AFSEC GUIDE 02 – APPLICATION OF STANDARDS FOR SMART METERING IN AFRICA

AN OVERVIEW

SHAWN PAPI
Member of AFSEC TC13 PT1, IEC TC13 WG14, SANC TC13 and NRS 049 WG

04 October 2018
CONTENTS

• Introduction

• Procurement and contracting of smart metering systems

• IT Infrastructure for smart metering systems

• Smart metering devices

• Communication technologies

• Safety and regulations

• Cyber security and data security

• Compliance testing requirements, resources and competencies
AFSEC TC13 PT1 has prepared the “AFSEC GUIDE 02” to:

- Provide guidance to African utilities with regards to the application of smart metering standards adopted by AFSEC TC13;

- Provide a basis for the design and deployment of *interoperable smart metering* systems across the African continent based on open standards;

- Highlight new regulatory requirements in relation to the safe operation and maintenance of smart metering systems, particularly issues such as remote load management and cyber security;

- Provide guidance on contracting and procurement of smart metering systems based on AFSEC metering standards;

- Provide guidance to African utilities on the design and deployment of IT infrastructure required as part of smart metering systems;
INTRODUCTION – GENERIC SMART METERING SYSTEM

SMART METERING DEVICES

COMMUNICATION TECHNOLOGIES

IT INFRASTRUCTURE

NOTE 1: Collector is also known as Data Concentrator/Network Gateway
NOTE 2: Private backhaul may be Optic Fiber, Ethernet WANs

INTRODUCTION – GENERIC COMMUNICATION ARCHITECTURE

- Enterprise Systems
  - 3rd Party Systems
  - Meter Data Management System
- Vending System
- Head-end System
- Network Gateway
  - Kiosk Controller
  - Appliance Control Device
  - Home Automation
- Metering Device
- Customer Interface Unit
  - Internet
  - Private Network
  - Social Media

Key to Colours:
- Systems Integration
- Field Integration
- Customer Integration
- Optional
To ensure efficient deployment of large-scale smart metering systems, it is recommended that tendering be done in sequential phases, as follows:

- Meter Data Management Systems (MDMS), where required;
- Head End Systems (HES) with smart metering devices;
- Metering enclosures (kiosks), where required;
- Device installations, including site audits, site clean-up;

Additionally, thorough training for utility staff should be included as a mandatory requirement in all smart meter tenders and contracts.
IT INFRASTRUCTURE

Thorough system integration testing (i.e. “system walk through”) should always be conducted by utility staff and the system vendor/integrator prior to commissioning and handover.

Relevant standards for IT systems include:

- NRS 049 South African industry specification for smart metering systems, architecture, data exchange and companion specification for COSEM functions;
- IEC 61968 series for application integration between Enterprise Resource Planning Systems (ERPS), MDMS, HES and other external systems;
- IEC 62056-1-0 framework for smart metering communications architecture;
- IEC 62056 series for communication protocols between HES and smart metering devices;
- IEC 62055 series for prepayment meters;
- SANS 1524-6-10 for prepayment token vending systems.

The guide provides a comprehensive, but not exhaustive, list of functional requirements for MDMS and HES.

Due consideration should be given to the extent of IT hardware capabilities required in relation to the amount of data to be stored, processed, etc.
SMART METERING DEVICES
Guide 02 covers the application of standards in relation to:

• Meter type testing;
• Acceptance and inspection methods;
• Prepayment meters;
• Vending systems and key management;
• Environmental and climatic requirements relevant to metering devices in Africa;
• Extended national requirements;
• Safety requirements;
• Meter dependability requirements;
• Bi-directional metering;
• Split or multi-part meter configuration;
• Data concentrator functionality;
Wi-Fi connects *different devices* from *different manufacturers*!

Wi-Fi networks ubiquitous – found in airports, restaurants...

Wi-Fi antennas comply with one specification (physics)
The interoperability framework for smart meter communication is defined in IEC 62056-1-0.
SAFETY RULES & REGULATIONS

New functionality brought about by smart metering systems, such as remote (dis)connect and load management, necessitate a re-evaluation of existing meter safety rules and regulations.

Guide 02 provides recommendations for:

• Safety aspects of switching consumer loads;
• Safety of remote switching algorithms;
• Customer safety aspects of device design;
• Public safety aspects of smart metering systems;
The transmission of customer data through public networks increases the vulnerability of smart metering systems to cyber-attack. Utilities need to consider:

• WHY SECURITY?
  ✓ Need to protect customer privacy and integrity of smart metering infrastructure

• WHAT TO PROTECT?
  ✓ Sensitive customer and operational data, such as consumption, debt, tariffs, etc.
  ✓ Critical commands, such as remote (dis)connect, tariff programming, over-air firmware upgrades and token transfers, etc.

• WHERE TO PROTECT?
  ✓ IT back-office
  ✓ Communication channels (Application Layer-to-Physical Layer)
  ✓ Field devices (Tamper resistance)
  ✓ End-to-end security

• HOW TO PROTECT?
  ✓ Application of standardised and approved security algorithms (NIST/FIPS, etc.)
  ✓ Implementation of appropriate security policy
COMPLIANCE TESTING REQUIREMENTS, RESOURCES & COMPETENCIES

Rigorous in-service and laboratory-based smart meter testing are essential to assure required performance, safety and revenue, Guide 02 covers recommendations for:

- Surveillance testing and in-service testing requirements and sampling procedures
- In-service safety testing
- Certification and accreditation
- Integrity of reporting and results
ACKNOWLEDGEMENTS

AFSEC Secretariat: Paul Johnson

AFSEC TC13 Chairman: Roland Hill

Project Leader: Casimir Nyirinkindi

Editors: Don Taylor & Dave Tarr

All members & invited experts of AFSEC TC13 PT1
THANK YOU