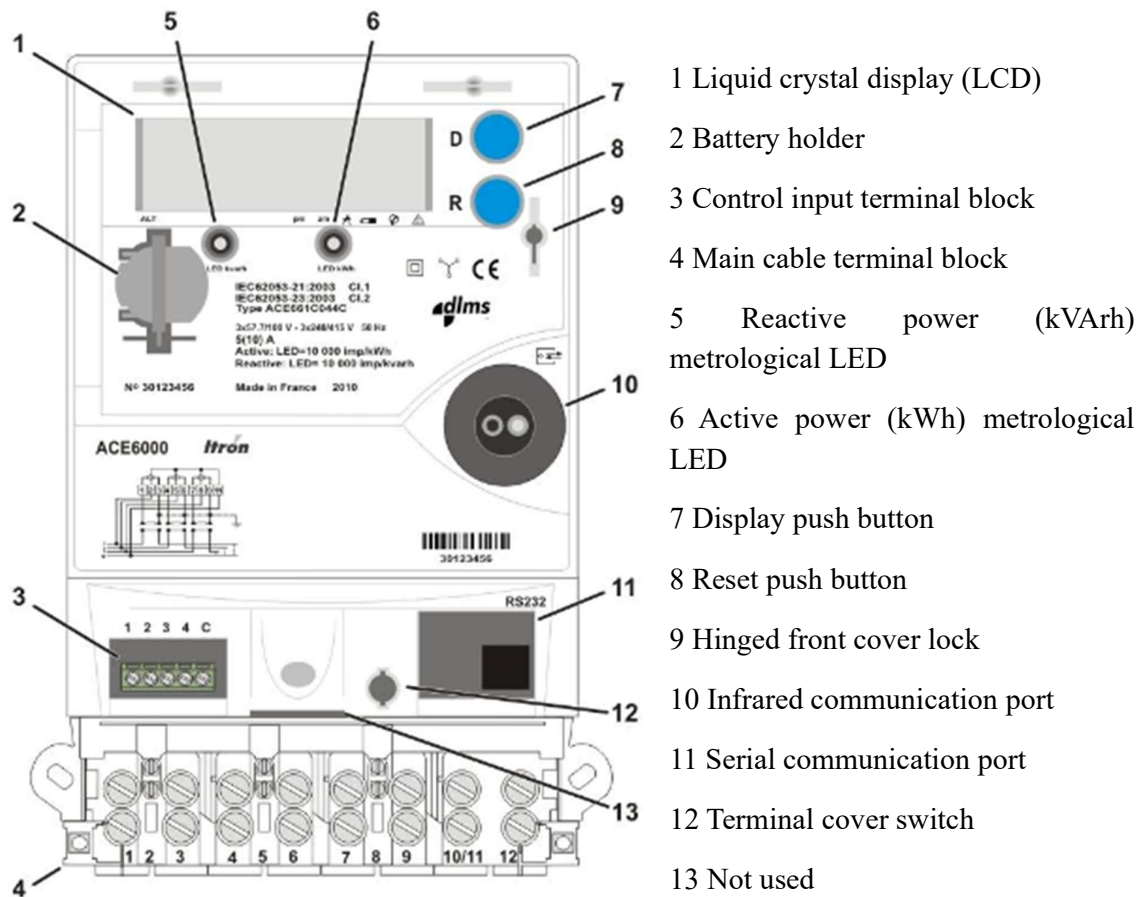


Figure 2.2 : Itron ACE6000
Electricity Meter Components

As shown in Figure 2.2, the software provides a comprehensive visual interface that enables analysts to track consumption trends, identify synchronization issues, and pinpoint the exact moments of suspected meter tampering [10].

2.10 Conclusion

The comprehensive analysis of non-technical losses within the Mostaganem electrical network reveals a deeply entrenched and multifaceted crisis that extends far beyond simple engineering inefficiencies. Estimated to cost the utility billions of dinars annually—most glaringly highlighted by the staggering 1.8 billion DZD in accumulated unpaid bills alone—these losses are rooted in complex socio-economic behaviors, rapid urban expansion, and persistent administrative bottlenecks.

The geographical mapping demonstrates that the phenomenon adapts to its environment. While dense urban centers like Tidjdit and Derb suffer heavily from sophisticated meter tampering and clandestine residential hookups, the vast rural expanses of the Wilaya are increasingly victimized by highly destructive, organized cable theft, which severely compromises grid stability and drains maintenance budgets. Concurrently, internal administrative hurdles, such as inaccessible residential meters leading to inaccurate estimated billing, and the slow integration of new customer data, create artificial, yet financially damaging, gaps in the region's energy balance.

While modern metering technology—exemplified by the deployment of the ACE6000 series and its associated diagnostic software—provides the SDO with unprecedented capabilities to track and mathematically log instances of reverse current, neutral loss, and physical tampering, technology alone is insufficient without robust organizational enforcement. The massive accumulation of structural debt, particularly by dominant municipal entities like the APC of Mostaganem, unequivocally demonstrates that commercial losses require sustained political and administrative resolutions, not merely technical patches.

Chapter 3: Proposed Solutions for Reducing Non-Technical Losses in Mostaganem Electrical Network

3.1 Introduction

Reducing non-technical losses (NTL) is one of the most important steps to improve the efficiency and financial health of any electrical distribution network [4] , [5]. In this chapter, we will discuss the various practical solutions available to tackle this problem., the main goal here is to evaluate these solutions based on the actual reality of the Mostaganem province [20].

Mostaganem is a region with a diverse geography; it includes crowded urban centers, rapidly growing suburban neighborhoods, and wide agricultural and rural areas. Because of this diversity, a single, universal solution will simply not work everywhere. What is highly effective in a city building might be too expensive or completely impractical for a remote village.

Therefore, to provide a realistic framework that the local utility company can actually use, we will categorize our proposed solutions into two main areas. First, we will examine technical prevention methods, which involve physical upgrades and equipment changes to the grid to stop theft at the source. Second, we will discuss administrative and commercial actions, which focus on fixing internal management errors, improving billing accuracy, and dealing with the legal and social sides of the problem.

3.2 General Technical and Practical Solutions

3.2.1 External Meter Relocation

In many neighborhoods across Mostaganem, especially in older urban areas and traditional houses, electricity meters were historically installed inside the home, in hallways, or behind locked courtyard gates. While this was standard practice in the past, it currently creates two major vulnerabilities for the utility company.

First, it leads to a massive administrative problem. When utility agents (Sonelgaz) do their rounds to read the meters during regular working hours, many families are simply not home. Without physical access to the meter, the company is forced to issue "estimated bills" based on the customer's past consumption. If the family used more power than estimated, that unbilled energy automatically shows up in the system's records as a non-technical loss. Second, an indoor meter provides a safe, hidden environment for deliberate electricity theft. A consumer can comfortably bypass the internal wiring, break the seals, or slow down the meter disk behind closed doors without any fear of being caught by a sudden inspection.



Figure 3.1: Electrical Meter Box

External meter relocation is a highly practical and logical solution to both of these problems. This process involves moving the meters from inside the private property to the exterior boundary walls, or grouping them together into standardized, locked street cabinets (often referred to as *coffrets de comptage*) [19] .

From an operational standpoint, this change is highly effective. It gives utility inspectors 100% unrestricted access to read or audit the meters at any time of the day, completely eliminating the need for estimated bills. Furthermore, placing the meter in a public space acts as a strong physical and psychological deterrent. It becomes extremely difficult and risky for a customer to secretly manipulate the wires when the equipment is fully exposed to the street, neighbors, and passing utility patrols. For a province like Mostaganem, this represents a very realistic, affordable, and immediate physical intervention to secure the network, especially when compared to the massive budget required for full smart meter deployment.

3.2.2 Smart Meter Installation

Moving from traditional electromechanical meters to smart meters, often part of an Advanced Metering Infrastructure (AMI), is widely considered the modern standard for upgrading electrical grids [16]. Unlike older meters that simply record total consumption on a mechanical dial, smart meters are active digital communication devices. They measure electricity usage precisely and automatically transmit this data back to the utility's central system using communication networks, such as GSM, 3G/4G, or Radio Frequency (RF).

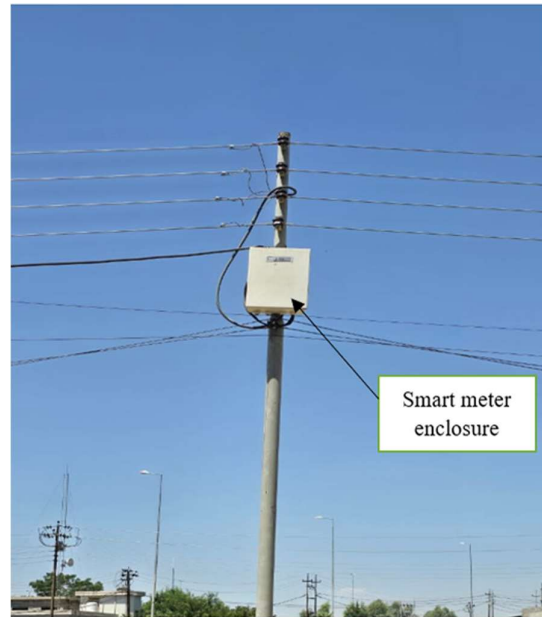
From an operational perspective, this technology directly targets non-technical losses in two main ways. First, it completely removes the need for human meter readers to physically visit every house. This single change eliminates manual reading mistakes, stops the practice of sending "estimated bills" when customers are not at home, and prevents any potential collusion between the meter reader and the consumer. Second, and most importantly for theft prevention, smart meters are equipped with internal anti-tampering mechanisms. If someone attempts to physically open the meter cover, bypass the phase wire, or reverse the electrical current, the meter instantly registers the anomaly [4] [17].



