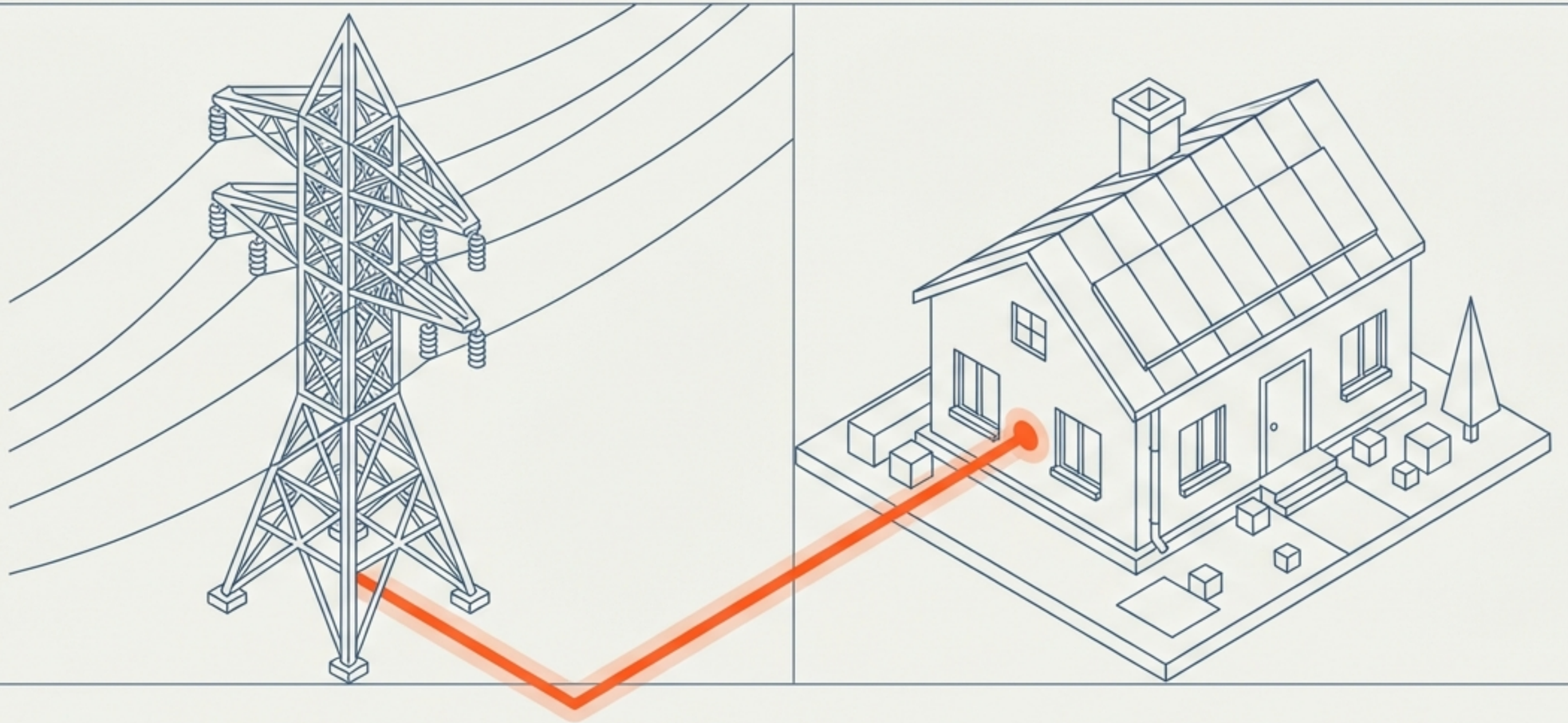


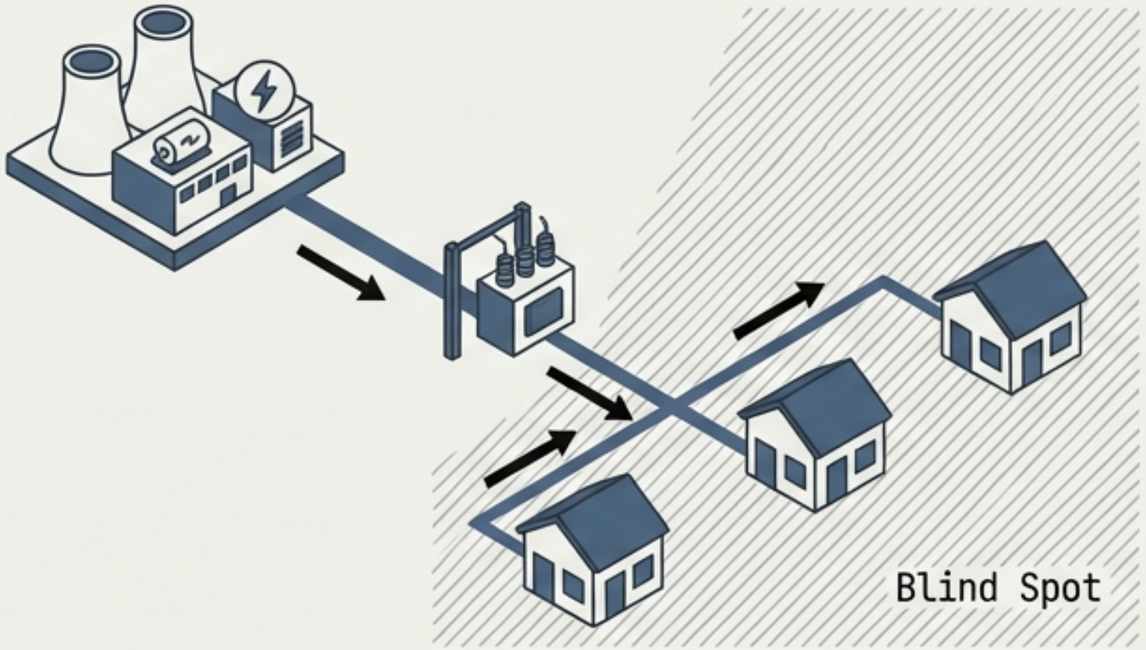
Smart System Automation – The Intelligent Edge

Course EE-3020 | Department of Electrical Engineering

Professor: Selvanathan T.

The Grid is Blind Beyond the Substation

TRADITIONAL GRID



Supply-Following-Demand Model.
The utility cannot see consumption in real-time.
