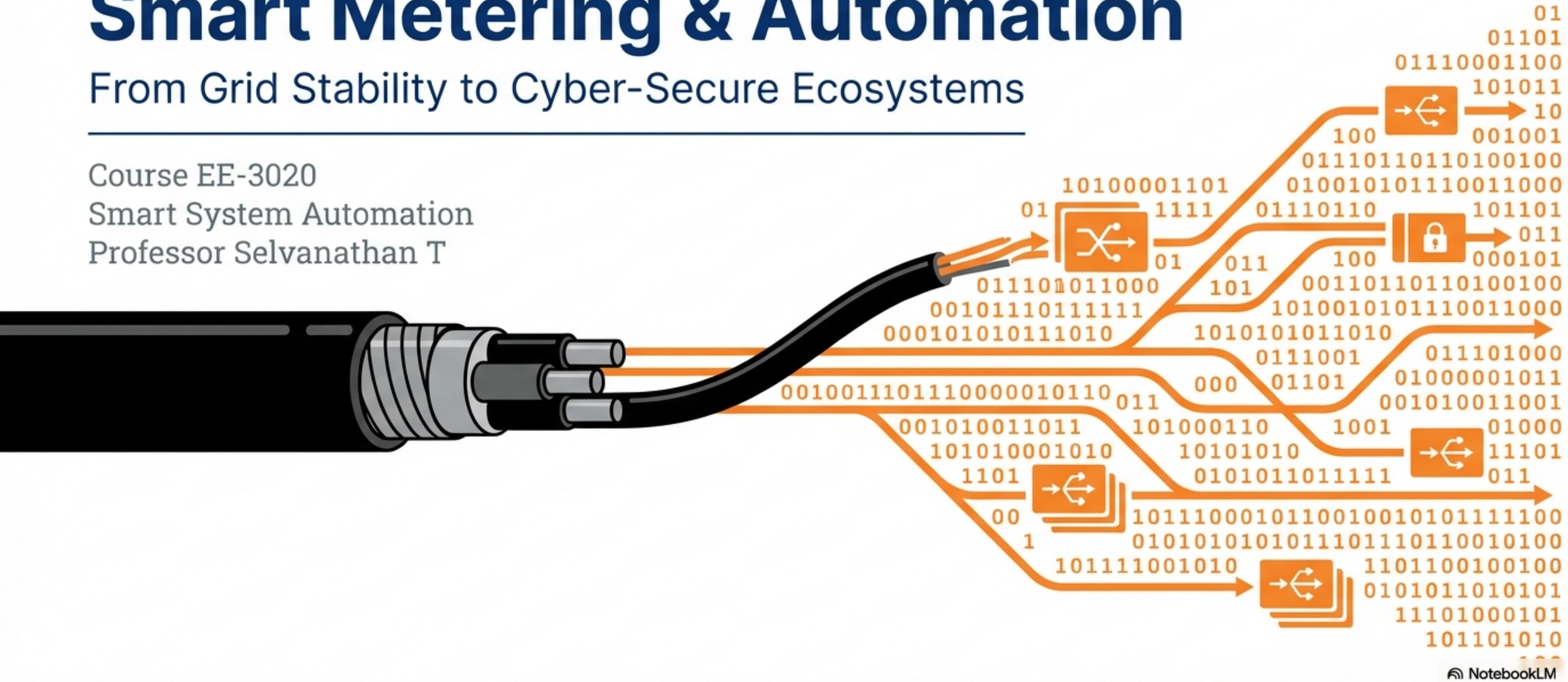
The Intelligent Edge: Smart Metering & Automation

From Grid Stability to Cyber-Secure Ecosystems

Course EE-3020
Smart System Automation
Professor Selvanathan T



The Grid in the Dark: Why Modernization is Critical

The Problem

The Blind Spot: Traditional grids lose visibility beyond the substation.

The Consequence: Peak demand strains infrastructure, leading to inefficiency and potential blackouts.

Old Paradigm: Supply-following-demand (Reactive).

The Solution

The Shift: Demand-following-supply (Proactive).

Key Concept 1: Demand-Side Management (DSM)
Planning and implementation of utility activities to influence consumer use.

Key Concept 2: Demand Response (DR)
Mechanisms encouraging consumers to reduce demand during peak hours.

The Actuators: Defining Smart Appliances

A residential or commercial appliance that can sense, receive, and respond to operational signals to optimize energy consumption.

