Design and Implementation of Test Cases for IDIS Compliance in UMEME's OneSait Smart Metering Project

Guillermo Varas Yuste
Escuela Técnica Superior de Ingeniería (ICAI)
Madrid, Spain
201807489@alu.comillas.edu

***Abstract*—This thesis focuses on designing and implementing test cases to ensure the IDIS compliance of smart meters within UMEME's OneSait Smart Metering Project in Uganda. Through a review of DLM-S/COSEM and IDIS protocols, simulations were conducted using MATLAB to validate key functionalities like meter registration, remote tariff programming, and firmware updates. In addition to compliance, the study addresses cybersecurity risks, proposing encryption and authentication enhancements to secure UMEME's infrastructure. Results confirmed the reliability of IDIS-compliant meters while identifying areas for improvement, contributing to the modernization and security of Uganda's energy grid.**

***Index Terms*—IDIS, DLSM/COSEM, smart metering, simulation, Uganda, UMEME.**

I. Introduction

In the evolving landscape of global energy systems, smart grid technologies and smart metering solutions have become essential for improving the efficiency, reliability, and security of electricity distribution networks. Smart meters offer significant advancements over traditional systems by enabling real-time monitoring, remote data transmission, and automated control. A critical aspect of their deployment is ensuring robust communication standards, such as DLMS/COSEM and IDIS, which guarantee seamless interoperability across diverse devices and manufacturers.

This thesis addresses the importance of these standards within UMEME's OneSait Smart Metering Project in Uganda, aimed at modernizing the country's energy infrastructure. The primary objective is to design and implement test cases that validate IDIS compliance of the smart meters in UMEME's network. These tests simulate real-world scenarios—such as meter registration, tariff programming, periodic readings, and firmware updates—to ensure the meters meet international standards and perform reliably under operational conditions.

In addition to compliance, the thesis also tackles the rising cybersecurity challenges associated with interconnected smart metering systems. With an increasing vulnerability to cyberattacks, it explores encryption, authentication, and firmware management strategies to enhance the security of UMEME's infrastructure.

By conducting extensive simulations using MATLAB, the study evaluates the smart meters' performance under diverse conditions, identifying areas for improvement. This work not only validates compliance with international standards but also proposes measures to enhance the security and reliability of Uganda's smart grid, contributing to the broader goals of energy efficiency and sustainability.

a) Objectives

1) Research and Analysis of DLMS/COSEM and IDIS Standards: To thoroughly understand these protocols and ensure their effective application within UMEME's infrastructure.
2) Design and Implementation of IDIS-Compliant Test Cases: To create and simulate real-world scenarios that validate smart meters' compliance with IDIS standards.

3) Simulation of Use Cases: To evaluate smart meters' behavior in realistic conditions, identifying strengths and areas for improvement.
4) Exploring and Proposing Cybersecurity Measures: To identify vulnerabilities and recommend stronger security measures, including encryption and advanced authentication, to protect UMEME's infrastructure.

In conclusion, this thesis contributes to the successful implementation of UMEME's smart metering project by ensuring compliance with IDIS standards and addressing critical cybersecurity concerns. These efforts will enhance the reliability, efficiency, and security of Uganda's energy infrastructure, supporting the country's transition to a sustainable energy future.

II. State of the Art

Smart grid technologies and smart metering systems are fundamental to modern energy infrastructures, requiring robust standards for interoperability, security, and efficiency. The Device Language Message Specification/Companion Specification for Energy Metering (DLMS/COSEM), supported by the Interoperable Device Interface Specifications (IDIS), forms the basis for communication and data exchange within smart grids. These protocols enable seamless interoperability across diverse devices and systems, ensuring scalability and reliability in energy management infrastructures [1].

A. DLMS/COSEM Protocol

DLMS/COSEM is a standardized protocol designed to facilitate communication and data exchange in smart metering systems. It supports various communication media, such as power line communication (PLC) and radio frequency (RF), ensuring flexibility and adaptability in different environments. Its layered architecture enhances integration and scalability, making it a cornerstone for smart metering deployments across the world [2]. This standardization promotes interoperability, allowing devices from different manufacturers to communicate seamlessly in smart grid infrastructures.

B. Security Considerations

Security is a critical concern in smart metering systems due to the sensitivity of the data involved. Wang [3] highlights cybersecurity vulnerabilities in DLMS/COSEM implementations, particularly in the High-Level Data Link Control (HDLC) layer, where buffer overflow issues could lead to denial-of-service attacks. To mitigate these risks, comprehensive security measures such as encryption and authentication are essential, ensuring that data transmission between meters and utilities is secure and reliable.