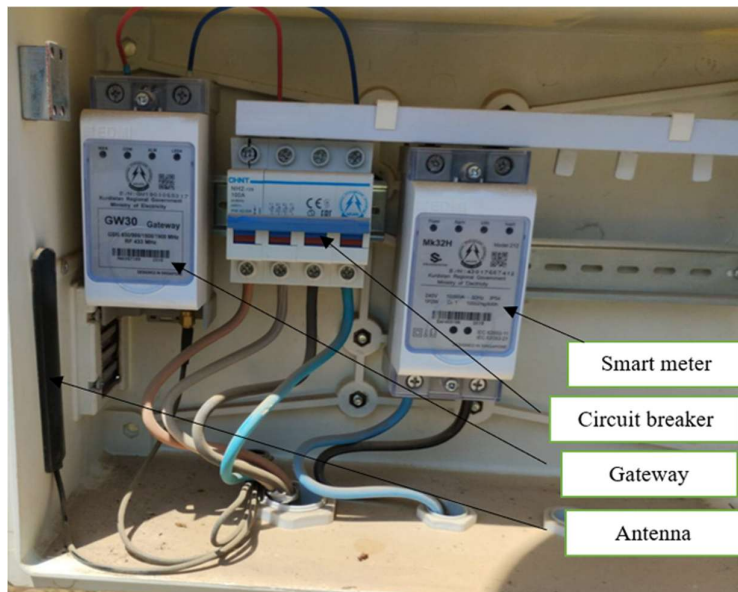
Figure 3.2 : smart meter

To further enhance the physical security of these devices, one highly effective field configuration is to install the smart meters inside locked enclosures mounted high up on electricity poles, rather than at eye level. As illustrated in **Figure3 3.**, this specific setup creates a formidable physical barrier against tampering. Inside the enclosure, the system typically houses the smart meter itself, a circuit breaker, a communication gateway, and an antenna.

Placing the equipment at such a height makes unauthorized physical access extremely difficult and dangerous for potential thieves. Even if a determined fraudster somehow attempts to force the box open, the enclosure's security mechanisms will instantly trigger an alert to the utility company so they can take direct action. Meanwhile, the integrated gateway and antenna ensure that all customer consumption data is continuously and securely transmitted over the wireless network directly to the central control room.



a



b

Figure 3.3: Smart Meter (SM) implementation: (a) External enclosure mounted on a utility pole; (b) Internal components of the SM system.

While smart meters offer excellent technical benefits, they come with a very high initial financial cost. Implementing this solution requires not only purchasing thousands of expensive digital meters but also building the necessary IT infrastructure, setting up secure data servers, and paying continuous telecommunication fees for data transfer. For the local utility company, replacing the entire existing fleet of meters across all urban and rural areas of the province is financially impossible in the short term. Instead, it makes more economic sense to consider

smart meters as a gradual solution, perhaps starting only with industrial customers or specific distribution transformers that have a proven history of extremely high losses.

3.2.3 Prepaid Metering Systems

One of the biggest financial headaches for any utility company—including Sonelgaz here in Mostaganem—is collecting payments after the electricity has already been consumed. Prepaid metering systems flip this traditional model entirely. Instead of receiving a bill at the end of the month, consumers buy electricity credit in advance, much like a prepaid mobile phone plan. In Mostaganem, this would be particularly effective in transient areas like student housing near the university or commercial rental spaces in the city center. It completely eliminates the risk of unpaid bills and commercial debt. Furthermore, when consumers can actually see their credit dropping in real-time, it creates a psychological shift; they tend to conserve more energy and are far less likely to attempt tampering, knowing the system is strictly "pay-as-you-go."



Figure 3.4: Smart card prepaid electric meter

this **figure 3.3** is an example of prepaid smart metering

3.2.4 AI and Data Analytics for Theft Detection

While deploying teams to the streets is essential, doing it blindly across a province as large as Mostaganem is a massive drain on limited resources. This is where Artificial Intelligence (AI) and data analytics come into play [16]. By feeding historical consumption data into an AI algorithm at the control center, the system can automatically flag highly suspicious behavior. For instance, if a large villa in the Salamander neighborhood suddenly shows a drastic drop in electricity usage during the peak summer months—when air conditioners should be running at maximum—the algorithm instantly creates an alert. Instead of random checks, Sonelgaz can generate highly accurate "suspect lists," ensuring that when an inspection team is sent out, they are almost guaranteed to find a discrepancy [17].

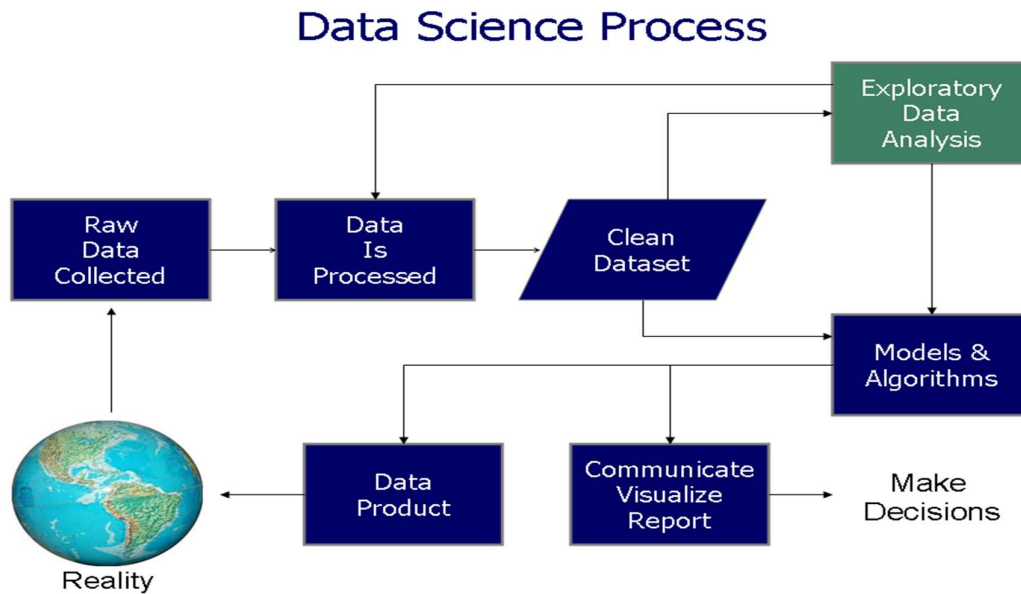


Figure 3.5 : Data visualization process

3.2.5 GIS-Based Monitoring and Mapping

Given the diverse and sometimes complicated geography of Mostaganem—from the dense, winding streets of traditional neighborhoods to the wide agricultural perimeters of the Dahra region—having a clear spatial understanding of the grid is crucial [8]. Geographic Information Systems (GIS) allow the utility to build a dynamic, digital map of the entire distribution network [2] [18]. By overlaying customer data, transformer locations, and billing records onto this map, technicians can visually pinpoint "red zones" where the energy injected simply does not match the energy billed. This mapping is actually the foundational step that makes the "micro-energy balancing" strategy (discussed earlier) possible, as it tells the company exactly which streets or rural feeders are suffering the highest losses.

3.2.6 Consumer Awareness and Public Campaigns

electricity theft isn't just an engineering problem; it's a human one [5]. In some communities, bypassing a meter is unfortunately seen as a minor, victimless offense rather than a serious crime that degrades public infrastructure. Technical upgrades must therefore be supported by a shift in social mentality. Launching sustained public awareness campaigns is a low-cost but highly effective strategy [19]. By using local radio or community outreach, Sonelgaz can educate citizens about the real dangers of illegal hookups, such as the severe risk of electrocution or electrical fires. Moreover, when people understand that their neighbor's stolen electricity is exactly what causes the annoying voltage drops and power cuts in their own homes, the community itself becomes a deterrent against casual fraud.

3.3 Single-Phase Targeted Solutions

In the residential sector, single-phase fraud individual losses may be small, but the cumulative financial damage across thousands of households is massive. The strategy here must focus on localizing the theft efficiently.

3.3.1 Micro-Energy Balancing at Transformer Level

In densely populated historic centers like Tidjdit or Derb, clandestine hookups are easily hidden within the complex, narrow urban fabric, making them incredibly difficult for inspectors to visually trace. Searching these neighborhoods blindly is a waste of limited utility resources.

Micro-energy balancing solves this by installing a master measurement device directly at the output of a specific Low Voltage distribution transformer feeding a targeted neighborhood [2] [18]. By calculating the total energy injected into that local grid and comparing it against the aggregate consumption of all billed single-phase meters connected to it, the utility can accurately isolate the missing energy. If the injected energy significantly exceeds the billed consumption, the utility instantly knows that illegal hookups or meter tampering exist within that exact street. This allows the company to deploy inspection teams strictly to identified "red zones."

3.4 Three-Phase Targeted Solutions

Three-phase connections represent the highest financial stakes for the utility. In Mostaganem, the vast rural and agricultural expanses—such as Bouguirat, Sidi Ali, and Safsaf—are primary hotspots for unauthorized extensions and heavy infrastructure vandalism. Solutions here must serve as severe physical deterrents.

3.4.1 Asymmetric Phase Distribution: A Physical Deterrent Strategy

A frequent method of theft in rural communes involves throwing hooks over bare overhead lines to power heavy, three-phase agricultural equipment, such as unauthorized water pumps. A highly innovative and effective engineering countermeasure to this specific type of theft is the implementation of asymmetric phase distribution.

In a standard electrical network, three-phase power is distributed with perfect symmetry, maintaining a 120° angle between the phases to generate the uniform rotating magnetic field required by standard induction motors. However, to deter theft, the utility can intentionally modify the transformer winding configurations on vulnerable rural feeders to create asymmetric phase angles (for example, shifting the angles to 60°, 50°, and 130°).