Two-Way Communication

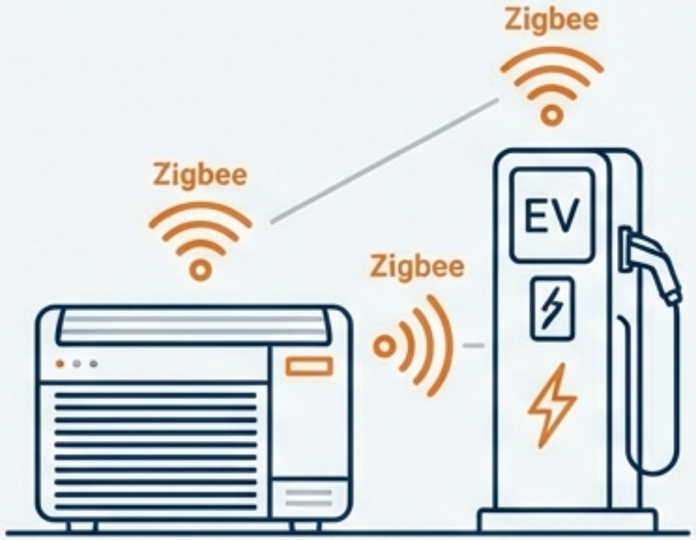
Utilizes Zigbee, Wi-Fi, Bluetooth, or Power Line Carrier (PLC) to talk to the ecosystem.

Sensing & Intelligence

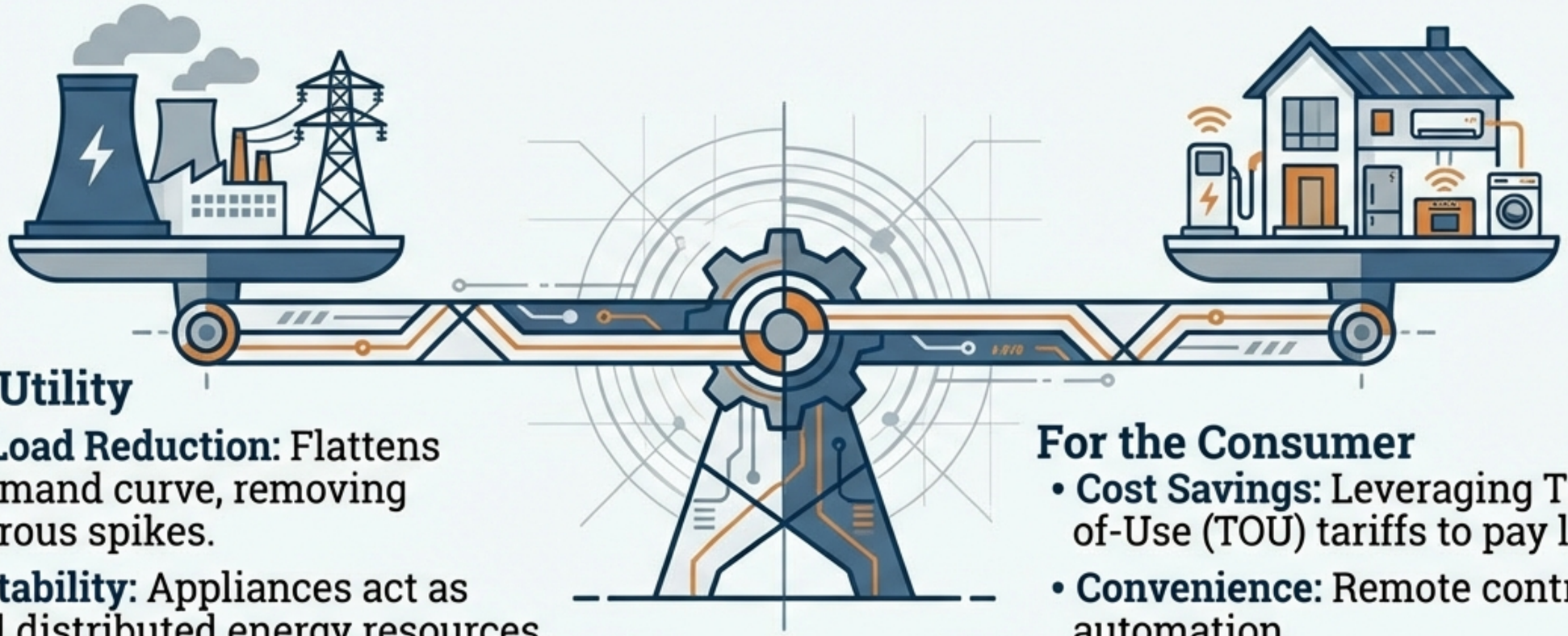
Detects operational cycles, user presence, and grid signals independently.