Regular security assessments, intrusion detection systems, and robust key management strategies are critical for maintaining the integrity of smart meter systems. Mohammadali [4] proposes a hierarchical key management scheme for DLMS/COSEM-based smart metering infrastructures, which enhances security by ensuring that different keys are used at various levels of communication, preventing a compromise at one level from affecting the entire system.

C. Validation and Compliance Testing

Validation and compliance testing are essential for ensuring that smart meters meet industry standards and function reliably. Mendes [5] presents the ValiDLMS framework, an open-source tool that combines fuzzing techniques and security analysis to validate DLMS/COSEM implementations. This framework helps detect security vulnerabilities and non-conformance issues, allowing developers to address them early in the deployment process.

By leveraging tools like ValiDLMS and passing rigorous compliance tests such as the OIML R46 standard [6], utilities can ensure that their smart meters operate securely and meet international performance standards. These tests are critical for building trust with consumers and ensuring the reliability of smart grid deployments.

D. IDIS Protocol and Standards

The IDIS protocol enhances DLMS/COSEM by providing specific use cases that ensure interoperability among smart meters from different manufacturers. The latest IDIS Package 3 introduces advancements in meter reading, power quality monitoring, and security features [7]. These enhancements are vital for the evolving smart grid landscape, ensuring that smart meters meet the demands of modern infrastructure. The rigorous IDIS certification process verifies that devices comply with international standards for performance, security, and interoperability, fostering reliable communication across the smart grid.

III. UMEME's Project Paradigm

UMEME, Uganda's largest electricity distribution company, plays a critical role in managing electricity distribution to millions of Ugandans. The OneSite smart metering project is a key initiative aimed at modernizing UMEME's network through advanced smart meters, enhancing billing accuracy, reducing losses, and improving operational efficiency.

A. Uganda's Electricity Market

Uganda's electricity sector has seen significant growth, with generating capacity increasing from 320 MW in 2002 to over 1,346 MW in 2023, driven by large hydroelectric projects such as Karuma and Isimba [8]. Renewable energy sources dominate the market, with hydro contributing about 80% of the total capacity [8]. Despite growth, challenges like low rural electrification rates and underutilized generation capacity due to limited transmission investments persist [8].

B. Regulatory Environment

The Electricity Regulatory Authority (ERA) regulates Uganda's electricity market by setting tariffs, ensuring compliance, and fostering investment. ERA's tariff setting process balances cost recovery with affordability through the Quarterly Tariff Adjustment Methodology (QTAM), which adjusts tariffs based on fuel prices, exchange rates, and inflation [9]. ERA also ensures compliance with safety and operational standards through audits and inspections [10].

C. UMEME's Overview and Responsibilities

UMEME operates Uganda's electricity distribution network, distributing 97% of the country's electricity. It has reduced technical losses from 38% in 2005 to about 18% by 2022 and expanded its customer base to over 1.6 million connections. UMEME has implemented prepayment metering systems and advanced technologies to enhance billing accuracy and reduce losses [11].

D. Challenges Faced by UMEME

UMEME faces numerous challenges, including outdated infrastructure leading to power losses of up to 20%, limited rural electrification, and financial constraints affecting infrastructure upgrades. High tariffs have also sparked dissatisfaction among consumers, while vandalism and electricity theft further diminish financial resources [12] [13]. The OneSite solution aims to address these issues by improving UMEME's control over meters and customer interactions through enhanced monitoring and data analytics.

E. OneSite Smart Metering Project

The OneSite Smart Metering project, led by Minsait, aims to modernize UMEME's electricity distribution systems. This project integrates smart metering with advanced data management to reduce losses, improve billing accuracy, and enhance customer engagement [14]. The system supports multiple communication protocols, including DLMS/COSEM and IDIS, ensuring flexibility and scalability [14]. Real-time monitoring and analytics help UMEME detect electricity theft and optimize operations [14]. Prepayment and post-payment models further cater to diverse customer needs, improving financial stability and revenue collection [14].

In addition to operational improvements, the project aligns with UMEME's sustainability goals by tracking energy usage patterns and implementing measures to reduce waste. This smart metering system positions UMEME as a leader in energy efficiency and supports the country's broader electrification goals [14].

