

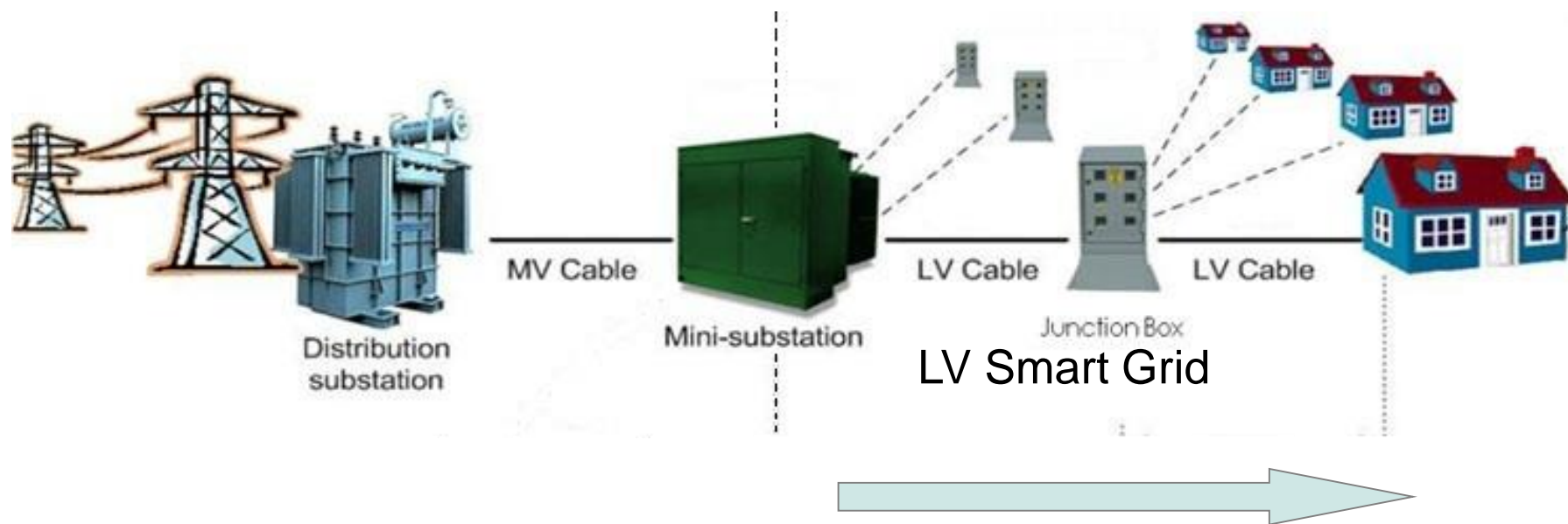
Secure Reliable Communications for the LV Smart Grid



