Technical Options to Address Cyber Security, Interoperability and Other Issues with ZigBee SEP

July 27, 2011

Webinar Presentation to the Smart Grid Investment Grant (SGIG) Consumer Behavior Study (CBS) Utility Forum

Ron Hofmann

CaRon Energy Strategies

Roger Levy

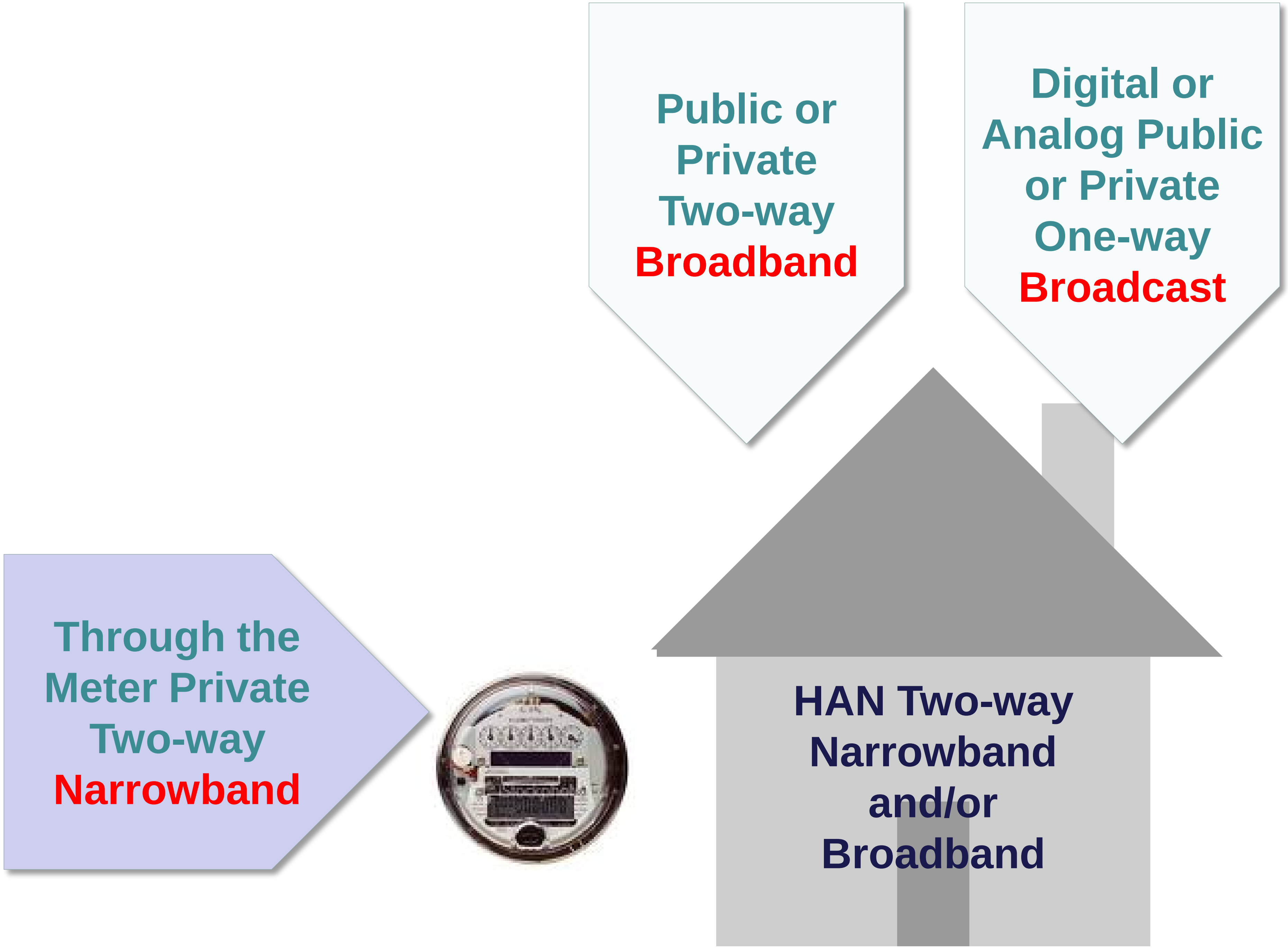
Levy Associates

Karen Herter

Herter Energy Research Solutions

BERKELEY LAB

Communication Options To / Within HAN



Public or Private Two-way **Broadband**

Digital or Analog Public or Private One-way **Broadcast**

Through the Meter Private Two-way **Narrowband**

HAN Two-way Narrowband and/or Broadband

Communication Options

❑ **Narrowband (RF)**

- ZigBee (IEEE 802.15.4)
- Wireless HART (IEEE 802.15.4)
- Z-wave (proprietary)