Result: Inefficiency, Over-provisioning, Blackout Risk.

SMART GRID

Demand-Following-Supply Model.
Enabled by ICT (Information and Communication Technology).
Result: Full visibility, Peak Shaving, Dynamic Stability.

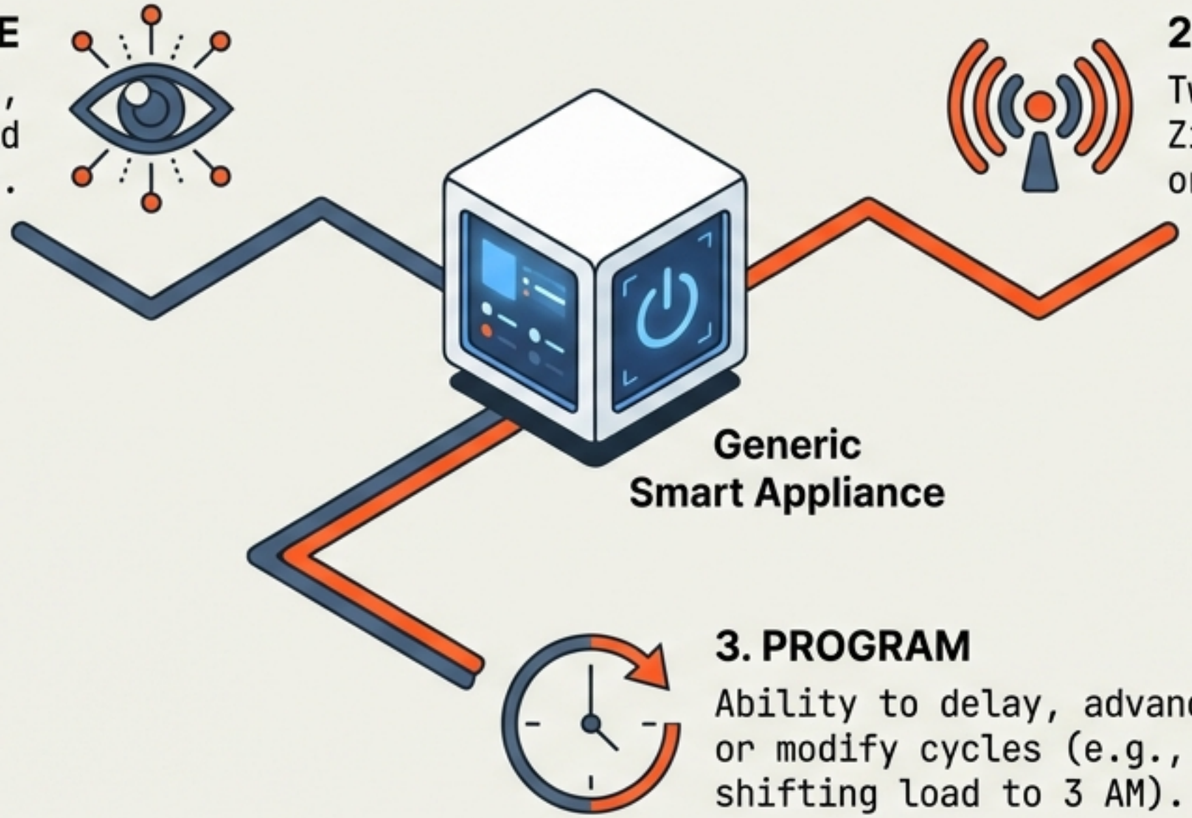
CORE CONCEPT: Demand-Side Management (DSM) & Demand Response (DR).
Solving infrastructure strain by adjusting usage, not just increasing generation.