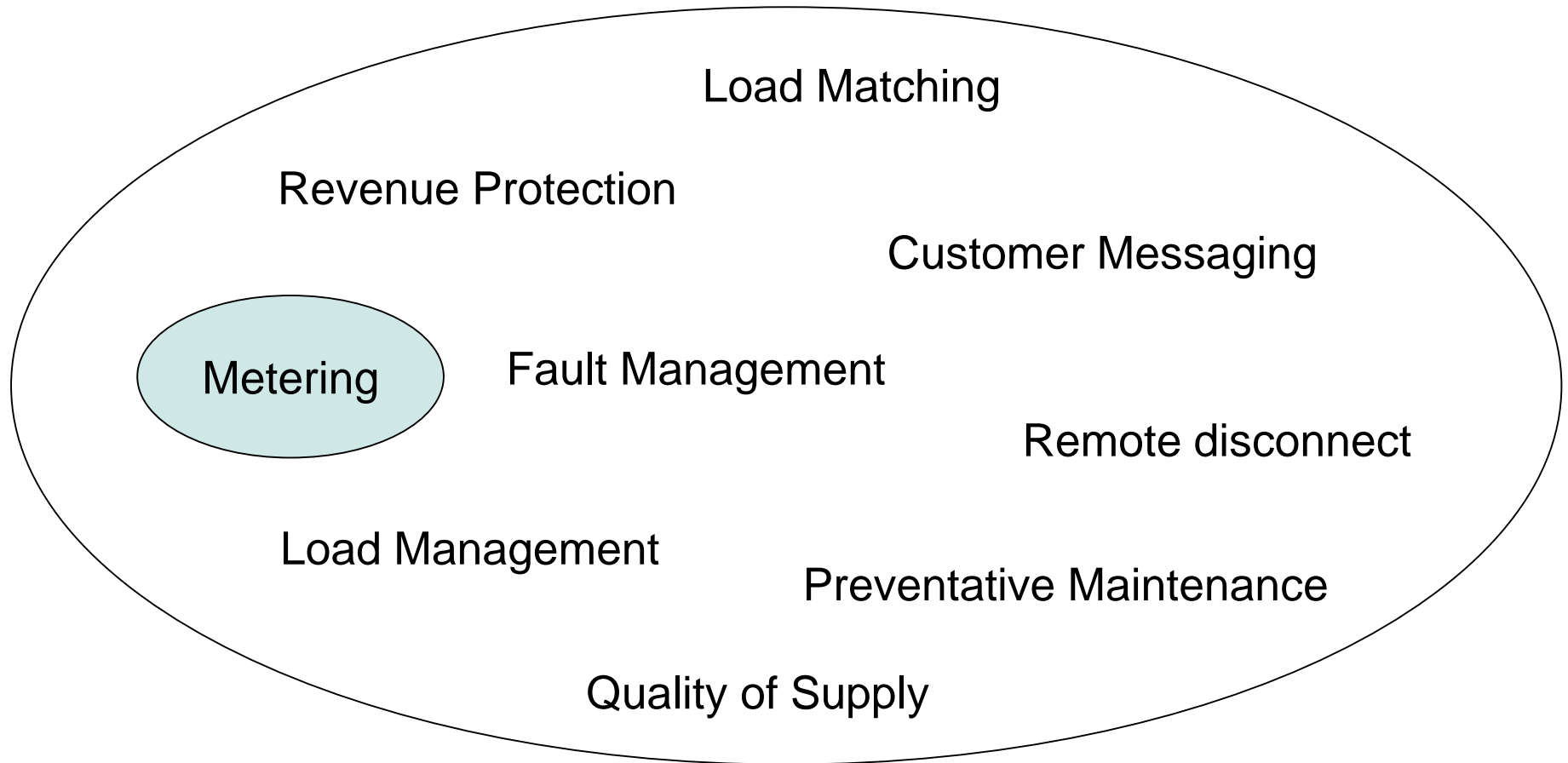
Andrew Goedhart
System Architect
Util Labs