❑ **Broadband (RF, wired and Powerline Carrier (PLC))**

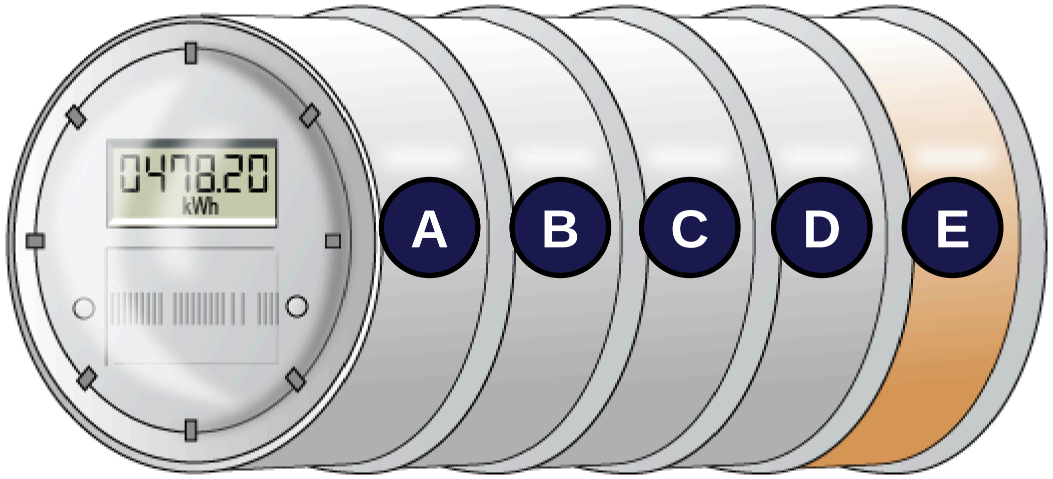
- WiFi (IEEE 802.11)
- Ethernet (IEEE 803)
- HomePlug (IEEE P1901)
- Cellular (GPRS)

❑ **Broadcast (RF)**

- AM/FM analog radio (private frequency)
- Digital FM radio (RDS/ RBDS)
- Paging (private frequency)

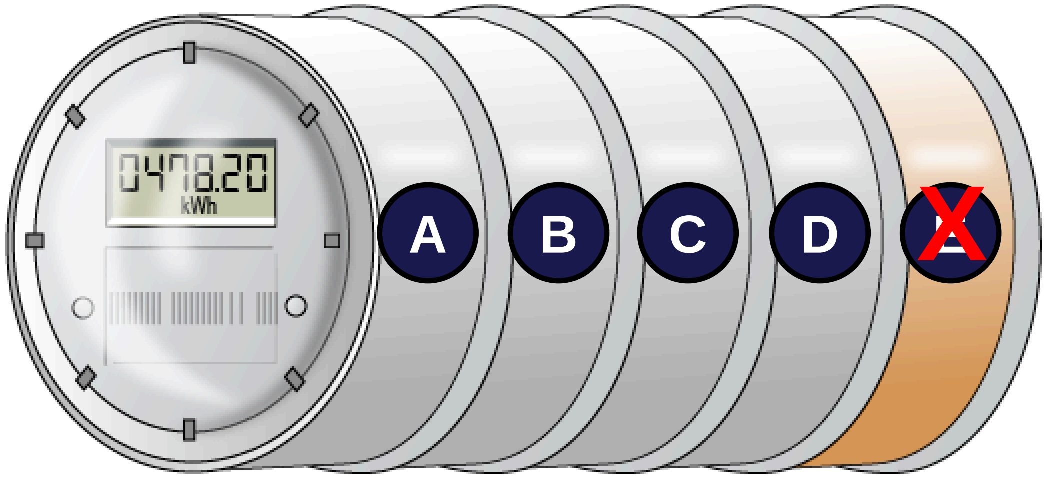
Which Meter are you Using?

1 Smart Meter with HAN Gateway



A. Metrology
B. Service Switch
C. Utility (AMI) Network Transceiver
D. Computing and Memory
E. HAN Gateway Transceiver (ZigBee Pro, SEP 1.0)

2 Smart Meter no HAN Gateway



A. Metrology
B. Service Switch
C. Utility (AMI) Network Transceiver
D. Computing and Memory
~~E. HAN Gateway Transceiver (ZigBee Pro, SEP 1.0)~~

What is ZigBee ?

- ❑ Started in 1998 (ZigBee Alliance, 2003)
- ❑ Two-way wireless **narrowband** communication specification
  - ▪ Low-cost and low-power
  - ▪ Mesh network topology for personal area networks
- ❑ Still evolving
  - ▪ SEP 1.0 layered on ZigBee Pro*, not secure
  - ▪ SEP 1.1 layered on ZigBee Pro*, not secure
  - ▪ SEP 2.0 layered on ZigBee IP, not complete