IV. Prepayment Systems

Prepayment systems allow consumers to pay for electricity in advance, offering flexibility and improved cash flow for utilities. These systems help address challenges such as electricity theft and non-payment, providing real-time data on usage and reducing administrative burdens. Prepayment systems improve revenue collection, lower operational costs, and empower consumers to manage their energy consumption effectively.

In Uganda, UMEME's Yaka prepayment meters have been widely adopted. Customers purchase electricity tokens in advance, which they input into their meters. This system provides convenience through various purchasing channels, including mobile money, and helps consumers monitor usage. However, the reliance on manual input and outdated technology exposes the system to inefficiencies and fraud [15]. To address these issues, UMEME is upgrading Yaka meters to comply with the Standard Transfer Specification (STS)2 standards, ensuring enhanced security and better interoperability [16].

A. Advanced Prepayment Solutions

Advanced prepayment systems automate transactions, eliminating manual input and enabling digital payments via mobile platforms. These systems, such as Itron's Smart Pay [17], offer real-time billing and remote disconnection features, improving efficiency and reducing the risk of errors. Minsait's Onesait Utilities platform [18] integrates advanced metering infrastructure with mobile solutions, enhancing customer engagement and providing utilities with real-time data for better decision-making. These systems improve service reliability, reduce operational costs, and strengthen fraud prevention.

B. Role of DLMS/COSEM in Prepayment

DLMS/COSEM standards are essential for modernizing prepayment systems, ensuring interoperability, security, and scalability. These standards enable seamless communication between meters and utility systems, supporting secure data exchange and preventing fraud through robust encryption and authentication mechanisms. By standardizing communication protocols, DLMS/COSEM facilitates the integration of advanced prepayment solutions with existing infrastructures [7].

C. IDIS in Enhancing Prepayment Systems

IDIS certification ensures interoperability, reliability, and security across devices in prepayment systems. Built on IEC 62056 DLMS/COSEM standards, IDIS-certified devices support various communication protocols, enabling integration with diverse network infrastructures. These solutions enhance prepayment systems by providing real-time data, remote management, and strong security features that protect against fraud and unauthorized access [7].

V. IDIS Use Cases Tests

This chapter focuses on simulating various IDIS use cases to evaluate smart meters' adherence to the IDIS Package 3 standards [19]. Each use case tests specific meter functionalities within the Advanced Metering Infrastructure (AMI). The goal is to assess the meters' ability to integrate into a smart grid, ensuring accurate and reliable operation.

The simulations replicate real-world scenarios to test meter performance. The details provided allow us to focus on the test results and their implications for meter functionality in this chapter.

A. UC 1: Meter Registration

Meter registration is crucial for ensuring the integration of new meters into the AMI network. During the test, the meter transmits its identification data (e.g., device ID, IP address) to the Head-End System (HES), which verifies and confirms successful registration. The expected outcome is the correct registration of the meter within the network, ensuring that it is prepared for subsequent operations.

B. UC 2: Remote Tariff Programming

This use case evaluates the meter's ability to receive and implement new tariff structures remotely. The HES sends updated tariffs, and the meter applies them, ensuring that consumer billing reflects current rates. Success is marked by the accurate application of the new tariff without any manual intervention, ensuring flexible and dynamic billing.

C. UC 3: On-Demand Reading

On-Demand Reading allows the HES to request real-time data from the meter, including energy consumption details. The simulation tests whether the meter can provide accurate and timely readings when requested by the HES. Any delays or incorrect data indicate a failure in this essential function, which could affect billing accuracy and energy management.

D. UC 4: Periodic Reading

Periodic readings are automatically sent by the meter at regular intervals, providing consistent updates to the HES for billing and monitoring purposes. The test assesses the meter's ability to transmit data at set intervals without errors or missed transmissions, ensuring that the system remains accurate and reliable.

E. UC 5: Connection and Disconnection

This use case tests the meter's remote connection and disconnection capabilities, essential for managing power delivery in scenarios such as nonpayment. The meter responds to HES commands, either connecting or disconnecting power as needed. The test also includes an automatic disconnection feature when current levels exceed predefined thresholds.

F. UC 6: Clock Synchronization

Clock synchronization ensures the meter's internal clock matches the HES's, which is vital for time-sensitive processes like billing. The meter adjusts its time based on synchronization commands from the HES, and the test verifies that this synchronization occurs without delay.

G. UC 7: Quality of Supply Reporting

This test assesses the meter's ability to track and report voltage levels, current, and power disturbances. The meter logs events like voltage sags or swells, providing crucial data for maintaining electricity supply reliability.