The Actuators: Smart Appliances

Definition: Devices capable of sensing, receiving, and responding to operational signals to optimize energy consumption.

1. SENSE & INTELLIGENCE

Detects operational cycles, user presence, and grid signals.



2. COMMUNICATE

Two-way data transfer via Zigbee, Wi-Fi, Bluetooth, or PLC.

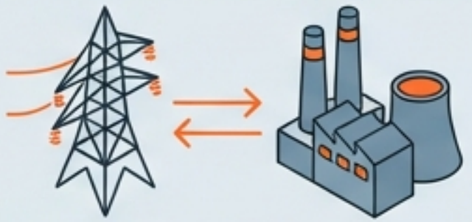
3. PROGRAM

Ability to delay, advance, or modify cycles (e.g., shifting load to 3 AM).

EXAMPLES: Smart AC (Geofencing), Smart Water Heater (Thermal Storage), Smart EV Charger (Managed Charging).

Value Generation at the Edge

FOR THE UTILITY (GRID OPERATOR)



Peak Load Reduction:
Flattens the demand curve.

Stability:
Acts as a virtual distributed energy resource.

Capital Efficiency:
Deferred investment in new peaker plants.

FOR THE CONSUMER

Economics:
Cost savings via Time-of-Use (TOU) tariffs.

Automation:
Remote control and “set-it-and-forget-it” convenience.

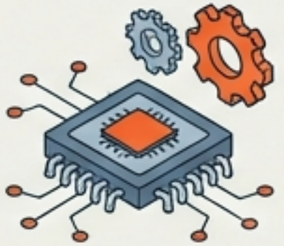
Sustainability:
Reduced carbon footprint by aligning usage with renewable availability.

Diagnostic Checkpoint: The Smart Appliance

01. CAPABILITY CHECK

Which is NOT a core smart capability?

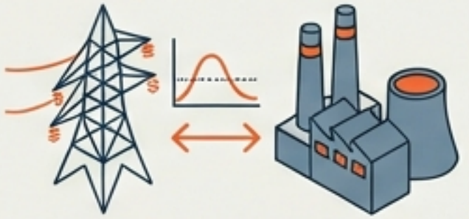
- [A] Two-way communication
- [B] Self-repair of internal circuits
- [C] Response to price signals



02. BENEFIT CHECK

What is the primary grid benefit of smart appliances?