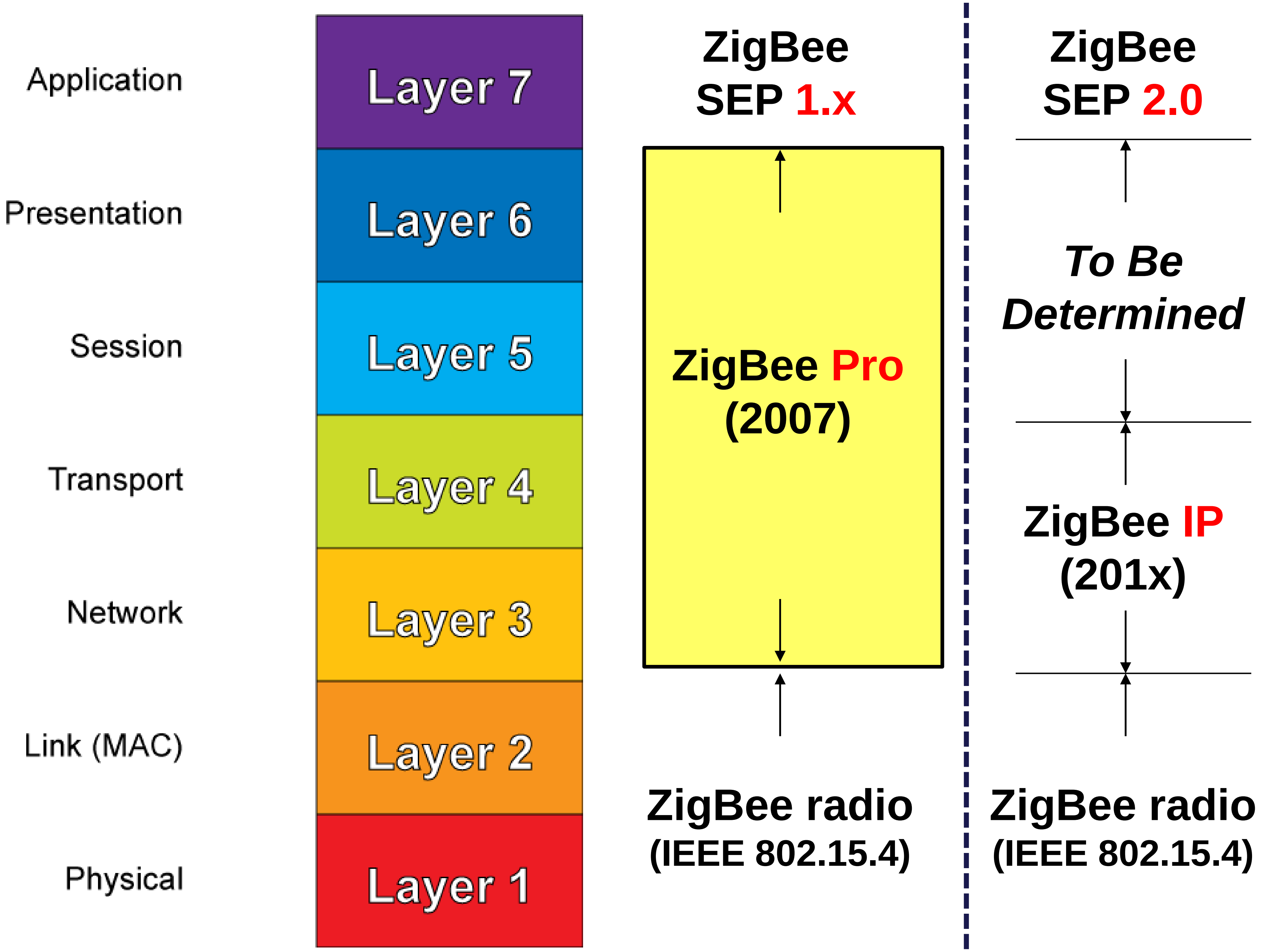
* ZigBee Pro: currently 4th & latest generation not backward compatible with prior versions and will not be compatible with ZigBee IP

Communication Protocols

- ❑ **Communication protocol**: standard rules for sending information over a physical channel
  - ▪ data structure
  - ▪ signal authentication
  - ▪ error detection
- ❑ **OSI* 7-layer model**: a framework for understanding the elements that make up a **communications protocol**

*Open Systems Interconnection Reference Model started in late 1970's.

ZigBee Pro vs. IP and SEP 1.x vs. 2.0



Application — Layer 7

Presentation — Layer 6

Session — Layer 5

Transport — Layer 4

Network — Layer 3

Link (MAC) — Layer 2

Physical — Layer 1

ZigBee SEP 1.x

ZigBee Pro (2007)

ZigBee radio (IEEE 802.15.4)

ZigBee SEP 2.0

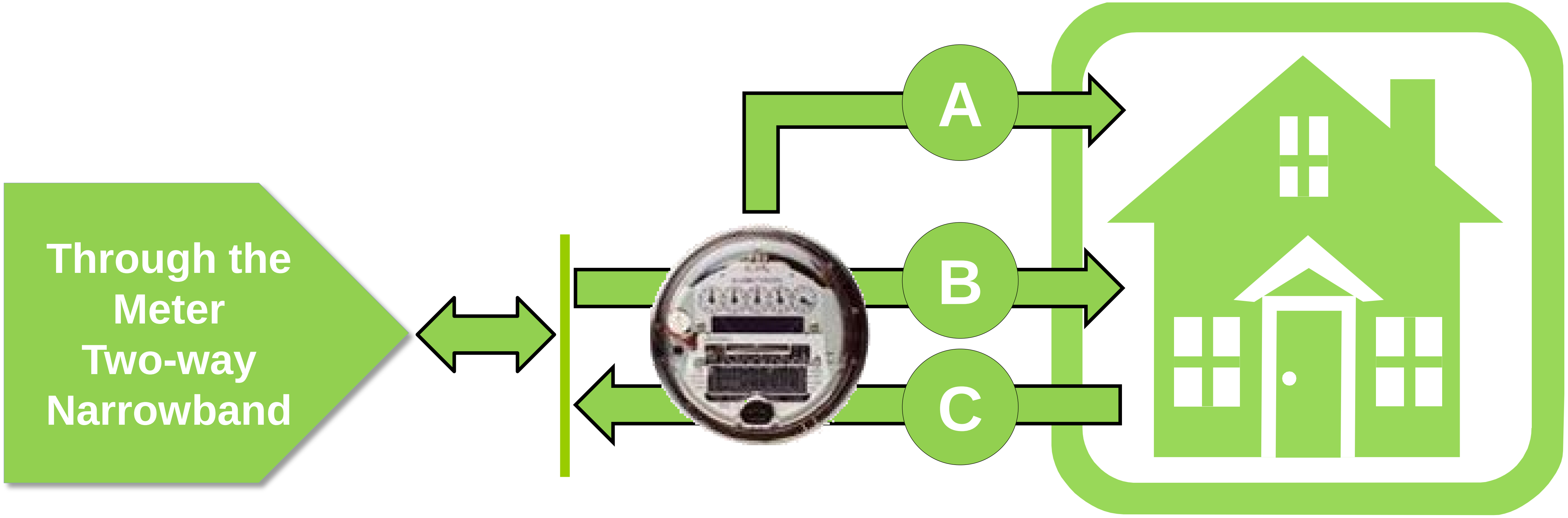
To Be Determined

ZigBee IP (201x)