This physical trap exclusively targets the thief. Legitimate residential consumers connected to the grid use only a single phase and a neutral wire; therefore, their household appliances will operate perfectly normally, completely unaffected by the shifted angles. However, if a fraudster attempts to steal power by connecting an unauthorized three-phase motor to this asymmetric grid, the lack of a 120° displacement will generate massive negative sequence torques within the machine. This results in violent mechanical vibrations, immediate overheating, and the rapid destruction of the stolen motor, serving as an ultimate physical and financial deterrent.

3.4.2 Smart Three-Phase Meter Tampering Detection at the Terminal Level

To implement efficient anti-theft solutions in the high-stakes industrial and agricultural sectors of Mostaganem, it is critical to understand the technical anatomy of how three-phase fraud is physically executed. **Figure 4.6** provides a standardized wiring diagram for a 3-Phase 4-Wire static meter connection. A precise analysis of this connection layout reveals exactly why traditional electromechanical meters are so vulnerable, and how modern smart meters are engineered to combat these specific fraud methods [4] .

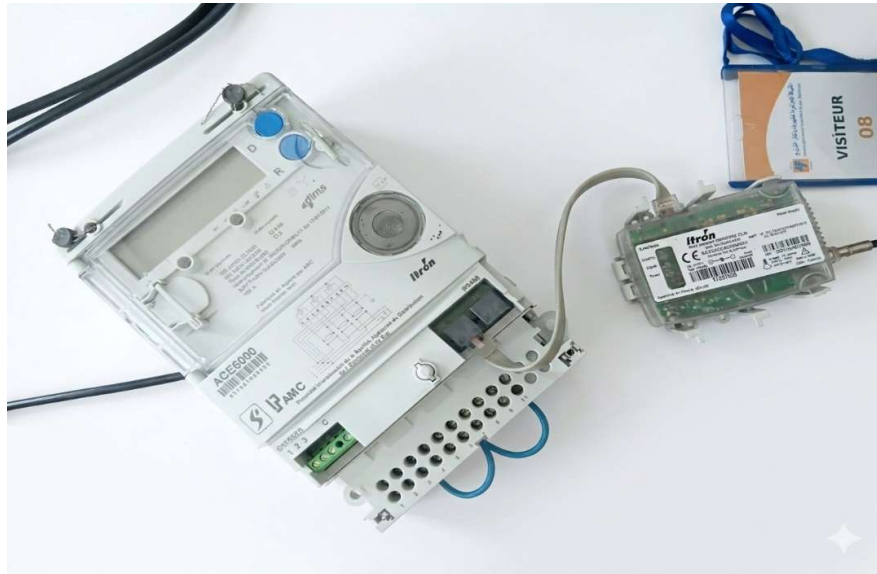


Figure 3.6: 3-Phase 4-Wire Meter Connection Diagram (showing Terminals 1, 3, 4, 6, 7, 9 for Phases L1, L2, L3 and Terminals 10, 12 for Neutral)

The vulnerability lies within the accessible terminal block. By understanding the wiring path shown above, a fraudster can execute simple but devastatingly effective theft techniques:

1. **Neutral Missing or Disconnection (Terminal 10/12 Manipulation):** This is one of the most common and dangerous frauds. If the neutral reference wire is disconnected at Terminal 10, older electronic meters fail to power their internal measurement circuits correctly, often ceasing to record any consumption while the consumer continues to pull massive power from all three phases, using an arbitrary or ground connection elsewhere.
2. **Phase Bypass or Current Reversal (Terminals 1/3, 4/6, or 7/9 Manipulation):** As seen in the diagram, power flows from 'Supply' to 'Load'. A thief can simply create a physical shunt (jumper) across terminals 1 and 3, effectively bypassing the internal current coil of Phase L1. Only a fraction of the current is measured, drastically reducing the bill. Alternatively, reversing the incoming and outgoing wires causes older meters to run backward.

The Smart Solution using this Diagram:

Modern smart meters deployed within an AMI framework, utilizing this very connection layout, possess advanced embedded intelligence to detect these actions the instant they occur.

Instead of needing field audits to visually trace these wire connections, the AMI system relies on:

- **Integrated Terminal Block Cover Sensors:** The physical cover over terminals 1 through 12 is equipped with a microswitch. If a fraudster attempts to open it to manipulate any of the phase or neutral connections shown in Figure 4.6 , the meter immediately logs a "Cover Open" event and sends a tamper alarm to the central system, facilitating instant enforcement actions.
- **"Neutral Missing" or "Per-Phase Unbalance" Alarms:** Smart meters utilizing this diagram are programmed to operate without a neutral reference (drawing internal power from Phase-to-Ground instead of Phase-to-Neutral). If the neutral wire is disconnected at Terminal 10, the meter does not shut down. Instead, it measures the voltage anomaly against ground and instantly generates a "Neutral Missing" tamper event, continuing to record power consumption perfectly based on internal calculated virtual ground.

3.4.3 Replacement of Bare Conductors with ABC Cables

Physical sabotage and direct tapping in isolated rural communes pose a persistent threat to network stability. The intensity of this issue is severe; in just one month, thieves in Mostaganem systematically stripped 5,260 meters of electrical cables, inflicting a direct financial prejudice of over 2.7 million DZD and causing sudden [20], prolonged power outages for citizens.

To physically secure the grid from both this destructive theft and clandestine connections (piquage illicite), replacing older bare wires with insulated Aerial Bundled Cables (ABC) is an essential upgrade. In an ABC system, the phase and neutral conductors are heavily insulated and tightly twisted together into a single bundle. This design makes it physically impossible for individuals to simply throw metal hooks over the line. To access the electricity, a perpetrator would need specialized tools to pierce the heavy insulation, which requires considerable time and carries a severe, immediate risk of lethal electrocution, effectively neutralizing the threat at the source [19] [18] .

3.5 Conclusion

In conclusion, this chapter has demonstrated that managing non-technical losses in the Mostaganem electrical network is a multi-dimensional challenge. It is not merely an engineering issue that can be instantly fixed by simply purchasing and installing expensive, high-end technology across the entire grid. While advanced solutions like smart metering infrastructure and completely replacing bare overhead lines with ABC cables represent the ideal technical standard for the future, our comparative analysis shows that they are currently limited by severe financial and logistical constraints.

Instead, the most practical and realistic approach for the local utility company right now is to adopt a targeted, mixed strategy. By strictly enforcing daily administrative checks, updating subscriber databases, and correcting internal billing errors, the company can stop a massive portion of commercial losses at virtually no cost. When this administrative rigor is combined with affordable physical prevention strategies—most notably the systematic relocation of meters to the outdoors and focused field inspections—the utility can establish a strong, highly visible deterrent against electricity theft. This balanced approach directly attacks the root of the problem, optimizing the network's efficiency without requiring an impossible budget.

Chapter 4: Dynamic Simulation of Electricity Theft and Automated Deterrence in a Medium Voltage Network

4.1 Presentation of the Case Study: The Mostaganem HTA Network

For this practical application, I chose to focus on the Medium Voltage (HTA 30 kV) sector managed by the Sonelgaz Distribution Directorate of Mostaganem (SDO). The reason for this choice is straightforward: while low-voltage residential electricity theft is common, the financial impact of a single industrial client (classified as *Grand Compte*) stealing electricity is devastating for the utility's budget.

In this case study, we are focusing on a typical heavy commercial unit—such as a large agricultural cold storage facility (*Chambre Froide*), which is a very common profile in local agencies like *Mosta-Est* or *Hassi Mameche*. According to the commercial database, these clients usually subscribe to high power capacities (e.g., 400 kW) to run heavy cooling motors.

The core problem arises when some of these clients intentionally bypass their billing meters to avoid high bills during peak summer seasons. This creates a massive gap between the energy injected by the Sonelgaz transformer and the energy actually registered by the client's meter. In the following sections, we will track this anomaly from the billing tables all the way to the Simulink electrical model.

4.2 MATLAB/Simulink Implementation and Network Parameters

In this section, a physical and logical simulation of the Mostaganem Medium Voltage (HTA) network was developed using MATLAB/Simulink (Simscape Electrical). The purpose of this model is twofold: to physically simulate a meter bypassing fraud (Non-Technical Loss) committed by a heavy industrial client, and to implement a digital "Smart Meter Logic" circuit capable of real-time anomaly detection.

The electrical model consists of a 30 kV three-phase source (representing the Mostaganem HTA grid) that is stepped down to 400 V via a 1 MVA transformer. This setup feeds a 400-kW industrial load through a 0.1 km distribution line. Two measurement nodes were established: Meter 1 records the total power injected by the transformer, and Meter 2 represents the client's billing meter.

To model the physical fraud, a Three-Phase Breaker was installed to act as a bypass line around Meter 2, programmed to activate precisely at $t = 0.5$ seconds. Finally, to simulate the Smart Metering algorithm, a logical circuit was integrated. A Subtract block continuously calculates the difference in active power between Meter 1 and Meter 2. This result is fed into a Compare To Constant block acting as a threshold alarm to detect any missing energy that exceeds normal technical losses.

The simulation was executed in Discrete mode with a sample time of 50 micro-seconds for a total simulation time of 1.0 second. The exact electrical and logical parameters configured within the Simulink blocks are detailed below.