_____

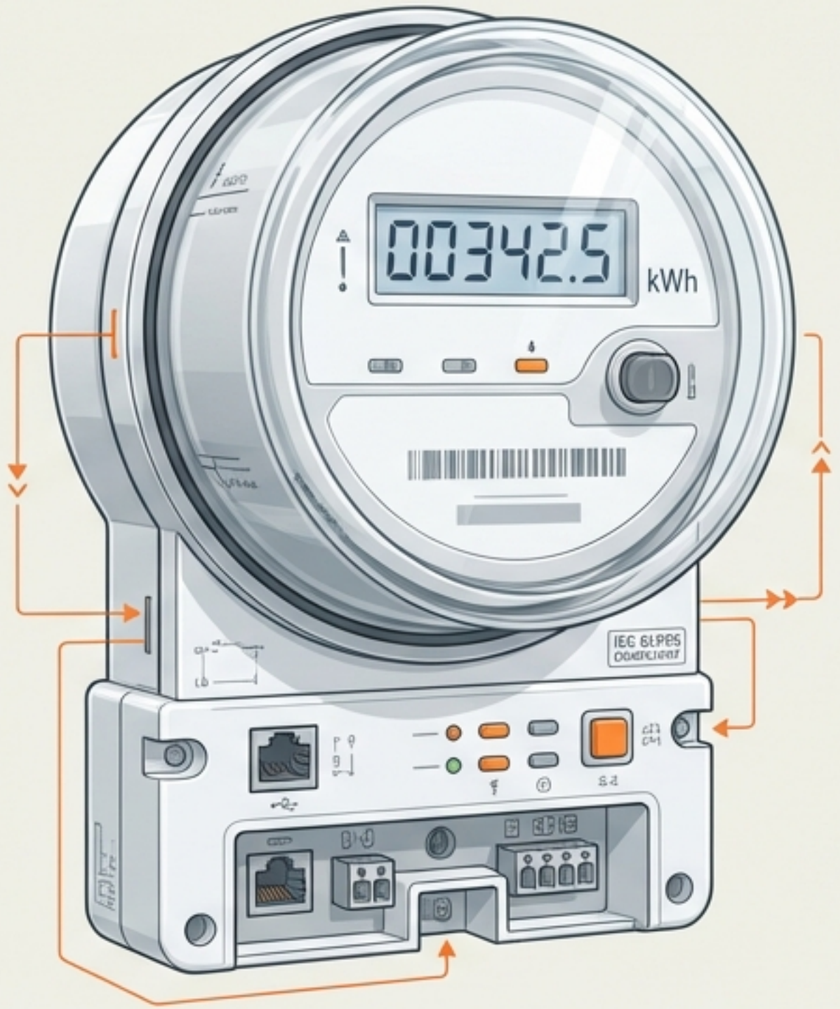


03. SCENARIO CHECK

True or False: A dishwasher running at 2 AM due to a low-cost signal is Demand Response.

[TRUE] / [FALSE]

The Gateway: Meet the Smart Meter



DEFINITION

IEC 62056 DEFINITION: A metering device that can measure, store, and report energy data, and has bidirectional communication capabilities.

CORE FUNCTIONS

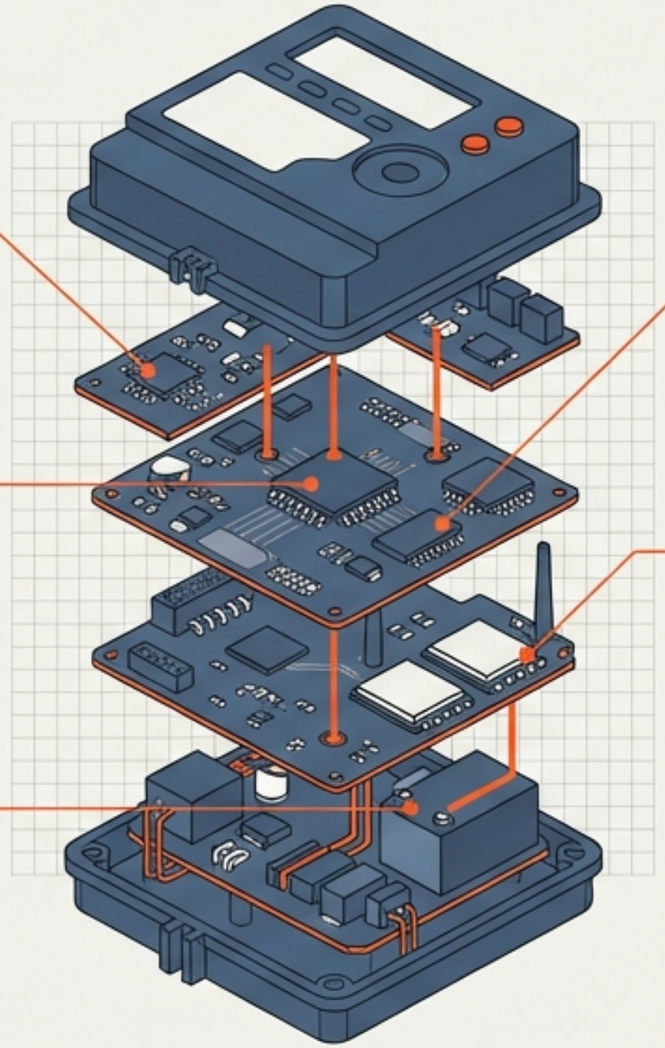
- **AMR (Automated Meter Reading):** Eliminates manual errors.
- **Dynamic Pricing:** Supports Time-of-Use (TOU) and Critical Peak Pricing (CPP).
- **Grid Visibility:** Instant outage detection and restoration verification.
- **HAN Gateway:** Acts as the communication hub for the Home Area Network.