ZigBee radio (IEEE 802.15.4)

SEP Functionality

	Function	Source	Application
A	Provide real-time meter data (kW, kWh)	Meter	In-home display
B	Provide price, reliability, and event signals	Utility	In-home display; Demand response
C	Retrieve device IDs, settings, event overrides	Consumer devices	Demand response; Tech support



12/18/2012

SEP Problems

	Problems	Consequence
1.	**Security:** Inadequate firewall protection could allow hacker access to the utility meter communication network and utility backend systems.	▪ HAN transceiver in-the-meter not turned on.. ▪ SEP functionality not available. ▪ No IHD support - No access to Near Real-Time meter data or price/cost data. ▪ No DR/Pricing support - No signaling or device information retrieval capability.
2.1	**Device Interoperability:** SEP 1.x consumer devices are not upward compatible with SEP 2.0. SEP 2.0 devices not compatible with SEP 1.x.	▪ SEP 1.x devices in the home may not work if meter HAN firmware upgraded to SEP 2.0. ▪ Customer behavior response to SEP 1.x may or may not be relevant to SEP 2.0.
2.2	**Device Upgradeability:** SEP 1.x upgrade to SEP 2.0 requires: ▪ Sufficient device memory to accommodate SEP 2.0 ▪ Broadband (IP) network within the home to manage upgrade process	▪ SEP 1.x devices in-the-home may become stranded ▪ Need for broadband capability o Requires gateway, e.g. in router o Limits device registration o Questions need for SEP
3.	**SEP 2.0 Uncertainty**: SEP 2.0 is 14 months late and its functionality , completion date, and compatibility with existing meters is uncertain.	▪ Delaying pilot implementation may not be a feasible option. ▪ Committing to SEP 1.x technology may risk utility / consumer investment.

A Provide Real-Time Meter Data

A_1 **Gateway with Limited SEP 1.x Functionality**

ANCI C12 table Access

A_2 **Meter Collar**

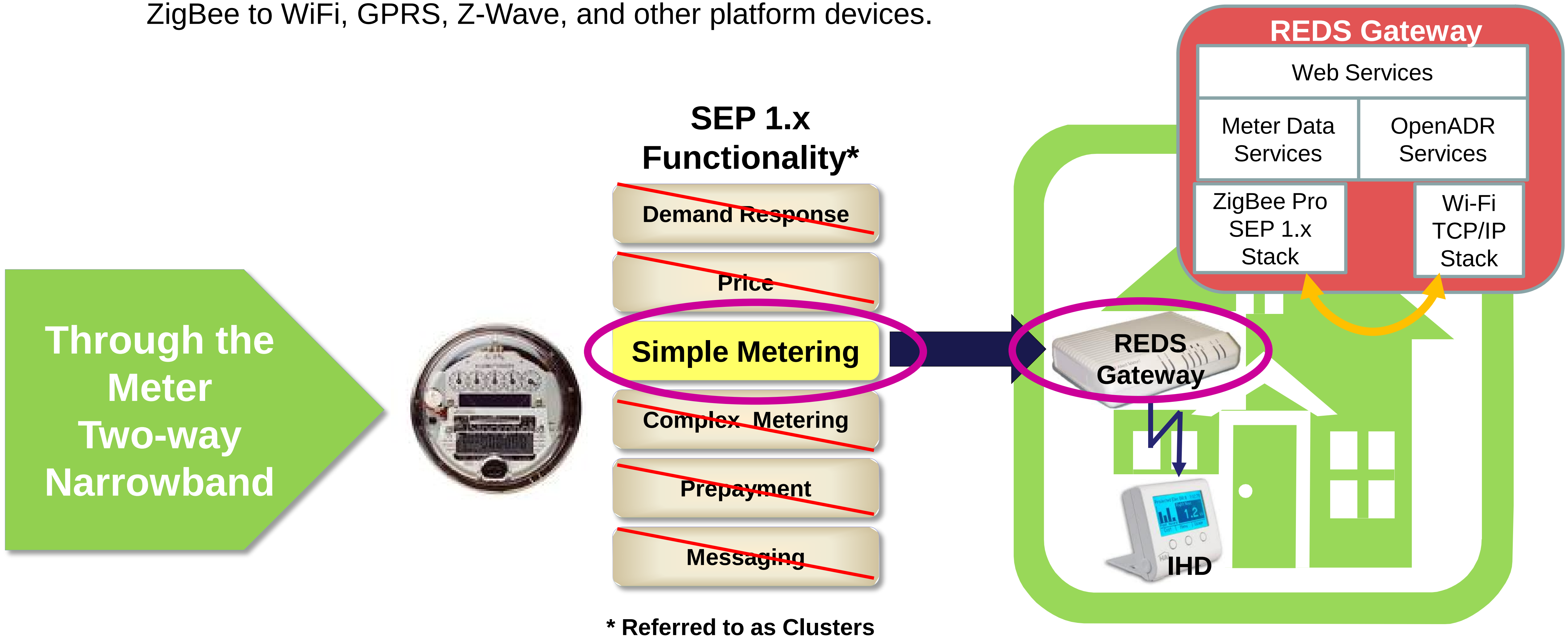
Proprietary products not synched with meter