MATLAB/Simulink Block Parameters for the HTA Network Simulation

1. Simulation Settings (powergui)

- Simulation Type : Discrete
- Sample Time (Ts): 50e-6 s
- Stop Time : 1.0 s

2. Three-Phase Source

- Phase-to-phase rms voltage: 30e3 V
- Frequency : 50 Hz
- 3-phase short-circuit level: 500e6 VA

3. Three-Phase Transformer

- Nominal power and frequency: 1e6 VA, 50 Hz
- Winding 1 (Primary): 30e3 V, R = 0.002 pu, L = 0.08 pu
- Winding 2 (Secondary): 400 V, R = 0.002 pu, L = 0.08 pu

4. Three-Phase PI Section Line

- Line length: 0.1 km
- Positive-sequence resistance (R1): 0.025 Ohms/km
- Zero-sequence resistance (R0): 0.09 Ohms/km
- Positive-sequence inductance (L1): 0.2387e-3 H/km
- Zero-sequence inductance (L0): 0.6e-3 H/km
- Positive-sequence capacitance (C1): 113.3e-9 F/km
- Zero-sequence capacitance (C0): 50.1e-9 F/km

5. Three-Phase Series RLC Load

- Nominal phase-to-phase voltage: 400 V
- Active power (P): 400e3 W
- Inductive reactive power (QL): 100e3 var

6. Three-Phase Breaker (Bypass)

- Initial state: 0 (Open)
- Switching times: 0.5 s

7. Compare To Constant (Smart Logic)

For full bypass Scenario :

- Constant Value (Threshold): 20000 (20 kW)

For Advanced Scenario Asymmetric Phase Bypassing :

- Constant Value (Threshold): 60000 (60 kW)

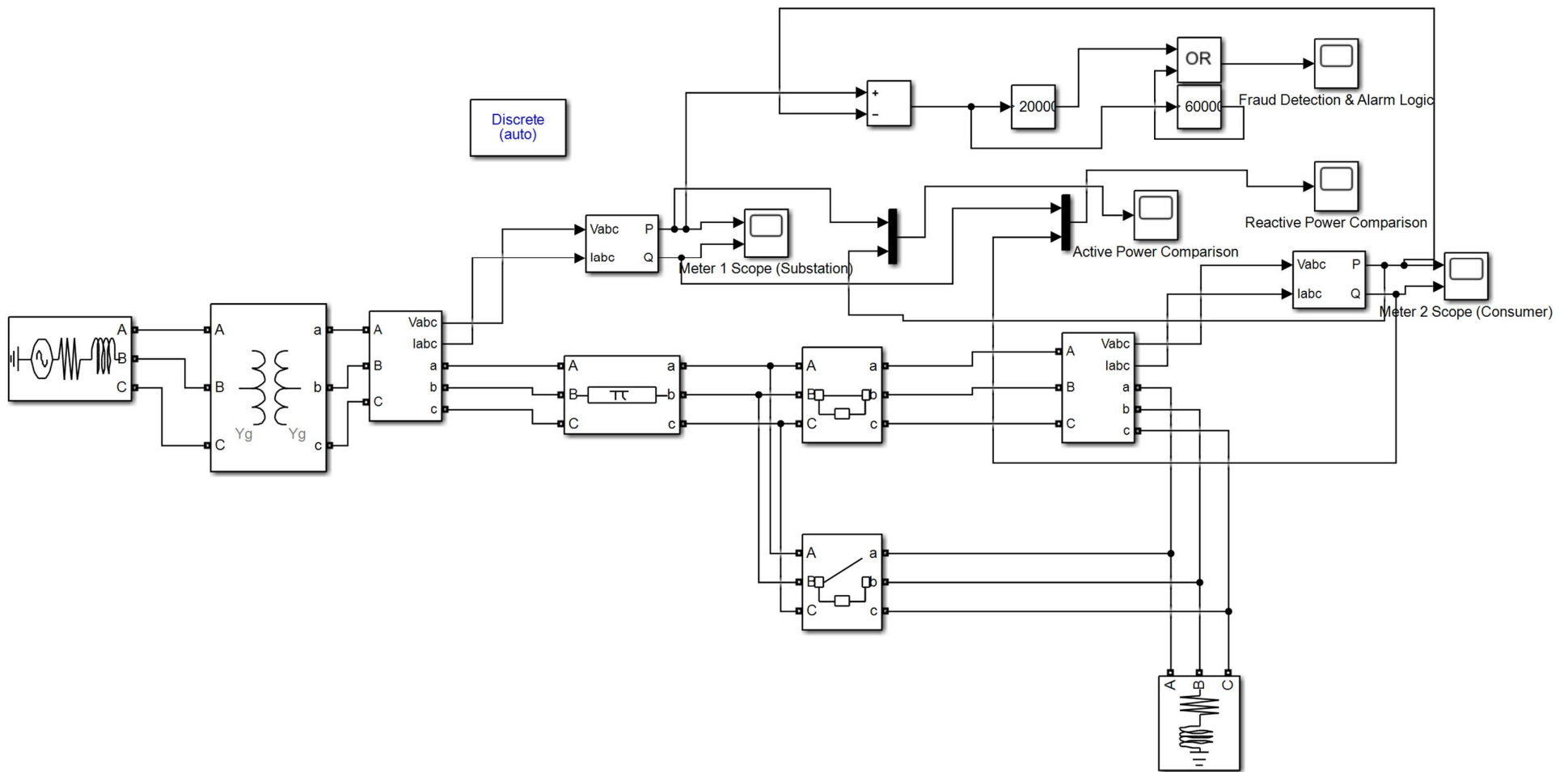


Figure 4.1: The complete MATLAB/Simulink model of the network and the smart detection logic

4.3 Results and Discussion

The simulation results provide a clear physical validation of both the fraud event and the success of the proposed smart detection logic.

4.3.1 Analysis of the Fraud Event (Active and Reactive Power)

As shown in the power response graphs (Figure 4.2 and Figure 4.3), the system operates within normal parameters until 0.5 seconds. During this initial phase, the energy balance is strictly maintained. Meter 1 injects approximately 415 kW of active power, and Meter 2 correctly records the 400 kW industrial load, with the 15 kW difference attributed to normal technical losses in the distribution lines. However, at exactly 0.5 seconds, the bypass breaker activates. Both the active power (Figure 4.2) and the reactive power (Figure 4.3) registered by the client's billing meter (Meter 2) drop abruptly to 0. Meanwhile, the main supply (Meter 1) continues to feed the heavy industrial load. The simultaneous drop in both active and reactive measurements confirms a complete meter bypass (all phases diverted). This massive discrepancy highlights a severe case of Non-Technical Loss (NTL), causing complete commercial blindness for the utility company. From an electrotechnical perspective, this unrecorded energy extraction is not merely an administrative issue, but a severe physical threat to the grid's stability. Even though the client's meter registers zero, the physical load continues to draw massive currents through the network. This invisible consumption artificially exacerbates Joule heating (I^2R) along the distribution feeders and places severe, uncoordinated thermal stress on the local transformer core, which ultimately degrades the network's voltage profile. These physical manifestations align closely with the findings of Depuru et al. [4], who established that unauthorized industrial loads significantly accelerate equipment degradation and cause localized power quality issues. Furthermore, as highlighted by Smith [5] in comparative NTL analyses, such massive discrepancies physically validate that traditional monthly billing cycles are fundamentally insufficient for detecting high-stakes industrial fraud, necessitating the shift towards real-time physical monitoring

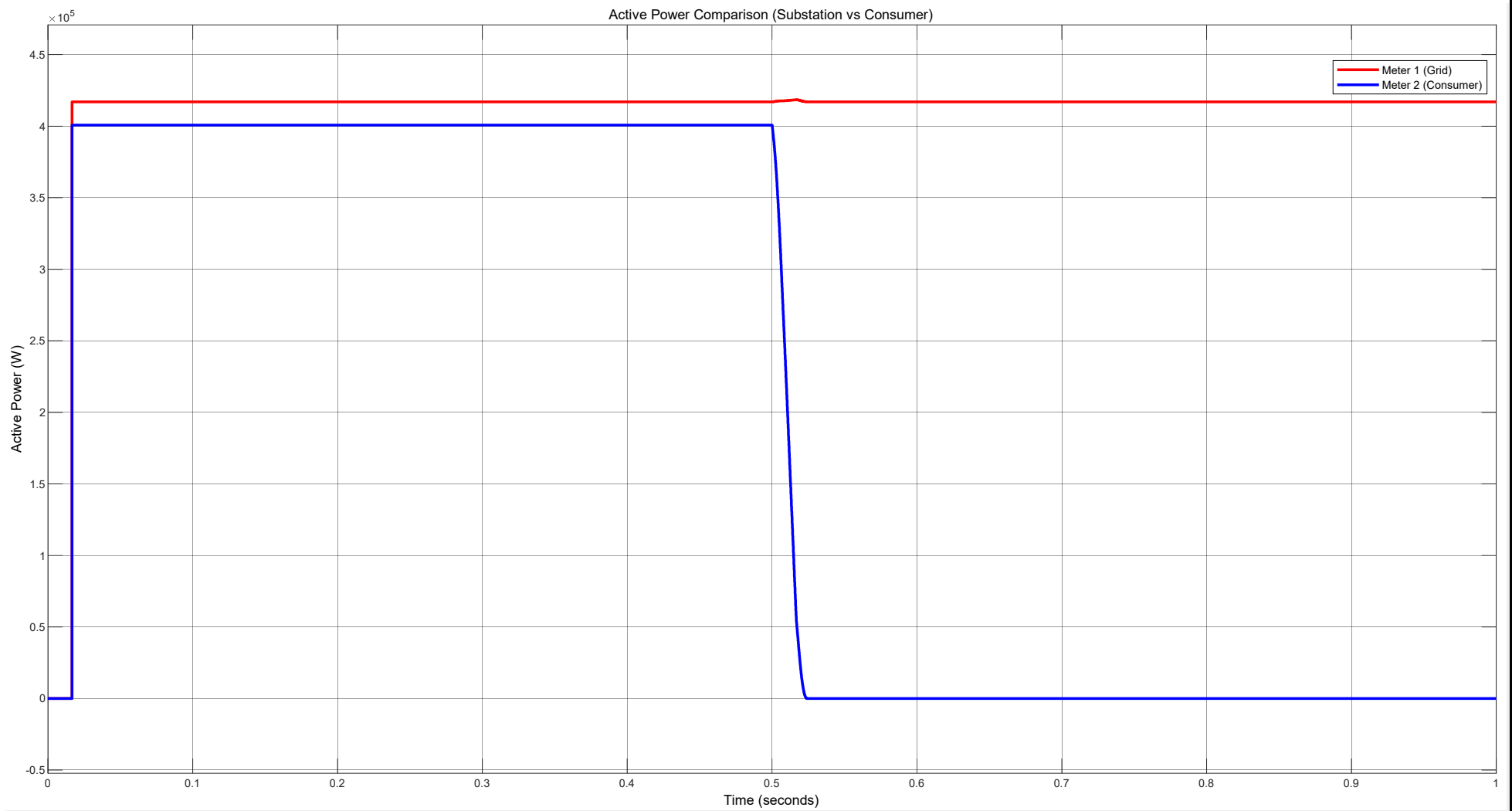


Figure 4.2: Active Power recorded by the Main Node and the Client Node showing the bypass event.