Deconstructing Meter Architecture

Measurement Unit
High-precision ADC with voltage/current sensors.

MCU (Processing Unit)
Computes kWh, kVArh, Power Factor.

Power Supply
Includes backup for outage reporting.



Secure Memory
Stores firmware, keys, and logs.

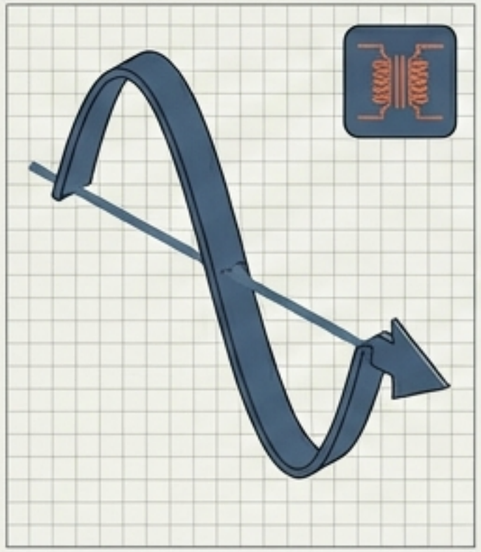
Communication Modules
WAN (to Utility) & HAN (to Home).

STANDARD: IEC 62056 (DLMS/COSEM) governs data exchange.

From Analog Signals to Digital Data

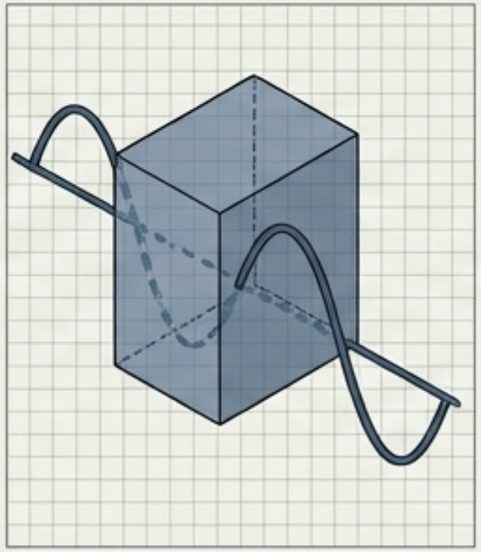
The Physics of Measurement

SENSING



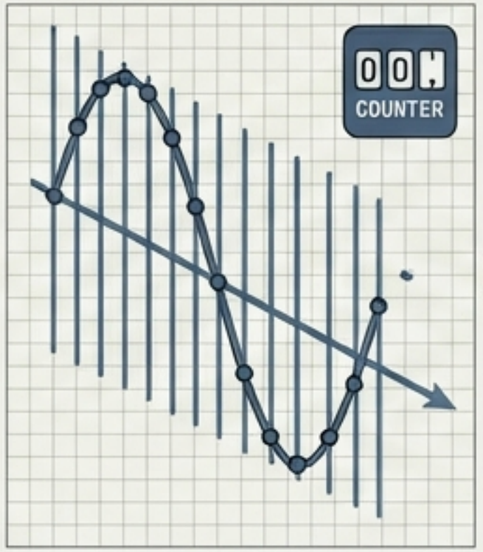
Current Transformers (CTs) step down high voltage/current.

CONDITIONING



Filtering and anti-aliasing.

ADC SAMPLING



Digital sampling (e.g., 128 samples/cycle).

CALCULATION

$$E = \int p(t)\,dt$$

Instantaneous Power

$$p(t) = v(t) \times i(t)$$

Accuracy Class: 0.5, 1.0, or 2.0 (IEC 62053)

Diagnostic Checkpoint: Meter Fundamentals

01. ARCHITECTURE CHECK

Which module communicates with the utility head-end system?