A_3 **Current Transformer (CTs)**

Installed in main electrical panel

A$_1$ Gateway with Limited SEP 1.x Functionality

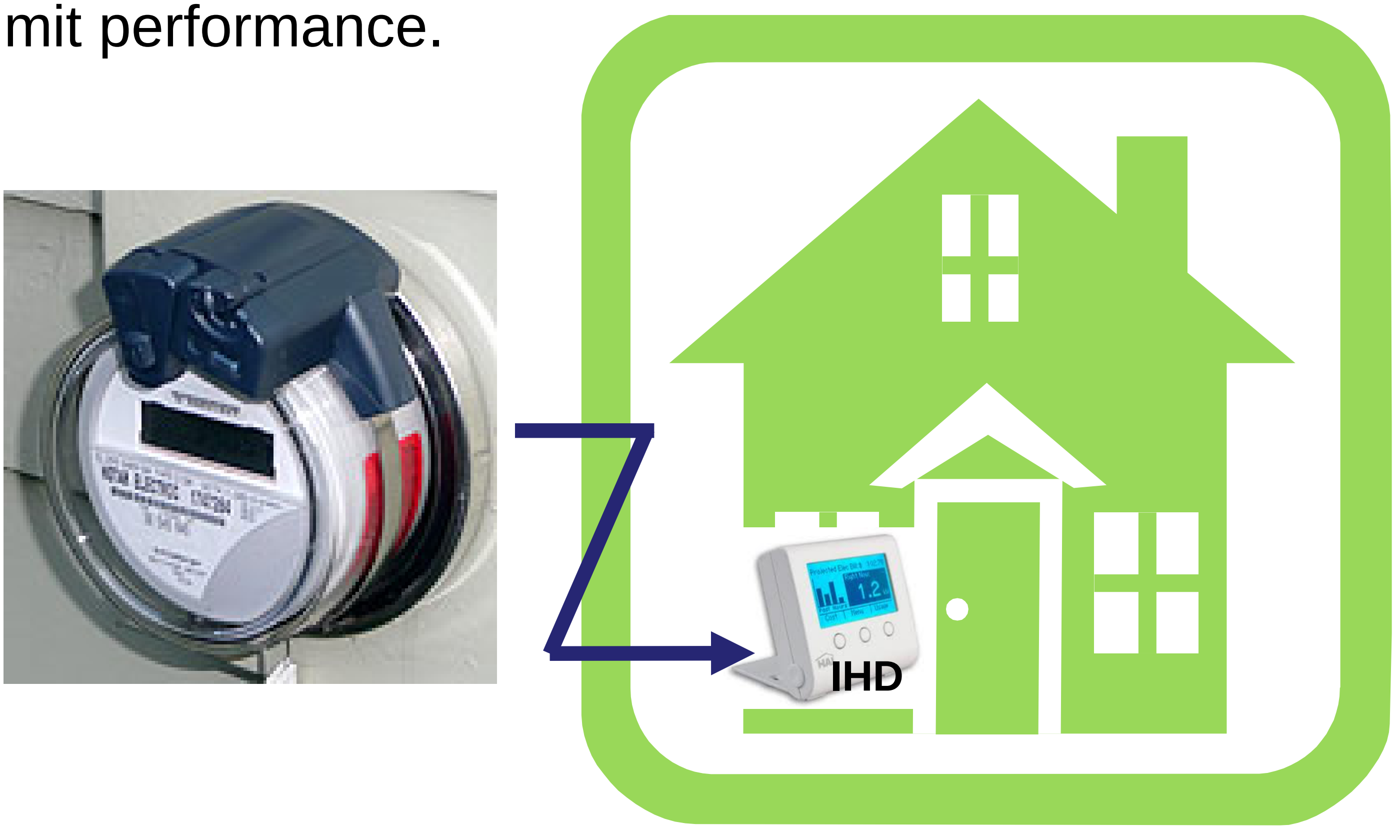
- ❑ **Residential Energy Display Survey (REDS)** project - in development by the Lawrence Berkeley National Laboratory Demand Response Research Center (DRRC) since summer 2010.
- ❑ **Design:** Gateway includes a ZigBee radio (IEEE 802.15.4) with limited subset of the SEP 1.x functions restricted to "Simple Metering", for one-way meter read. Gateway includes additional radios / capabilities to support communication to IHD and other devices.
- ❑ **Purpose:** mitigate security concerns with SEP 1.x and provide a way to open the HAN gateway and provide customer access to near real-time meter data (IHD support).
- ❑ **Gateway**: links the utility-controlled residential HAN and a residential local area network (LAN). Device's includes two protocol stacks (ZigBee Pro and TCP/IP) which provides a bridge from ZigBee to WiFi, GPRS, Z-Wave, and other platform devices.