Programmability

Can delay, advance, or modify cycles (e.g., shifting a a dishwasher cycle to 3 AM).



The Value Proposition: Utility Efficiency meets Consumer Control



For the Utility

- **Peak Load Reduction:** Flattens the demand curve, removing dangerous spikes.
- **Grid Stability:** Appliances act as virtual distributed energy resources.
- **Deferred Investment:** Reduces capital need for new 'peaker' plants.

For the Consumer

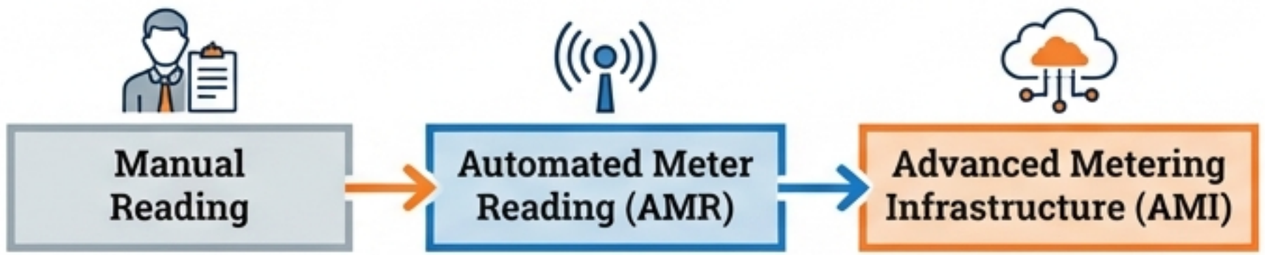
- **Cost Savings:** Leveraging Time-of-of-Use (TOU) tariffs to pay less.
- **Convenience:** Remote control and automation.
- **Carbon Footprint:** Aligns heavy usage with renewable energy availability.

The Gateway: Introduction to the Smart Meter

The Definition (IEC 62056)

A metering device that can measure, store, and report energy data, and has bidirectional communication capabilities to support advanced metering and control functions.

The Evolution



Key Functions

1. **Dynamic Pricing:** Supports Time-of-Use (TOU) and Critical Peak Pricing.
2. **Outage Detection:** Instantly pinpoints faults without customer calls.
3. **HAN Gateway:** Acts as the central hub for the Home Area Network.

Under the Hood: Smart Meter Architecture

Measurement Unit
(Sensors/ADC)

Processing Unit
(MCU/Power Factor Calc)
& **Secure Memory**
(Firmware/Keys)

Northbound Interface (WAN)

To Utility: Cellular (4G), RF Mesh, or PLC.

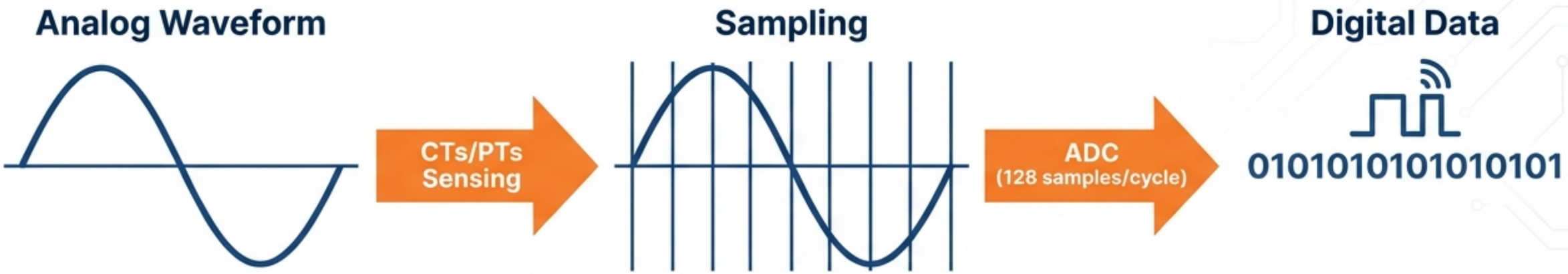
Southbound Interface (HAN)

To Home: Zigbee, Wi-Fi, Bluetooth.