- [x] HAN Interface
- [x] WAN Interface
- [x] Optical Port

02. MATH CHECK

The standard digital calculation for Active Energy (kWh) involves:

Integrating the product of instantaneous voltage and current samples.

03. STANDARDS CHECK

What does IEC 62056 primarily govern?

_____

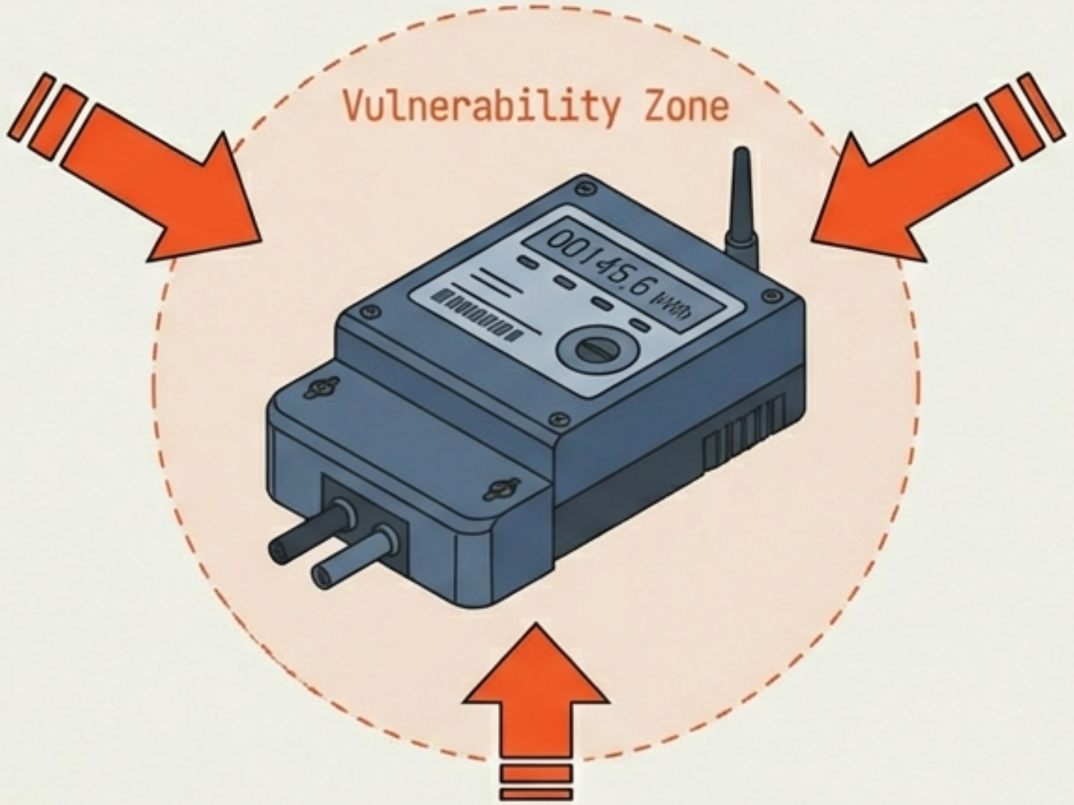
ANSWERS: 1. WAN Interface. | 2. Integration of V x I samples. | 3. Communication and data exchange.

The Attack Surface

Smart meters are both revenue collection points and critical grid sensors.

FINANCIAL FRAUD

Energy theft via tampering or data manipulation.



PRIVACY INVASION

High-resolution consumption data reveals user lifestyle patterns.

GRID ATTACK

Compromised meters used for DoS attacks or destabilizing load swings.

Security Domains & Principles

Framework: NISTIR 7628 Guidelines for Smart Grid Cybersecurity

Extended CIA Triad Diagram

Confidentiality

Protect consumer data

Integrity

No data alteration

Availability

Operational uptime

Auth & Auth

Identity & Permissions

LOGICAL DOMAINS

- **DEVICE DOMAIN:** Secure Boot, Hardware Security Modules (HSM).
- **COMMUNICATION DOMAIN:** Encryption (AES), Authentication (HMAC).

Threat Vectors and Countermeasures

Key Standard: IEC 62351 for data security.

DOMAIN	ATTACK VECTOR	ENGINEERING COUNTERMEASURE
PHYSICAL	Tampering with CT connections; Opening casing.	Tamper switches, Holographic seals, Event logging.
NETWORK	Eavesdropping, Replay Attacks, Man-in-the-Middle.	Strong Encryption (AES-128/256), TLS/DTLS, Cryptographic Nonces.
FIRMWARE	Exploiting code bugs for remote control.	Code integrity checks, Digitally signed firmware (PKI).