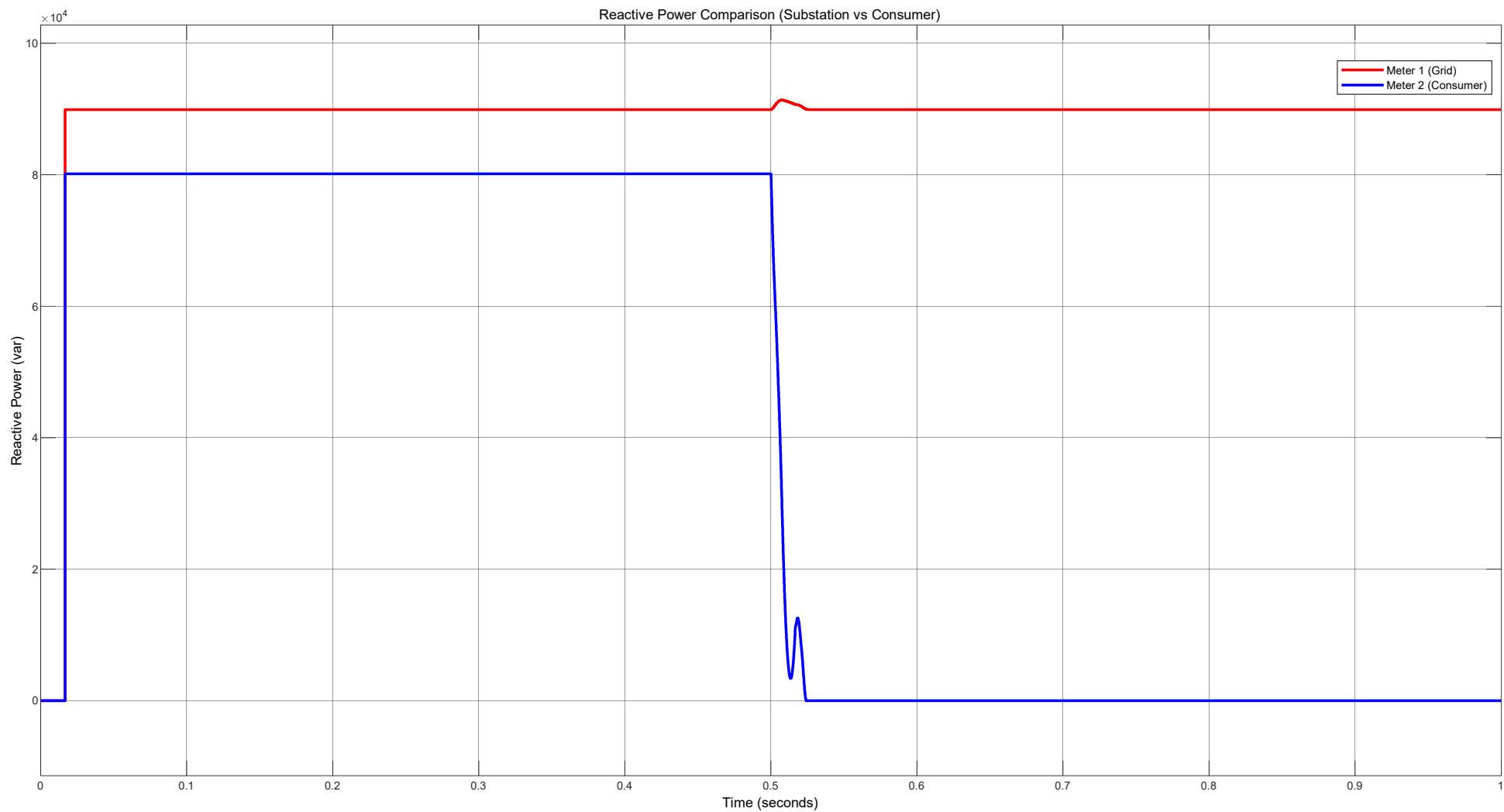


Figure 4.3: Reactive Power recorded by the Main Node and the Client Node.

4.3.2 Validation of the Smart Detection Logic

The effectiveness of the proposed smart metering solution is demonstrated by the alarm signal in Figure 4.4. By implementing a real-time energy balance algorithm, the system does not wait for a monthly billing cycle to identify the theft. The logic circuit successfully detects the massive power discrepancy (415 kW missing, which is greater than the 20-kW threshold) at the exact millisecond the fraud occurs (0.5 seconds). The alarm signal spikes immediately from 0 to 1, triggering an instant digital notification. This confirms that integrating automated smart infrastructures allows Sonelgaz to shift from a slow, reactive billing-audit process to a proactive, real-time security mechanism. As noted by McLaughlin *et al.* [17], Advanced Metering Infrastructures (AMI) equipped with multi-sensor data fusion are critical for immediately isolating anomalies that traditional visual inspections miss. Furthermore, this continuous real-time data streaming creates a solid foundation for deploying future Artificial Intelligence (AI) algorithms to predict complex tampering patterns, ensuring a robust and dynamic defense against evolving physical fraud techniques.

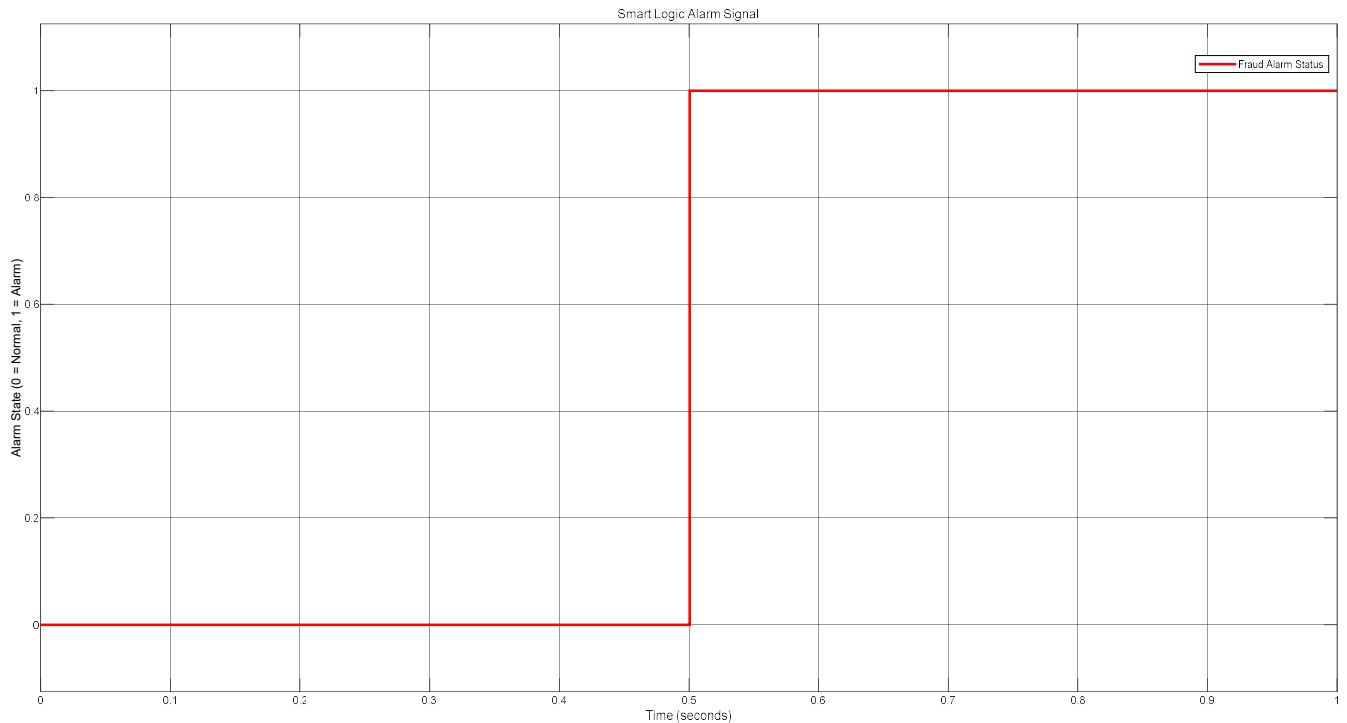


Figure 4.4: Automated Smart Meter Alarm triggering instantaneously at the exact moment of fraud.