Power Supply Unit
(with Backup Battery)

Standard Reference: IEC 62056 (DLMS/COSEM)

The Math of Measurement: From Analog to Digital



The Process

Sensing -> Signal Conditioning (Filtering) -> ADC Conversion.

The Core Formula

Active Energy (kWh) is the integration of instantaneous power over time:

$$Active\ Energy = \int p(t)dt$$

Digitally calculated as: $\sum[v(n) * i(n) * \Delta t]$

Accuracy Standards

Must meet Class 0.5, 1.0, or 2.0 requirements (IEC 62053-21/22).

Knowledge Checkpoint: Architecture & Function

Challenge: Which is NOT a core capability of a smart appliance? **(A)** 2-way comms, **(B)** Self-repair, **(C)** Programmability.

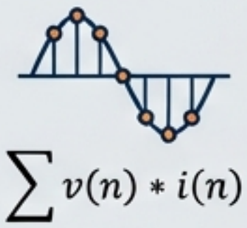
(B) Self-repair. Smart appliances diagnose, but self-repair is not a standard energy management feature.

Challenge: Which module connects the meter to the utility head-end system?

The WAN Interface. (Wide Area Network). The HAN connects inwardly to the home.

Challenge: How is Active Energy (kWh) calculated digitally?

Integration of samples. It is the summation of instantaneous voltage and current products.



The Attack Surface: Why Security is Paramount

Financial Fraud

Energy theft via tampering or data manipulation to lower bills

Grid Attacks

Compromised meters used for Denial-of-Service (DoS) or destabilizing load swings

Privacy Invasion

Granular consumption data revealing lifestyle patterns (occupancy, sleep schedules).

The Stakes: The meter is both a revenue collection point and a critical grid sensor.

Security Architecture & Domains

Based on NISTIR 7628 Guidelines

The Extended CIA Triad

- **Confidentiality:** Protect consumer data.
- **Integrity:** Ensure data/commands are not altered.
- **Availability:** Ensure operational uptime.
- **Authentication:** Verify identity and permissions.

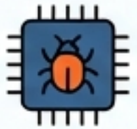
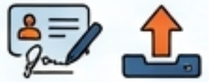
Logical Security Domains

Communication Domain
(Encryption/AES, Message Auth/HMAC)

Device Domain
(Secure Boot, Hardware Security Modules)

Data Domain
(Anonymization, Secure Storage)

Vulnerabilities & Countermeasures

Attack Type	Example	Defense Strategy
Physical Attacks 	Tampering with CT connections.	Tamper detection switches, seals, event logging. 
Network Attacks 	Eavesdropping or Man-in-the-Middle (MitM).	TLS/DTLS, Strong Encryption, Cryptographic nonces. 
Software Attacks 	Exploiting bugs for remote control.	**Signed Firmware Updates** (Prevents unauthorized code execution). 

The Compliance Landscape: Key Standards

Best Practice Philosophy: Defense-in-Depth (Layers) and Least Privilege (Restricted Access).

Security Scenario Analysis: The Corrupted Update

Case File

The Scenario

A utility discovers meters sending corrupted billing data. Local displays are correct, but reported data is wrong. Investigation reveals a compromised firmware update was installed.

The Violation

Integrity.
Data was altered between measurement and reporting.

The Vector

Device/Software Domain.
Malicious code introduced via update.

The Fix

Digitally Signed Firmware.
Ensures only authentic code from vendor is accepted. Encryption alone would not solve this.

Synthesis: The Smart Home Ecosystem in Action

Scenario: 5 PM - 9 PM Peak Pricing Event

Utility

Sends Price Signal via WAN

Smart Meter

Verifies signal, broadcasts to HAN (Zigbee)

Home Energy Manager

Processes signal against user preferences

Smart Appliance

Delays cycle until 11 PM

Outcome: Peak load reduced, consumer costs lowered, grid stability maintained.

Standards: IEC 62056, Zigbee Smart Energy, IEC 62351.

Summary: The Intelligent Edge

Actuators

Smart appliances provide demand-side flexibility.

Gateway

Smart meters are the foundation for measurement and control.

Precision

Energy is now a digital computation:

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

Defense

Security is a non-negotiable design requirement (NISTIR 7628).

The grid is no longer a one-way street of power; it is a bi-directional network of data, intelligence, and trust.