*** Referred to as Clusters**

A_2 Meter Collar *

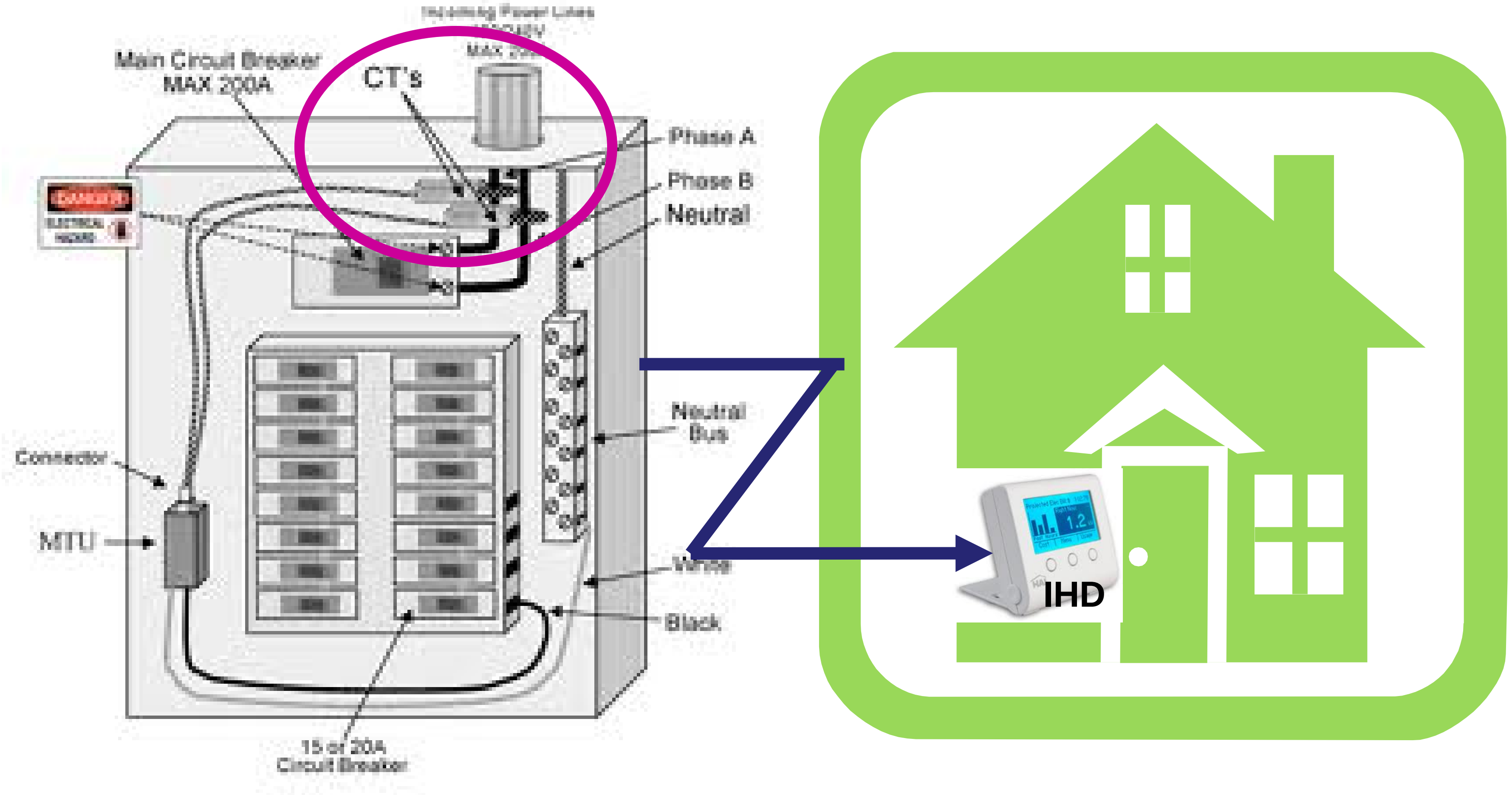
- **Design:** For advanced meters, read from the optical port.
- **Source:** Generally provided by vendors that supply both the collar and IHD.
- **Compatibility:** Collars may or may not be compatible with all meter brands.
- **Operation:** Collars broadcast wireless to display.
- **Limitations**: Operation limited by (1) distance from the collar to the IHD, (2) interference due to proximity to nearby meters also employing collars, (3) meter readings may not align with actual utility readings, and (4) battery life may substantially limit performance.



* Any decision to implement Meter Collars should carefully evaluate battery, wireless transmission, and accuracy performance to assure consistency with project requirements.

A_3 Current Transformer (CT)