4.4 Advanced Scenario: Asymmetric Phase Bypassing and Physical Deterrence Strategy

In real-world scenarios within the Mostaganem network, industrial clients often avoid bypassing all three phases simultaneously, as it requires complex tampering and is easily spotted during routine checks. Instead, they perform an "Asymmetric Bypass" by tampering with only a single phase (e.g., Phase A), effectively reducing their billed consumption by a third while keeping the factory fully operational.

To demonstrate the robust capabilities of the proposed Smart Grid architecture, the simulation was upgraded to include an automated Physical Deterrence Mechanism.

4.4.1 Upgraded Simulation Parameters

The bypass breaker was reconfigured to act only on Phase A. Consequently, the stolen active power is roughly 133.3 kW (one-third of the total load). To accommodate this asymmetric theft, the Smart Logic threshold was adjusted to 60 kW.

Furthermore, a Main Three-Phase Breaker was installed upstream of the client's facility. This breaker is remotely controlled by the Smart Alarm logic through a logical NOT gate. Under normal conditions (Alarm = 0), the NOT gate outputs a 1, keeping the main breaker closed and allowing power to flow.

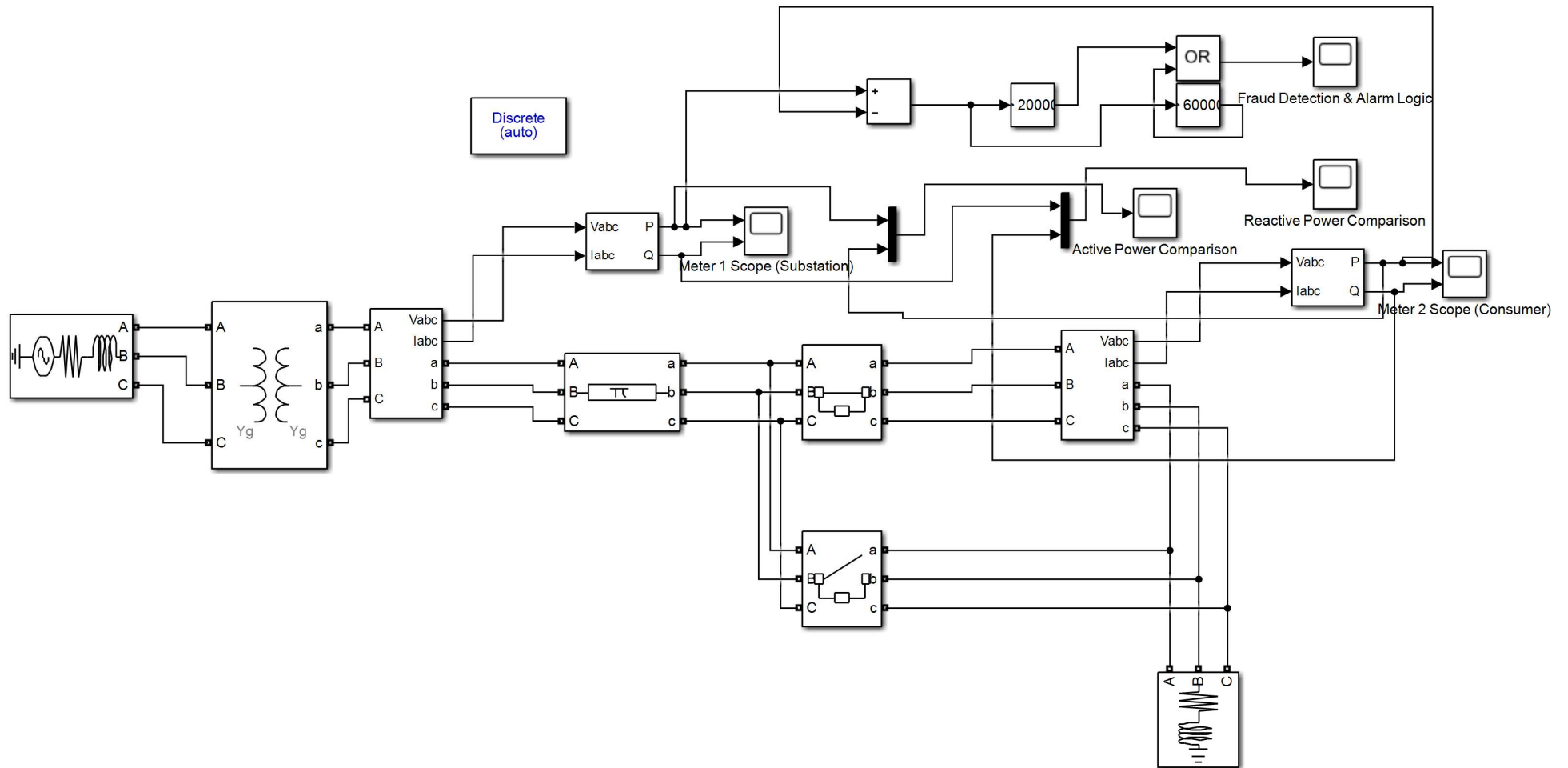


Figure 4.5: Upgraded Simulink model featuring Asymmetric Bypass and the Automated Physical Deterrent Breaker.

4.4.2 Results of the Deterrence Strategy:

When the simulation is executed, the asymmetric bypass occurs at $t = 0.5$ seconds. The results across all measured parameters strongly validate the effectiveness of the deterrence system.

1. Smart Logic Alarm Response:

The Smart Logic instantly detects the network unbalance and the missing 133.3 kW. Because the missing power exceeds the 60 kW threshold, the logic alarm instantaneously spikes from 0 to 1 at exactly $t = 0.5$ seconds. This digital signal is sent to the NOT gate, which flips the control signal to 0, forcefully opening the Main Breaker.

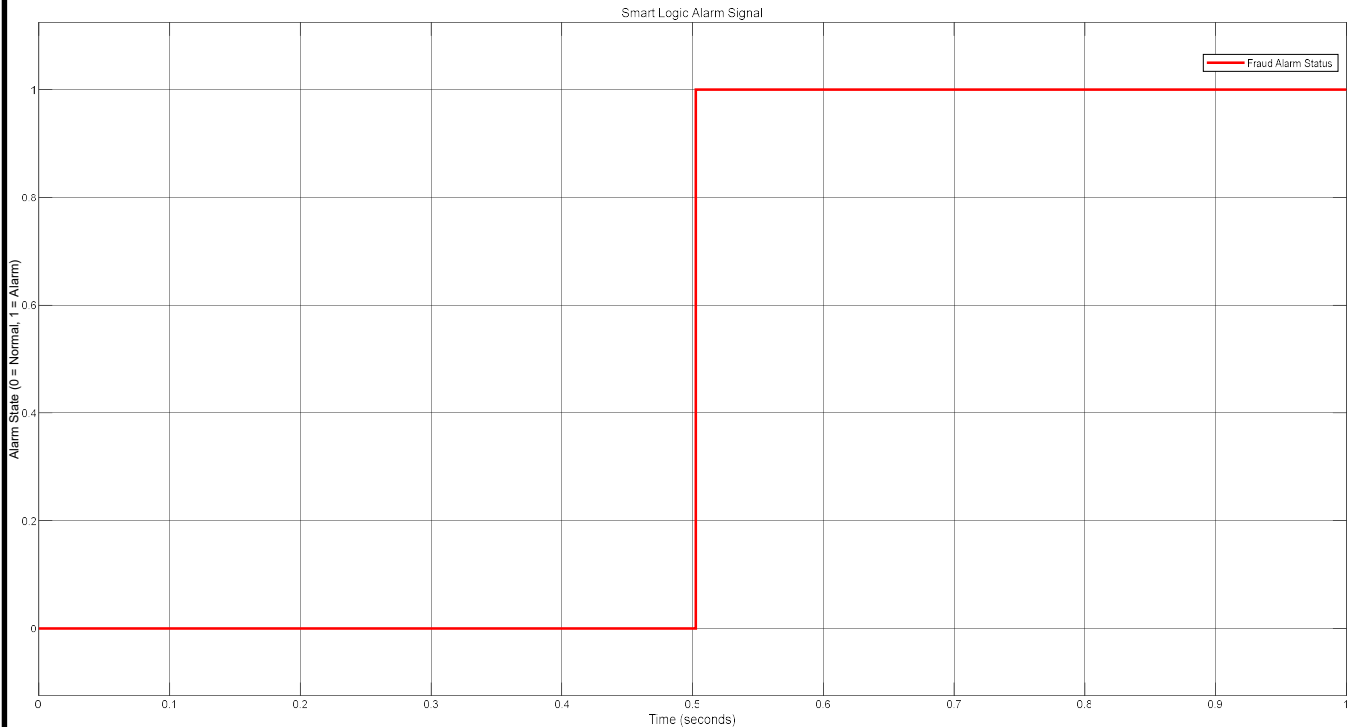


Figure 4.6: Smart Logic Alarm instantly detecting the asymmetric bypass and triggering the deterrence mechanism.

2. Active and Reactive Power Response (Total Blackout): As a direct result of the Main Breaker tripping, both the Active Power and Reactive Power curves undergo a drastic change. Instead of successfully stealing partial power, the active power drawn from the grid (Meter 1) and the power received by the client (Meter 2) both plummet to absolute zero. Similarly, the reactive power drops to zero, confirming the total shutdown of the industrial facility's motors. The client attempting to steal 33% of the power is penalized with a 100% power outage.