andrew.goedhart@utilabs.com

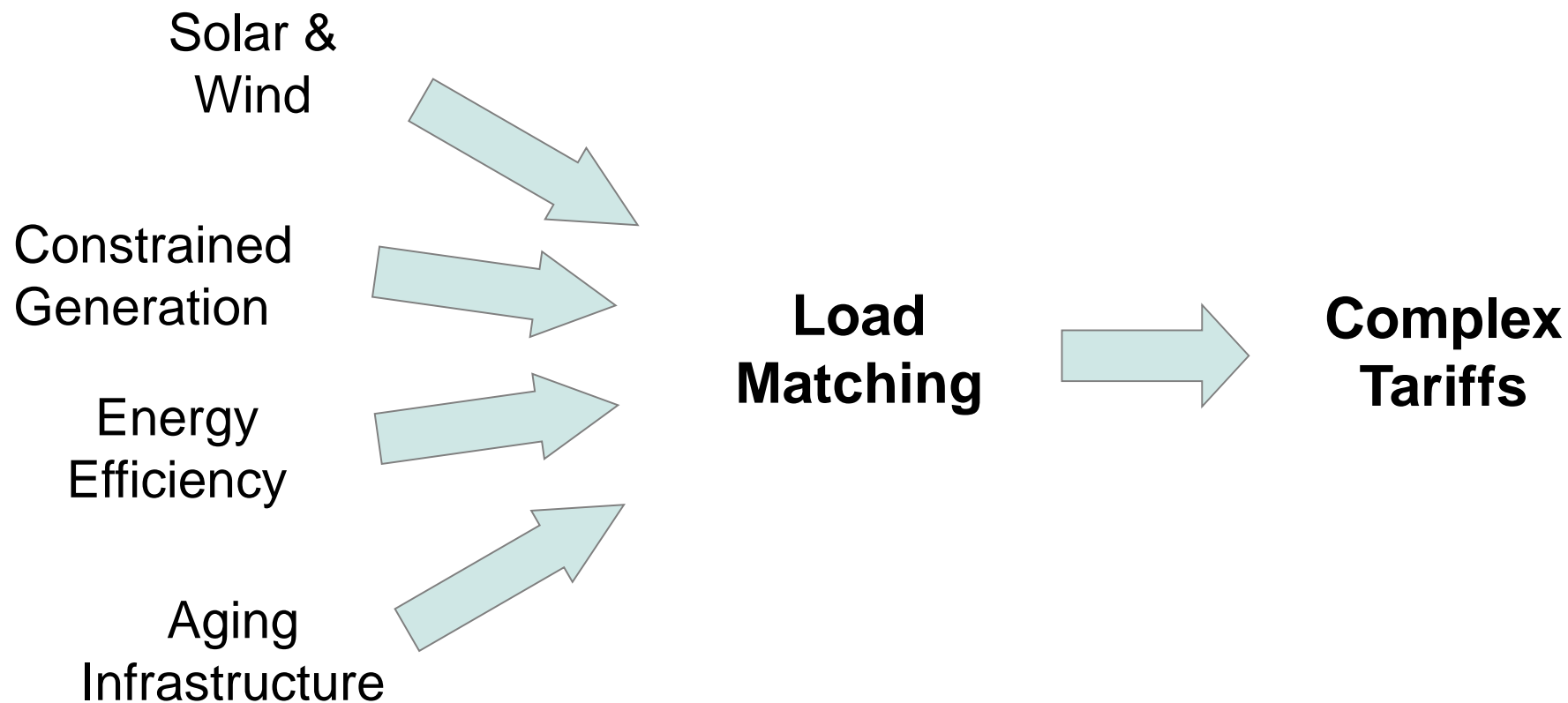
Location of LV Smart Grid



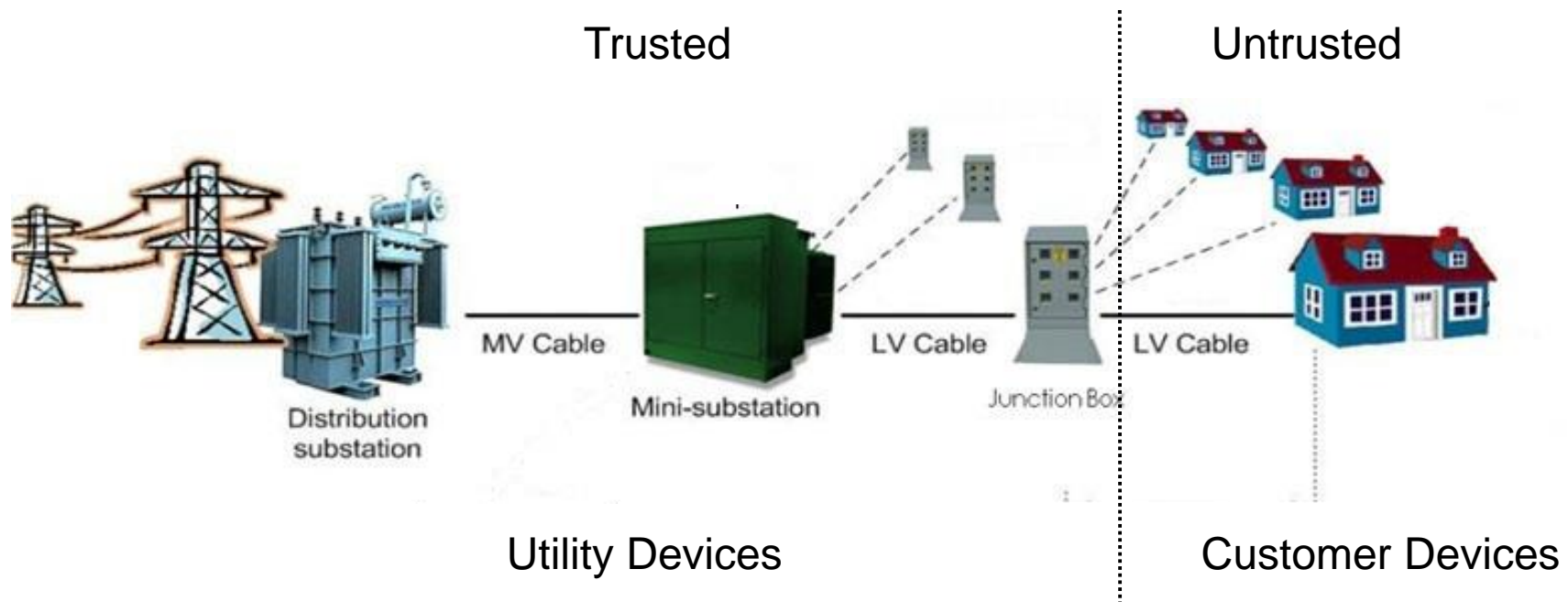
Functions of LV Smart Grid



Impact of Renewables

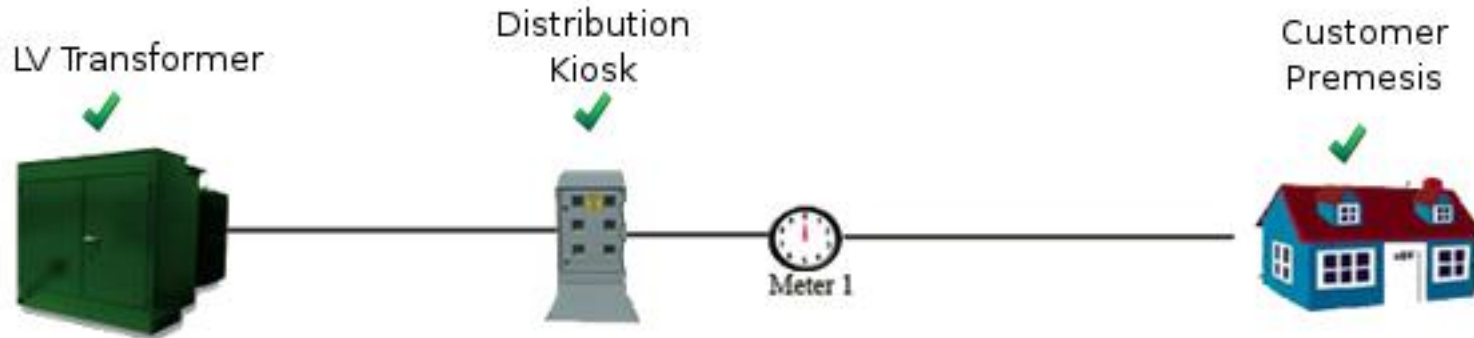