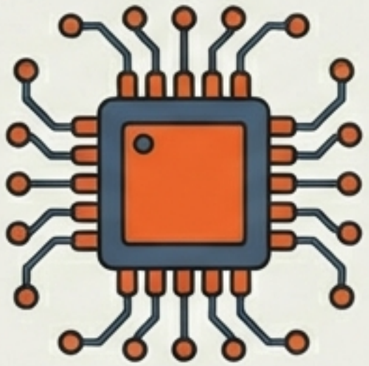
Scenario Analysis: The Corrupted Update

THE SITUATION: A utility finds hundreds of meters sending corrupted billing data, differing from local displays. Cause: Compromised firmware.

OBJECTIVE VIOLATED?

INTEGRITY.
Data altered between source and destination.

DOMAIN TARGETED?

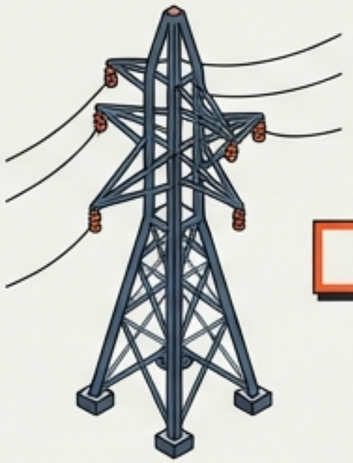
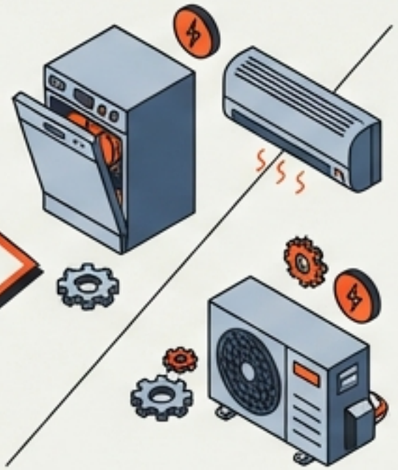


DEVICE/SOFTWARE DOMAIN.
Malicious code running on the meter itself.

MITIGATION?

DIGITALLY SIGNED FIRMWARE.
Ensures code is authentic and from a trusted source before execution.

The Smart Home Ecosystem: End-to-End

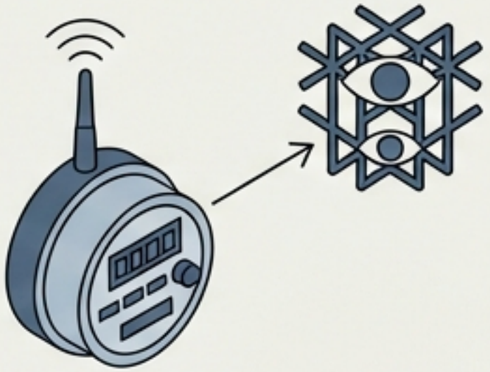
1 GRID	2 GATEWAY	3 INTELLIGENCE	4 ACTION	
	WAN 	HAN / Zigbee 	Command 	**RESULT:** Load reduced during 5-9 PM peak window.
Sends TOU Price Signal.	IEC 62056. Broadcasts to home.	Receives price. Decides action.	Delays load to off-peak.	

The Intelligent Edge: Key Takeaways

01. ACTUATORS

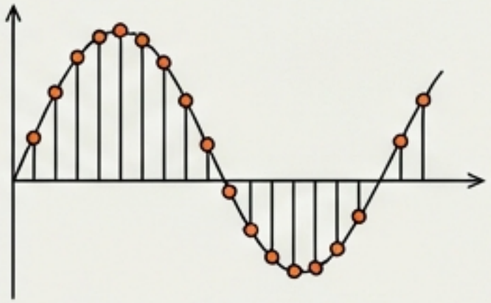
Smart Appliances provide the necessary demand-side flexibility.

02. GATEWAY



Smart Meters enable the transition from ‘Blind’ to ‘Sentient’ grids.

03. PRECISION



$$E = \int p(t)\,dt$$

Energy measurement is a digital sampling process. $E = \int p(t)\,dt$.

04. DEFENSE

Security (NISTIR 7628) is a core design requirement, not an add-on.