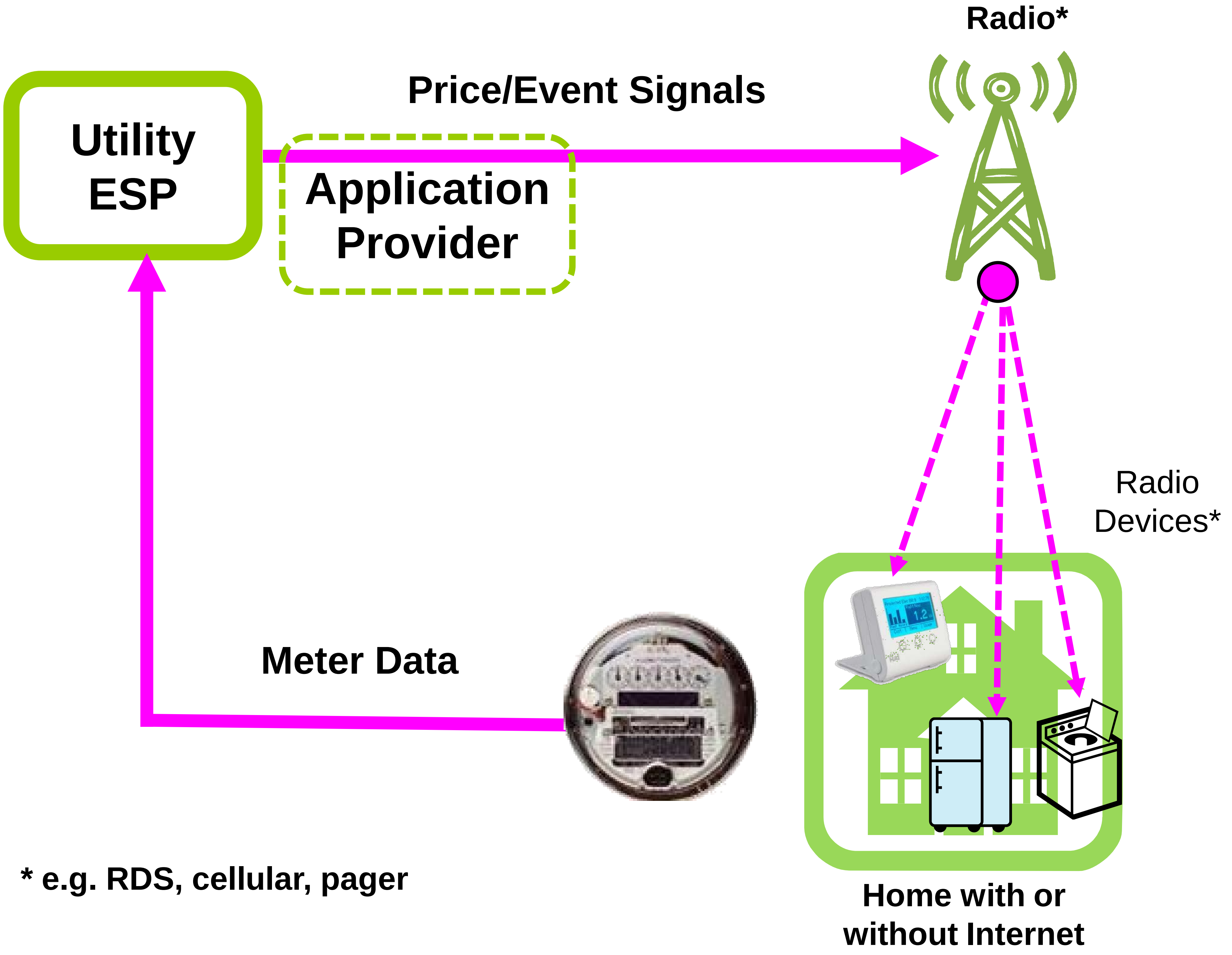
- ❑ **Design:** Current transformer (CT) installed inside the electrical panel – requires electrician.
- ❑ **Source:** Provided by vendors that supply both the CT and IHD.
- ❑ **Compatibility:** May or may not be compatible with all service panels.
- ❑ **Operation:** CT's connect to wireless capability to display.
- ❑ **Limitations**: Connection to IHD limited by wireless connection.



B Provide Price, Reliability, and Event Signals

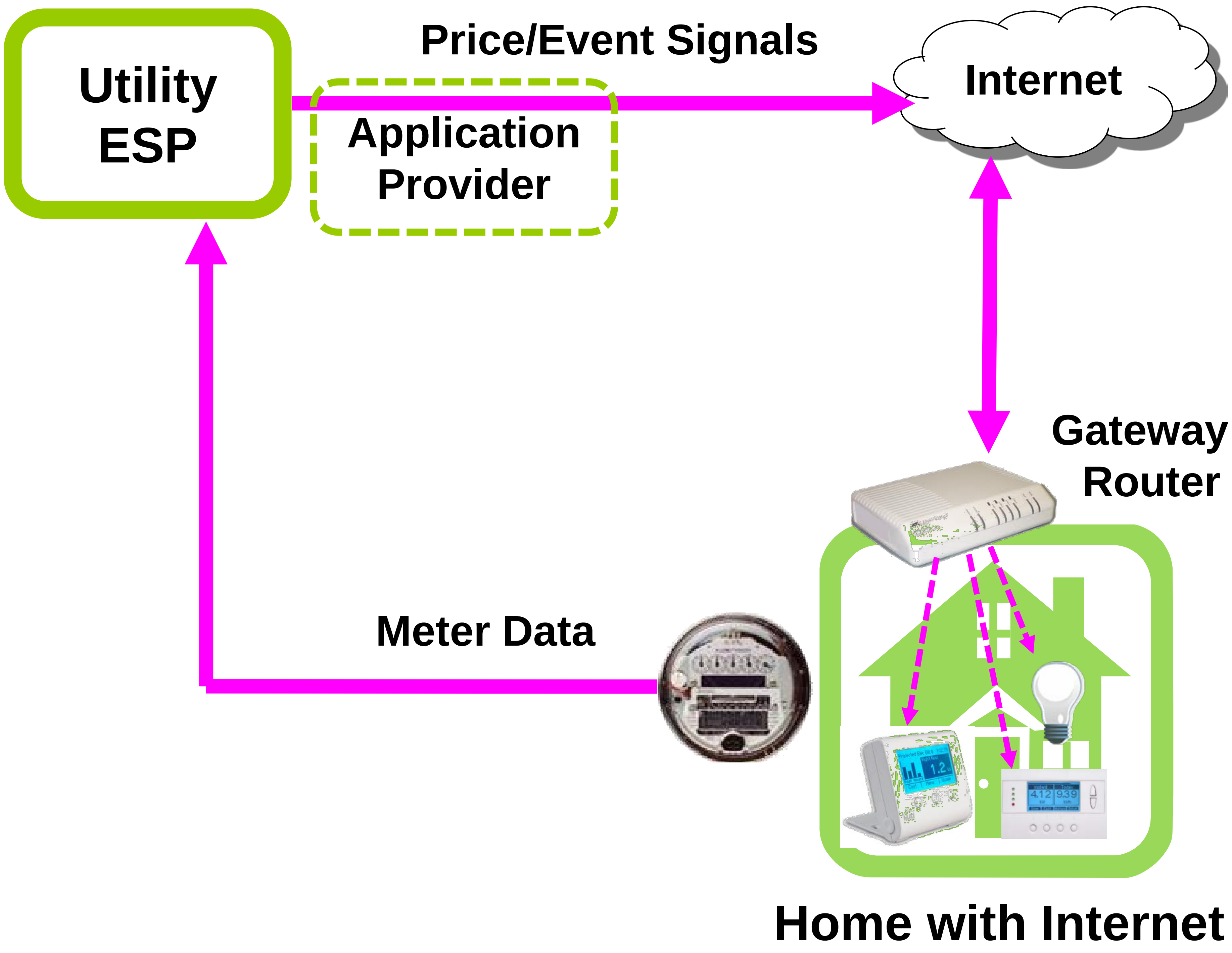
- B_1 Broadcast (Radio)
- B_2 Broadband (Internet)
- B_3 OpenADR: Broadband + Broadcast
- B_4 Packaged Internet-based Systems