Impact of Renewables



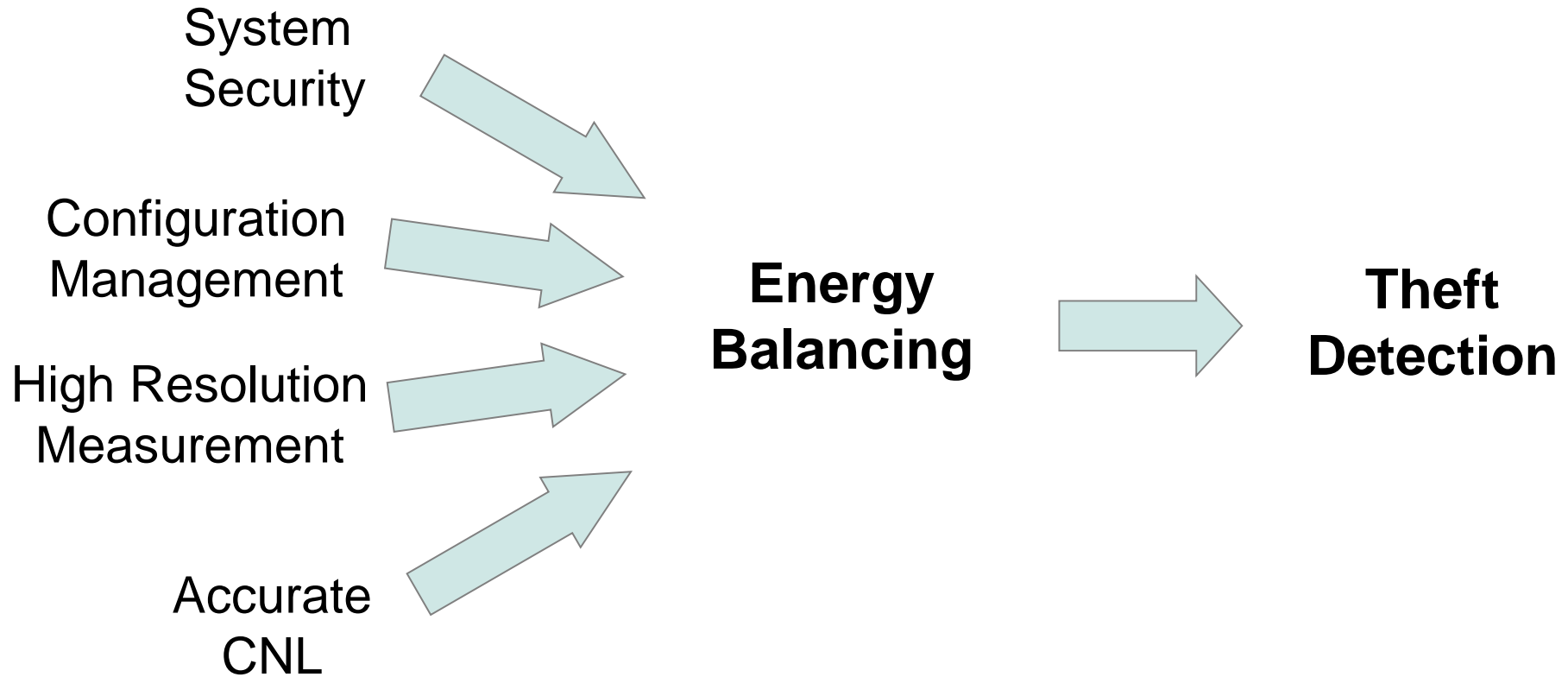
- Smart Grid extends into customer premises
 - Secure audit trails for billing
 - Privacy
- Customer devices incur cost based on supplied info

Operations and Maintenance