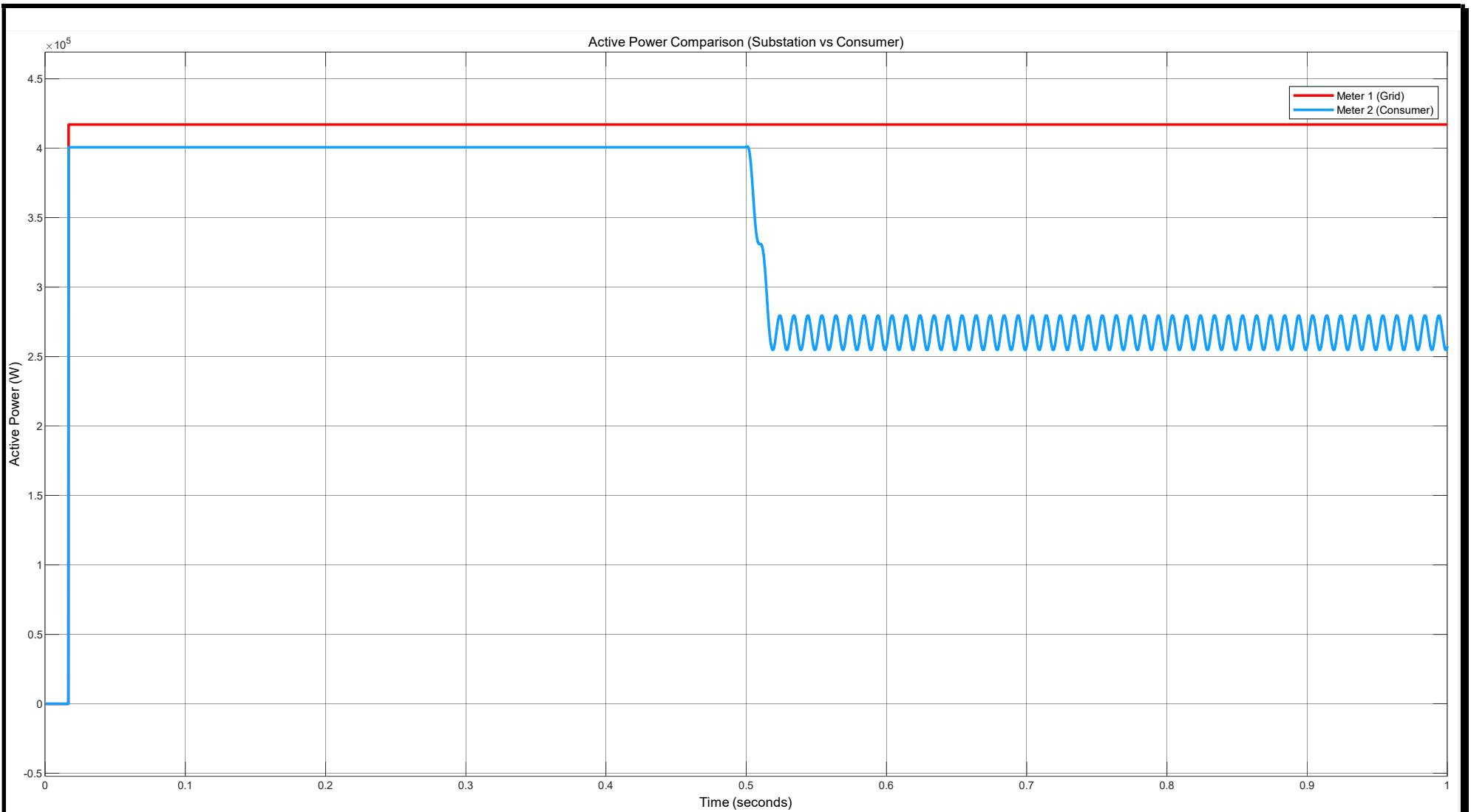


Figure 4.7: Active Power dropping to absolute zero due to the automated main breaker tripping.

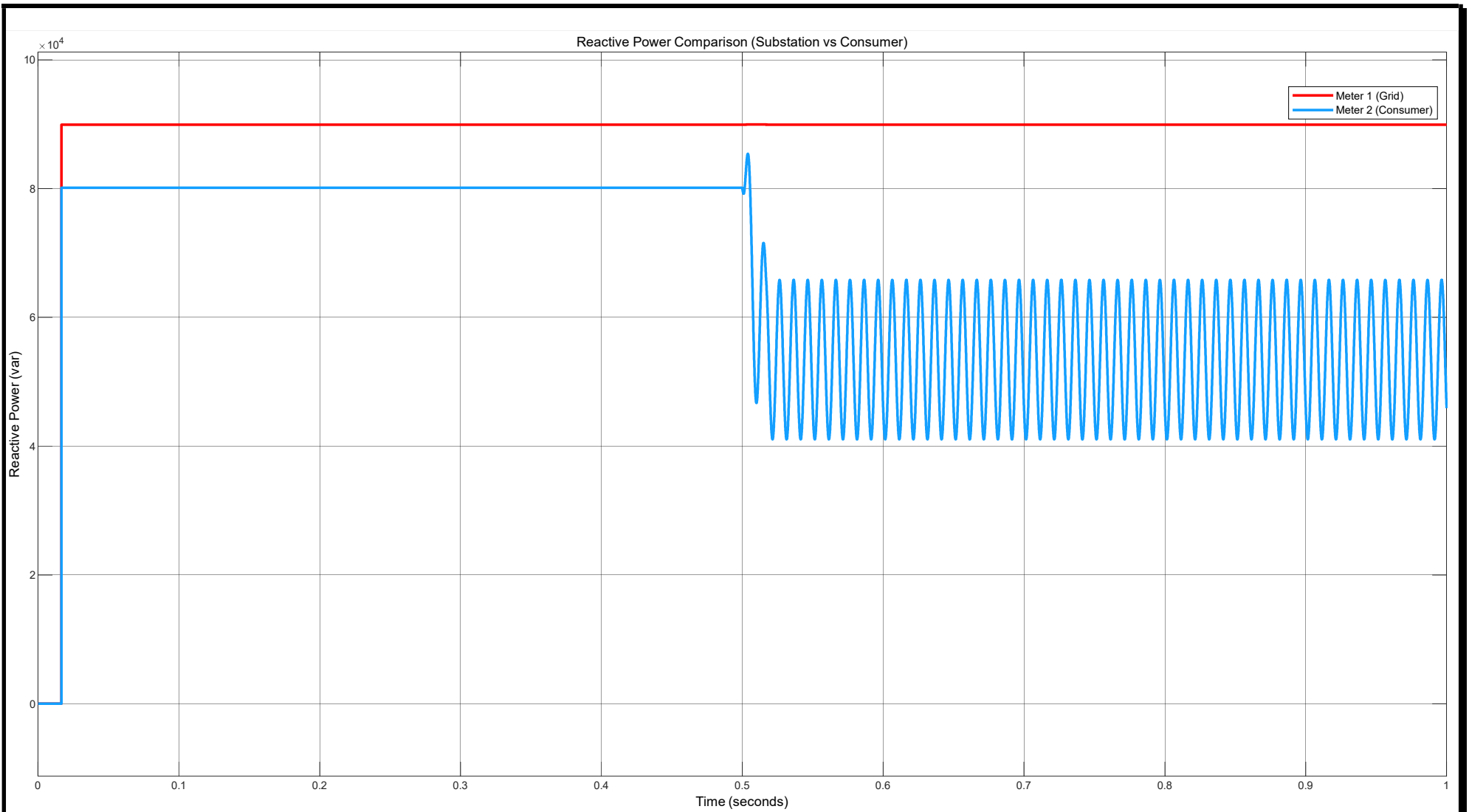


Figure 4.8: Reactive Power dropping to zero, confirming the total shutdown of the industrial facility.

4.5 Comprehensive Synthesis of Simulation Outcomes and Strategic Recommendations

4.5.1 Recap of the Simulation Paradigm

In this chapter, a highly dynamic electrotechnical simulation of the Mostaganem Medium Voltage (HTA) network was constructed using the MATLAB/Simulink environment. The primary objective was to transition the theoretical problem of Non-Technical Losses (NTL) into a measurable, physical model. By simulating a 400-kW heavy industrial load—representative of the prominent cold storage facilities in the region—the study successfully mapped the operational behavior of the grid during standard operations, complete meter bypassing, and asymmetric phase fraud. The integration of a digital Smart Detection Logic, paired with an automated physical deterrence mechanism, provided a comprehensive framework for testing advanced anti-theft solutions.

4.5.2 Cross-Analysis of the Power Curves and Alarm Responses

A holistic review of the graphical data generated reveals the stark vulnerability of traditional metering architectures. In the initial fraud scenario, the active and reactive power curves (Figures 4.2 and 4.3) demonstrated an instant drop to zero at the client's billing node, while the main grid continued to inject 415 kW to sustain the industrial motors. This visualizes the precise moment the utility enters a state of complete commercial blindness.

However, the introduction of the Smart Logic Alarm fundamentally altered this dynamic. The instantaneous digital spike from 0 to 1 (Figure 4.4) proved that differential energy balancing—calculating the variance between the injected transformer power and the billed client power—can detect massive anomalies in milliseconds.

The most critical results were derived from the advanced asymmetric bypass simulation. Recognizing that sophisticated fraudsters often manipulate only a single phase to avoid suspicion, the simulation targeted a 133.3 kW theft on Phase A. The logic successfully isolated this specific theft (Figure 4.6) and immediately commanded the upstream Main Breaker to trip. The subsequent active and reactive power curves (Figures 4.7 and 4.8) plummeting to absolute zero represent the ultimate physical validation of this thesis: penalizing a partial theft with a 100% automated power blackout.

4.5.3 Scientific Interpretation of the Physical Grid Impact

Extrapolating from these curves, the results dictate that NTL is not solely a financial crisis, but a severe electrotechnical hazard. The unrecorded power extraction captured in the simulation forces the distribution infrastructure into a highly dangerous operational state. Because the stolen energy is unmetered, the local 1 MVA transformer is continuously subjected to uncoordinated thermal stress, pushing it toward its absolute thermal limits.