H. UC 8: Load Management by Relay

Load Management by Relay allows the HES to control the meter's relay, connecting or disconnecting loads based on demand. The test evaluates whether the meter responds accurately to load control commands, managing electricity flow based on the grid's current needs.

I. UC 9: Firmware Update

This use case tests the meter's ability to receive and install firmware updates remotely. The simulation checks if the meter successfully installs new firmware while minimizing downtime, ensuring continued operation with enhanced features and security.

J. UC 10: Meter Supervision

Meter Supervision involves monitoring conditions like tampering, power outages, and error codes. The test evaluates the meter's ability to detect and report these issues to the HES, ensuring the integrity of the system.

K. UC 11: Consumer Information

This use case tests the meter's capacity to store and retrieve consumer data, such as account numbers and billing details. The simulation checks for accuracy in data storage and transmission, which is critical for effective customer service and billing.

L. UC 12: Communication Supervision

Communication Supervision monitors the quality and reliability of the connection between the meter and the HES. The test ensures that the meter accurately tracks connection status, reports issues, and maintains stable communication.

M. UC 13: Outage Supervision

Outage Supervision checks the meter's ability to detect and report power outages. The test ensures that the meter logs outages accurately and notifies the HES promptly, enabling quick responses to disruptions.

N. UC 14: Remote Parameter Configuration

This use case allows remote adjustments to meter settings, such as display modes and alarms. The simulation verifies that the meter correctly applies these remote configurations as instructed by the HES.

O. UC 15: Warning Message Management

Warning Message Management evaluates the meter's ability to generate alerts when specific thresholds, such as load limits, are exceeded. The meter must send accurate and timely warnings to the HES or consumer to prevent potential issues.

VI. Test Results and Analysis

The IDIS use case tests were simulated using MATLAB scripts, which simulate the interaction between smart meters and the HES. Each meter underwent a series of tests, and the results were plotted to evaluate performance, highlighting areas for improvement or compliance with IDIS standards.

A. Meter 1 Simulation

Meter 1 failed the Remote Tariff Programming (UC2) and Connection/Disconnection (UC5) tests, indicating issues with handling tariff updates and remote connection control. However, it successfully passed other tests, demonstrating strength in areas like meter registration and firmware updates.

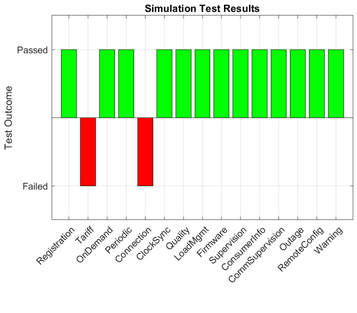

Figure 1: Meter 1 - Tests Results

B. Meter 2 Simulation

Meter 2 showed deficiencies in On-Demand Reading (UC3), Consumer Information (UC11), and Communication Supervision (UC12). These failures suggest issues with real-time data provision, consumer data management, and communication stability, which are critical for accurate meter operations.

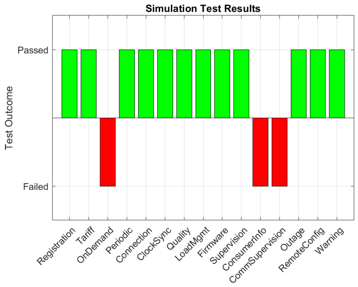

Figure 2: Meter 2 - Tests Results

C. Meter 3 Simulation

Meter 3 successfully passed all tests, demonstrating full compliance with IDIS standards. Its performance across all use cases confirms its readiness for deployment in real-world scenarios, offering reliable and efficient smart meter operation.

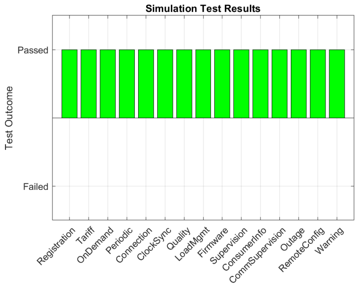

Figure 3: Meter 3 - Tests Results

This meter is ready for implementation in the UMEME network, ensuring compliance with IDIS standards for reliable operation.

VII. Cybersecurity in Smart Metering

This section examines the cybersecurity landscape in smart metering, focusing on UMEME's systems and the implications for Uganda's energy sector. The discussion identifies vulnerabilities in current infrastructures and suggests enhancements to protect against potential cyber threats.