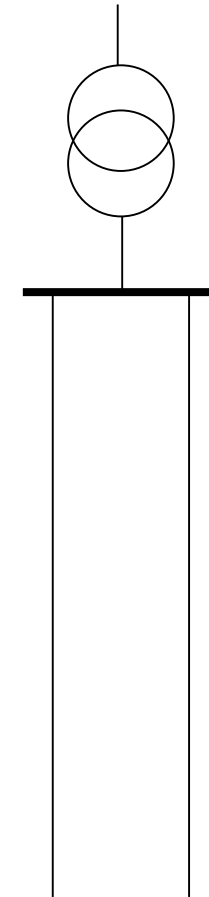
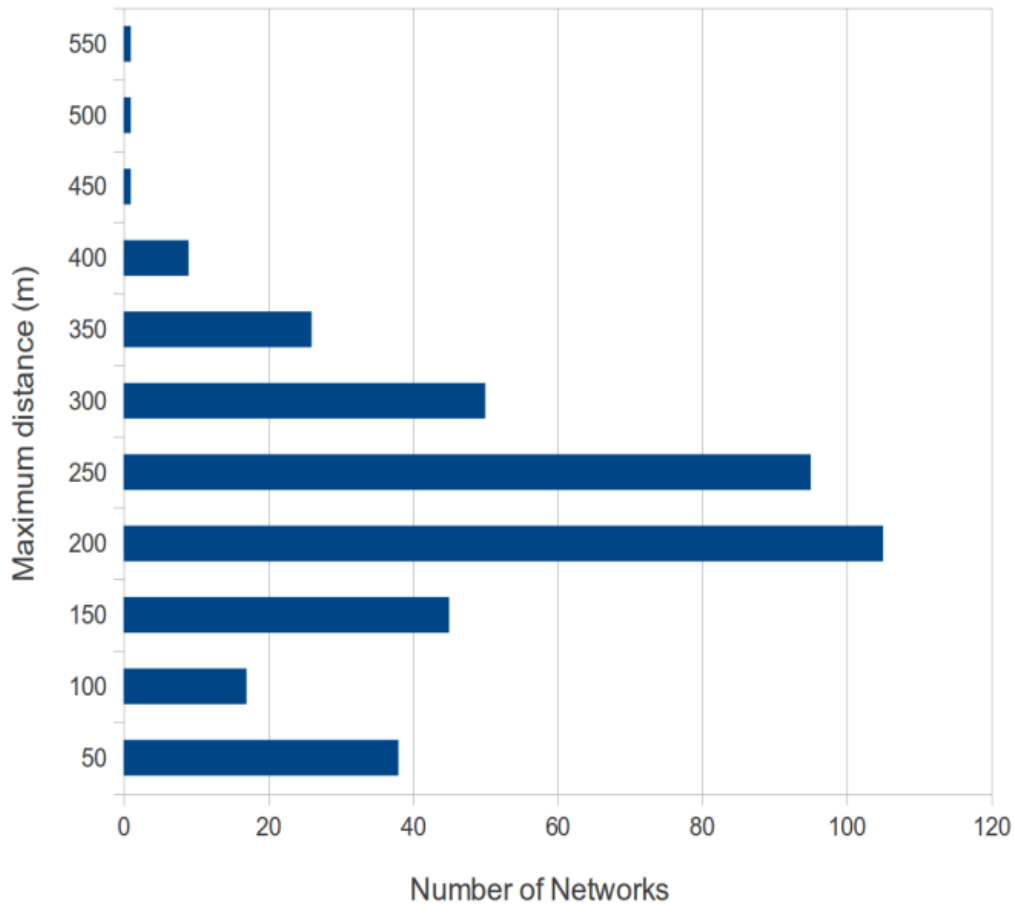
- Fault Location
 - Real-time Feedback
 - Push of Alarms
- Co-location of networks
 - Better **C**ustomer **N**etwork **L**ink data