Furthermore, the simultaneous manipulation of reactive power—which is critical for magnetizing industrial induction motors—is particularly destructive. When heavy inductive loads are bypassed, the grid is forced to supply massive magnetizing currents without any commercial visibility. This uncompensated reactive flow severely degrades the localized

voltage profile, dramatically increasing Joule heating in the distribution cables and negatively impacting the power quality for all legally connected consumers on that specific Mostaganem feeder.

4.5.4 Comparative Literature Analysis:

These physical and logical outcomes strongly corroborate the established theoretical frameworks within the scientific literature. The observed degradation in network stability seamlessly aligns with the findings of Depuru *et al.* [4], who argued that unregulated industrial electricity theft is a primary catalyst for accelerated equipment aging and premature transformer failures.

Moreover, while traditional comparative analyses by Smith [5] highlighted the inefficiency of standard billing cycles in curbing high-stakes fraud, our simulation results push the boundary further. Many contemporary smart grid models, such as those proposed by McLaughlin *et al.* [17], rely heavily on software-level data mining and post-event audits. In contrast, the implementation of the automated physical deterrence strategy (the NOT-gate triggered Main Breaker) in our simulation demonstrates that software detection is vastly more effective when directly coupled with hardware-level intervention. This hybrid approach validates the necessity for real-world, aggressive deterrence solutions, bridging the gap between digital detection and physical grid protection.

4.5.5 Final Conclusions and Takeaways for the Utility

The synthesis of these simulation results yields several definitive conclusions for the Sonelgaz Distribution Directorate of Mostaganem:

1. **Passive Auditing is Obsolete:** Traditional, monthly visual inspections are mathematically and operationally insufficient for identifying dynamic, high-capacity industrial fraud. The financial prejudice accumulates too rapidly before any human intervention can occur.
2. **Real-Time Differential Balancing is Mandatory:** The Smart Metering logic proved that calculating energy gaps at the micro-level (transformer vs. load) provides a flawless, immediate detection mechanism that cannot be fooled by downstream phase manipulation.
3. **Automated Deterrence is the Ultimate Solution:** Shifting from a reactive posture (issuing massive adjustment bills after the fact) to a proactive deterrence posture (automated circuit tripping) completely eliminates the financial loss at the exact moment the theft is initiated.

Ultimately, integrating Advanced Metering Infrastructure (AMI) with physical tripping mechanisms does not merely record theft; it makes the act of stealing electrotechnically impossible to sustain, ensuring the absolute preservation of both grid stability and utility revenues.

4.6 Conclusion:

This chapter successfully simulated severe Non-Technical Loss scenarios within the Mostaganem electrical network. The physical models proved how vulnerable traditional metering systems are to both complete and asymmetric bypass fraud. Furthermore, the integration of smart detection logic and physical deterrence mechanisms validated the core hypothesis of this thesis: upgrading to Advanced Metering Infrastructure (AMI) with real-time data analytics not only detects theft instantaneously but can also actively penalize fraudulent behavior. This technological shift is essential to secure the utility's financial revenues and maintain grid stability.

General Conclusion

At its core, the primary mission of any electrical distribution network is to deliver power safely, reliably, and efficiently to the end consumer. However, as this research has extensively demonstrated, the reality of managing such a vast infrastructure is far more complex. Non-technical losses represent much more than a simple administrative discrepancy or a minor margin of stolen electricity. They constitute a severe, systemic threat that compromises both the financial viability of utility companies and the fundamental physical stability of the distribution grid itself. Throughout this thesis, we have established a clear distinction between the unavoidable laws of physics that govern technical losses and the deeply human, socio-economic, and systemic drivers that fuel commercial losses.

By grounding our research in the specific operational realities of the Mostaganem electrical network, we were able to map out how this multidimensional crisis adapts to its environment. The Wilaya's diverse topography—ranging from rapidly expanding urban neighborhoods to isolated agricultural expanses and high-demand industrial zones—dictates the specific nature of the theft. In densely populated areas, the grid suffers from a high volume of clandestine hookups and residential meter tampering, creating a localized phenomenon of "death by a thousand cuts." Conversely, in the rural and industrial sectors, the utility faces highly destructive cable sabotage and sophisticated, high-capacity meter bypassing. These high-stakes industrial frauds, particularly in facilities like heavy cold storage units, drain massive amounts of active and reactive power, completely distorting the local energy balance.

A critical takeaway from our analysis is that traditional, reactive management strategies are fundamentally ill-equipped to handle modern electrical fraud. Relying on monthly visual inspections and standard billing cycles leaves the utility company commercially blind for weeks at a time. During these blind periods, the unmetered extraction of power forces distribution transformers to operate dangerously beyond their designed thermal limits. The hidden inductive draw from bypassed industrial motors severely degrades the localized voltage profile, dramatically increases Joule heating in the distribution cables, and accelerates the aging of expensive grid infrastructure. By the time a billing anomaly is discovered on paper, the physical and financial damage has already been done.

This inherent vulnerability was rigorously tested and validated through our MATLAB/Simulink case study. By constructing a dynamic electrotechnical model of a

Medium Voltage industrial bypass event, we transitioned the problem from a theoretical billing issue to a measurable physical hazard. More importantly, the simulation successfully proved that the solution lies in transitioning from passive observation to active, automated intervention. By integrating Advanced Metering Infrastructure with real-time differential logic, our model did not simply flag a discrepancy; it detected the exact millisecond the power went missing.

Going a step further, the implementation of the asymmetric phase distribution strategy alongside automated tripping mechanisms proved that a utility can actively defend itself. We demonstrated that by coupling smart digital detection with immediate hardware-level intervention—such as triggering a main breaker to enforce a total blackout on a cheating facility—the act of stealing power can be rendered electrotechnically impossible to sustain. This approach shifts the paradigm from trying to recover lost funds through adjustment bills to physically preventing the loss the moment it is initiated.

Ultimately, this thesis concludes that combating non-technical losses requires a profound operational transformation. Utility companies like Sonelgaz must evolve beyond the traditional "audit and bill" philosophy. To secure the long-term stability of the grid and protect vital revenue streams, the distribution network must become an intelligent, self-monitoring ecosystem capable of real-time detection and aggressive physical deterrence. Embracing this smart, hybrid approach is no longer just an innovative concept for the future; it is an absolute engineering and economic necessity to guarantee a resilient and sustainable energy sector.

References:

- [1] J. D. Glover, M. S. Sarma, and T. J. Overbye, *Power System Analysis and Design*, 5th ed. Stamford, CT: Cengage Learning, 2011.
- [2] T. Gönen, *Electric Power Distribution System Engineering*, 3rd ed. Boca Raton, FL: CRC Press, 2014.
- [3] P. Antmann, "Reducing Technical and Non-Technical Losses in the Power Sector," World Bank Group, Washington, DC, Background Paper, 2009.
- [4] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft," *Energy Policy*, vol. 39, no. 2, pp. 1007–1015, 2011.
- [5] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, vol. 32, no. 18, pp. 2067–2076, 2004.
- [6] Office National des Statistiques (ONS). (2008). *Recensement Général de la Population et de l'Habitat (RGPH) 2008 - Wilaya de Mostaganem*. Alger: ONS.
- [7] Sonelgaz-Distribution. (2023). *Document n°07 - 2023: Organisation et structures des Directions de Distribution*. Alger: Groupe Sonelgaz.
- [8] Direction de Distribution de Mostaganem (DTE). (2022). *Rapport Annuel d'Activité 2021: Bilan technique et investissements*. Mostaganem: Sonelgaz.
- [9] Direction de Distribution de Mostaganem (Division Commerciale). (2026). *Bilan de la clientèle, évolution du portefeuille (2025-2026) et Base de Données HTA*. Mostaganem: Sonelgaz.
- [10] Itron S.A.S. (2012). *ACE6000 Guide d'utilisation et Guide d'utilisation ACE Pilote: Mise en œuvre et validation des installations de comptage*. France: Itron
- [11] Groupe Sonelgaz. (2025). *Bilan Énergétique et Financier National 2024: Évaluation des pertes, créances et actes de malveillance*. Alger: Sonelgaz.
- [12] Direction de Distribution de Mostaganem (Division Commerciale). (2026). *Bilan des Créances et Statistiques Clientèle: Cartographie des pertes non-techniques et recouvrement*. Mostaganem: Sonelgaz.
- [13] Direction de Distribution de Mostaganem (Division Technique). (2025). *Rapport Opérationnel et Bilan des Incidents: Actes de vandalisme et vols de câbles (Mois de Novembre)*. Mostaganem: Sonelgaz.
- [14] Direction de Distribution de Mostaganem (DTE). (2025). *Rapport d'Investissement: Programme d'électrification rurale et mise à niveau du réseau HTA/BTA*. Mostaganem: Sonelgaz.

- [15] Direction de Distribution de Mostaganem (Inspection Commerciale). (2025). Rapport d'Audit Énergétique: Détection des fraudes industrielles et anomalies de comptage (Secteur des chambres froides). Mostaganem: Sonelgaz.
- [16] M. Yigit, V. C. Gungor, and S. Baktir, "A transition to the smart grid: State of the art, open research issues, and future directions," *Computer Networks*, vol. 67, pp. 1-14, 2014.
- [17] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319-1330, 2013.
- [18] A. S. Pabla, *Electric Power Distribution*, 6th ed. New York: McGraw-Hill Education, 2014.
- [19] M. Jamil and A. S. Anees, "Real world solutions to electricity theft," in *Power Quality and Distribution Utility Network Proceedings*, 2015.
- [20] Société Algérienne de Distribution de l'Electricité et du Gaz (Sonelgaz), "Rapport annuel sur les pertes réseaux et la gestion commerciale - Direction de Distribution de Mostaganem," Document Interne, Mostaganem, Algérie, 2025.