VIII. Current State of Cybersecurity in Utility Data Transfer

UMEME's infrastructure, like many in developing regions, heavily relies on DLMS/COSEM protocols, which present several security vulnerabilities, including weak encryption and authentication measures [3]. Smart meters are often vulnerable to physical tampering, and the communication networks lack robust protection, making them susceptible to data interception and manipulation [5].

Insecure communication between smart meters and utilities poses a significant risk, with firmware vulnerabilities exposing the system to breaches and data spoofing [20]. The system is also vulnerable to Distributed Denial of Service (DDoS) attacks that could disrupt power distribution and cause outages [3]. Insufficient firmware security further heightens the risk of unauthorized modifications [21]. These issues necessitate an urgent overhaul of UMEME's cybersecurity protocols.

IX. Proposed Security Enhancements

To enhance cybersecurity, UMEME must adopt a multi-layered approach incorporating modern encryption, authentication, and continuous monitoring solutions.

A. Encryption and Authentication Upgrades

Adopting Advanced Encryption Standard (AES) with Galois/Counter Mode (GCM) ensures stronger data protection against interception [22]. Implementing High-Level Security (HLS) protocols for mutual authentication between meters and utilities reduces the risk of unauthorized access, while Public Key Infrastructure (PKI) enables secure key exchange [20].

B. Key Management

Using Elliptic Curve Diffie-Hellman (ECDH) for key exchange provides robust communication security, and regular key rotation practices mitigate risks associated with key compromise [5].

C. Secure Firmware Updates

Firmware updates should be digitally signed and verified using asymmetric cryptography to prevent unauthorized modifications, ensuring only authentic updates are applied [21].

D. Network Segmentation and Monitoring

Implementing Virtual Private Networks (VPNs), firewalls, and intrusion detection systems (IDS) will secure communication channels and protect against unauthorized access [3]. Network segmentation using VLANs can also limit the impact of breaches by isolating critical system components.

E. Tamper Detection and Access Control

Tamper detection mechanisms that trigger alerts when meters are physically tampered with can safeguard devices against unauthorized access [5]. Role-Based Access Control (RBAC) will limit access to sensitive data and system components, reducing the risk of insider threats [21].

X. Implementation Strategy

A. Step 1: Technical Assessment

A thorough assessment of UMEME's current infrastructure will identify vulnerabilities, with input from key stakeholders to ensure alignment with security best practices and standards.

B. Step 2: Encryption and Key Management Implementation

Upgrade to AES-GCM encryption, PKI, and ECDH-based key exchange methods, complemented by regular key rotation practices to enhance system security [22].

C. Step 3: Secure Firmware and Network Segmentation

Implement secure firmware management, ensuring all updates are signed and verified. Segment networks using VPNs and firewalls to protect communication channels [3].

D. Step 4: Tamper Detection and Access Controls

Deploy tamper detection mechanisms and enforce RBAC to mitigate unauthorized access and enhance physical and digital security [5].

E. Step 5: Pilot Testing and Continuous Monitoring

Pilot testing will validate security improvements before full deployment. Continuous monitoring and incident response plans will be critical to adapt to emerging threats and ensure system resilience [14].

By adopting these security measures, UMEME can strengthen its cybersecurity posture, protecting its infrastructure from evolving threats while maintaining operational reliability and customer trust [5].

XI. Conclusion

This paper represents a significant step in the research and implementation of smart metering systems within Uganda's electricity distribution network, focusing on UMEME's OneSait Smart Metering Project. Key objectives—analyzing DLMS/COSEM and IDIS standards, developing IDIS-compliant test cases, and enhancing cybersecurity measures—have been successfully addressed.

A. UMEME's Smart Metering Project

The examination of UMEME's smart metering initiative highlights the importance of ensuring device interoperability and adherence to DLMS/-COSEM and IDIS standards. These measures are essential for efficient energy distribution, remote configuration, and dynamic billing. The integration of Minsait's Onesait Prepayment Solution improves billing accuracy, reduces losses, and enhances customer satisfaction by enabling real-time prepayment data.

B. Use Case Tests for IDIS Compliance

A significant contribution of this paper is the development of IDIS-compliant use case tests. These tests simulate key functionalities like remote tariff programming, on-demand readings, and connection management. The results validate that UMEME's smart meters are ready for deployment, with proven compliance under real-world scenarios.