Fraud and Theft Detection



Distribution Topology

Maximum Distance from Mini-substation to Kiosk

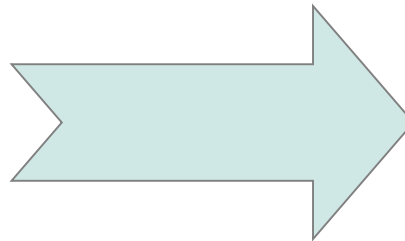


Communications Evolution

Metering

LV Smart Grid

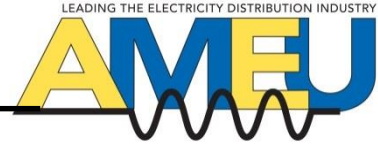
**Connection
Based Polling**



**Near Real-Time
Command and
Control**



System Requirements

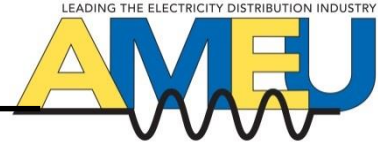


- Command and Control
 - Deterministic access/throughput under heavy load
 - Fairness
 - Priority
 - Low Latency
 - Increased data rates/ Increased data efficiency
 - Co-location of power and communication networks
 - Accurate timing
 - Robust security
-

Security

- Requirements
 - PPI bill
 - FIPS 200
 - NISTIR 7628
 - Device Authentication / Authorization
 - Data Encryption
 - Integrity / Non-repudiation
-

Current Standards



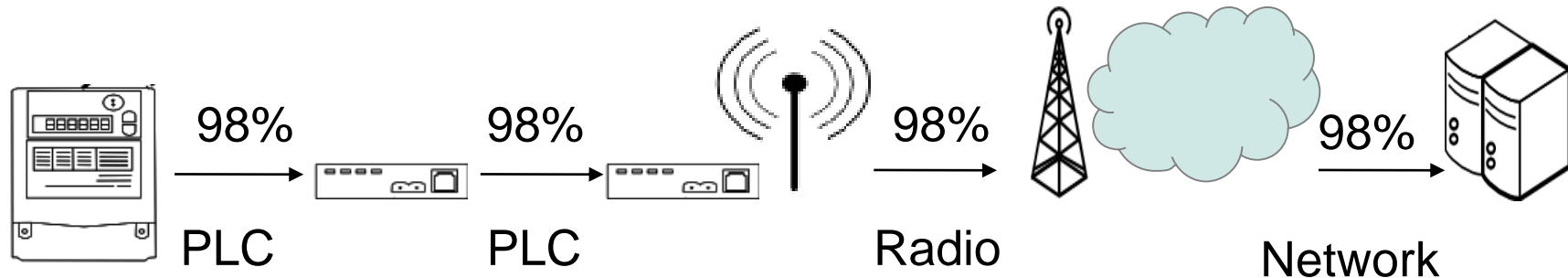
Metering SANS/IEC 62056-21)

Initially Designed for

- local serial Communications
- Infrequent meter reads
- Stand alone configuration of meter
- Inherent Problems
 - Session based
 - Does not meet basic security requirements
 - FIPS200, NISTIR 7628



Session Based



Chance of session based protocol succeeding:

$$0.98 \times 0.98 \times 0.98 \times 0.98 = 92\%$$

Store and forward performance field trials

99.7%

(Delivery of 24 hour measurement data)

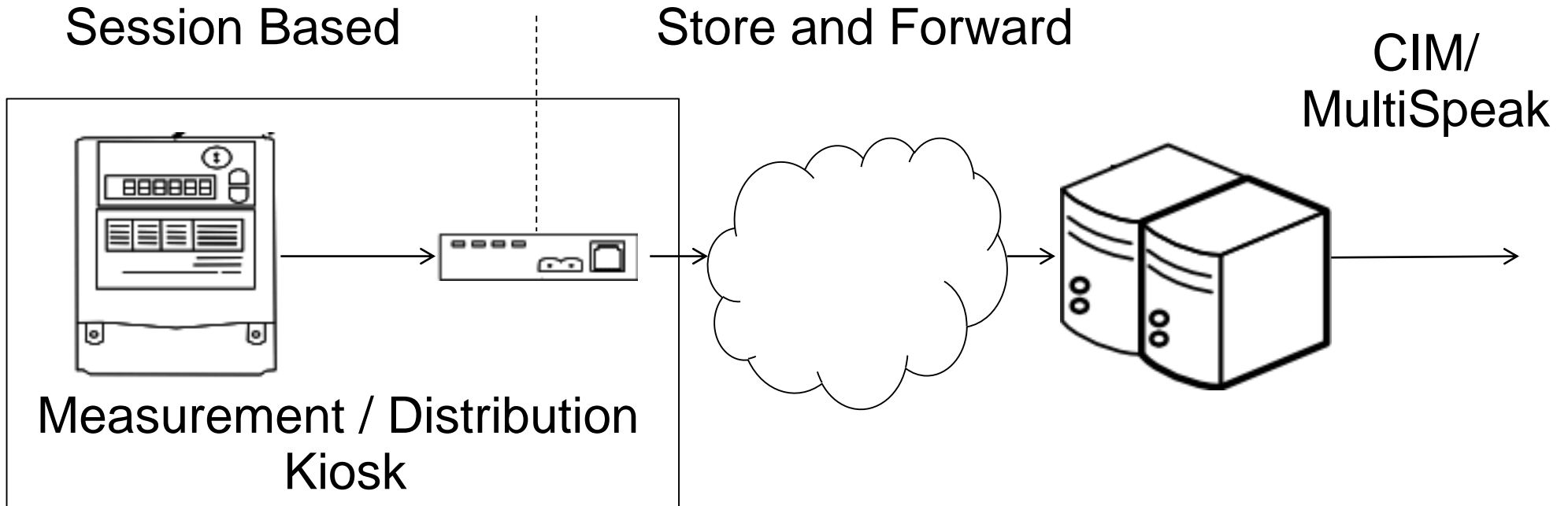
Protocol Level Optimizations

- High bit error rates
 - Small network packets
 - Optimising bandwidth
 - Reduce routing and packet overhead
 - Data compression
 - Links Frequently dropped
 - Packet based push
 - Store and forward
 - Implement FIPS security standards
-

PLC Physical Layer

- SANS 50065-1:2012 and ICASA allow both
 - CENLEC A (3Khz – 95kHz)
 - FCC (150-480 kHz)
 - FCC has better:
 - Smaller form factor
 - Lower cost
 - Less noise
 - More bandwidth
 - Open Standards: Prime vs G3
 - Field tests -> **G3-PLC (FCC -1 profile)**
-

Open Solution



- DLMS-COSEM session kept local
- Multiple managed by local gateway
- Packet based store and forward out of kiosk