C. Cybersecurity in Smart Metering

Cybersecurity vulnerabilities in UMEME's metering systems were identified, including weak encryption and insufficient tamper detection. The paper recommends solutions such as AES-256 encryption, stronger authentication protocols, and improved tamper detection to strengthen the smart metering system against cyber threats, ensuring its security and reliability.

D. Final Thoughts

This work provides a robust foundation for UMEME's smart metering deployment, combining IDIS compliance with enhanced security measures. The insights offered here are relevant for both UMEME and other utilities looking to implement secure, efficient smart metering systems.

References

[1] T. J. Ngcobo and F. Ghayoor, "An overview of DLMS/COSEM and g3-plc for smart metering applications," *International Journal on Smart Sensing and Intelligent Systems*, vol. 15, 1 2022.

[2] D. U. Association, "EXCERPT FROM Companion Specification for Energy Metering DLMS/COSEM Architecture and Protocols DLMS User Association," 2020.

[3] C. L. Wang, J. A. Shih, I. E. Liao, and C. T. Chien, "An Evaluation of Cybersecurity Risks of DLMS/COSEM Smart Meter Using Fuzzing Testing." Institute of Electrical and Electronics Engineers Inc., 2022.

[4] A. Mohammadali, M. H. Tadayon, and M. Asadian, *A New Key management for AMI Systems Based on DLMS/COSEM Standard*, 2014.

[5] H. Mendes, I. Medeiros, and N. Neves, "Validating and Securing DLMS/COSEM Implementations with the ValiDLMS Framework." Institute of Electrical and Electronics Engineers Inc., 7 2018, pp. 179–184.

[6] C. T. Chien, C. L. Wang, I. E. Liao, and S. J. Wang, "Implementing OIML R46 Communication Unit for DLMS/COSEM Security Suite 1 and Passing CTT V3.1 Test." Institute of Electrical and Electronics Engineers Inc., 2023.

[7] IDIS, "Package 3 IP Profile X (extended functionality) Edition 2.0," 2023. [Online]. Available: https://www.idis-association.com/downloads

[8] International Energy Agency (IEA), "Energy Policy Review Uganda 2023," 2023. [Online]. Available: www.iea.org

[9] Electricity Regulatory Authority (ERA), "Manual for the ERA Tariff Model," 2012.

[10] ——, "The ERA Compliance and Enforcement Manual," 2019. [Online]. Available: https://www.era.go.ug/index.php/resource-centre/regulatory-instruments/guidelines-and-standards

[11] "What does UMEME exit mean for electricity consumers in Uganda?". EPRC. (accessed 2024-07-12). [Online]. Available: https://eprcug.org/eprc-highlights/what-does-umeme-exit-mean-for-electricity-consumers-in-uganda/

[12] "Power Struggles: Uganda's Uneven Electricity Distribution". NilePost. (accessed 2024-07-21). [Online]. Available: https://nilepost.co.ug/uganda/202469/power-struggles-ugandas-uneven-electricity-distribution

[13] "Achievements and Challenges of Uganda's Power Sector". RMI. (accessed 2024-07-21). [Online]. Available: https://rmi.org/achievements-and-challenges-of-ugandas-power-sector/

[14] Minsait, "Utility Customer Information System - Technical Proposal for UMEME," 2024.

[15] "Prepayment Metering". UEDCL. (accessed 2024-07-11). [Online]. Available: https://www.uedcl.co.ug/prepayment-metering/

[16] "Umeme embarks on upgrade of Yaka meters". KIKUBO LANE. (accessed 2024-07-11). [Online]. Available: https://kikubolane.com/2024/01/08/umeme-embarks-on-upgrade-of-yaka-meters/

[17] "Prepayment". Itron. (accessed 2024-07-11). [Online]. Available: https://es.itron.com/es/categories/prepayment

[18] M. Onesait, "A World Class Customer Management Solution Supporting the future of utilities." [Online]. Available: www.acspower.com

[19] IDIS, "IDIS Package 3 Specification Summary," 2023.

[20] S. G. Hoffmann, R. Massink, and G. Bumiller, "New Security Features in DLMS/COSEM-a Comparison to the Smart Meter Gateway."

[21] D. Kohout, T. Lieskovan, and P. Mlynek, "Smart Metering Cybersecurity—Requirements, Methodology, and Testing," *Sensors*, vol. 23, 4 2023.

[22] I. Rigoev and A. Sikora, *Security Aspects of Smart Meter Infrastructures*. Springer Science and Business Media Deutschland GmbH, 2023, vol. 97, pp. 77–154.