B1 Broadcast (Radio) to Home Devices

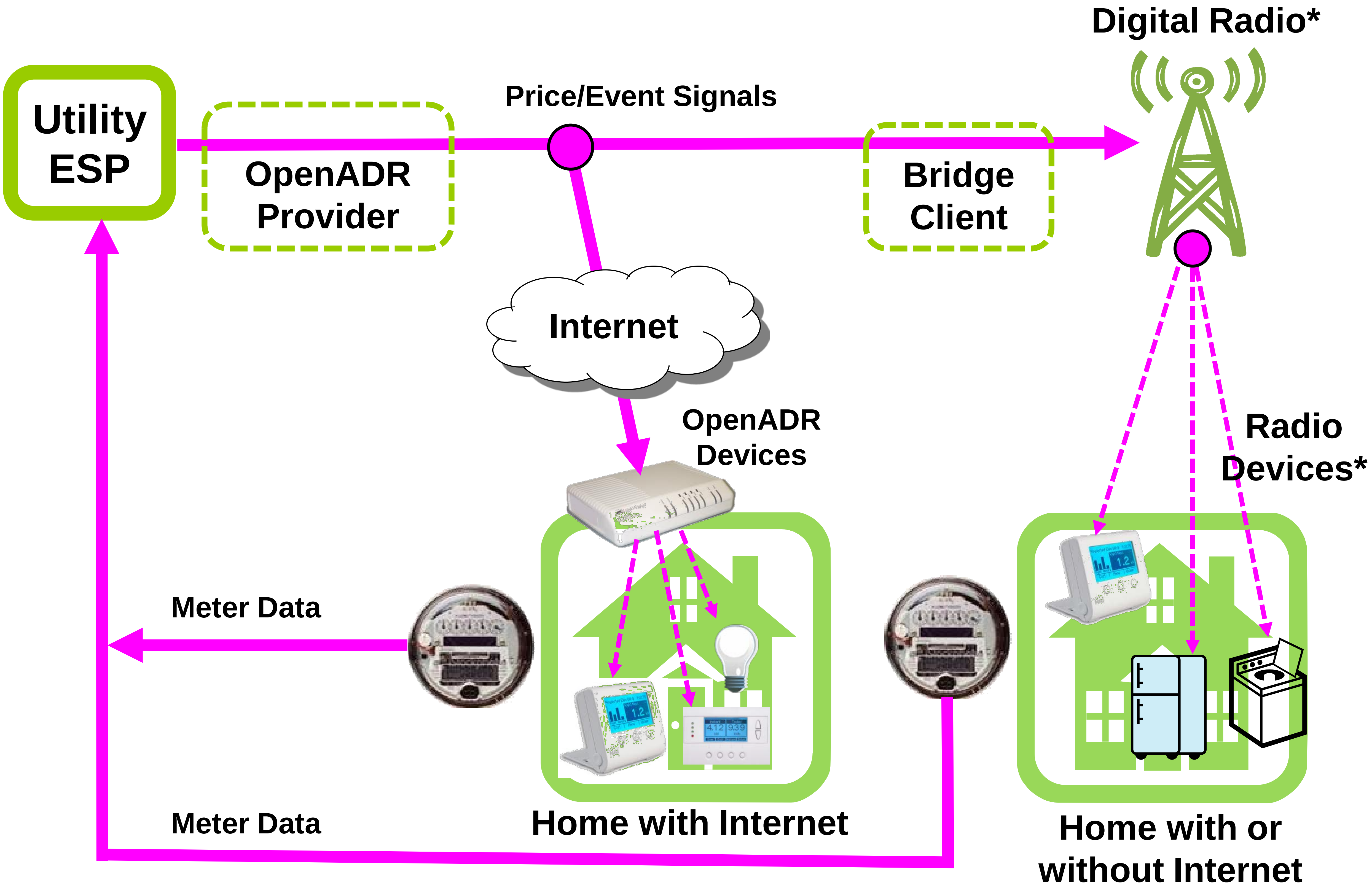


* e.g. RDS, cellular, pager

B_2 Broadband (Internet) to Home Gateway Router



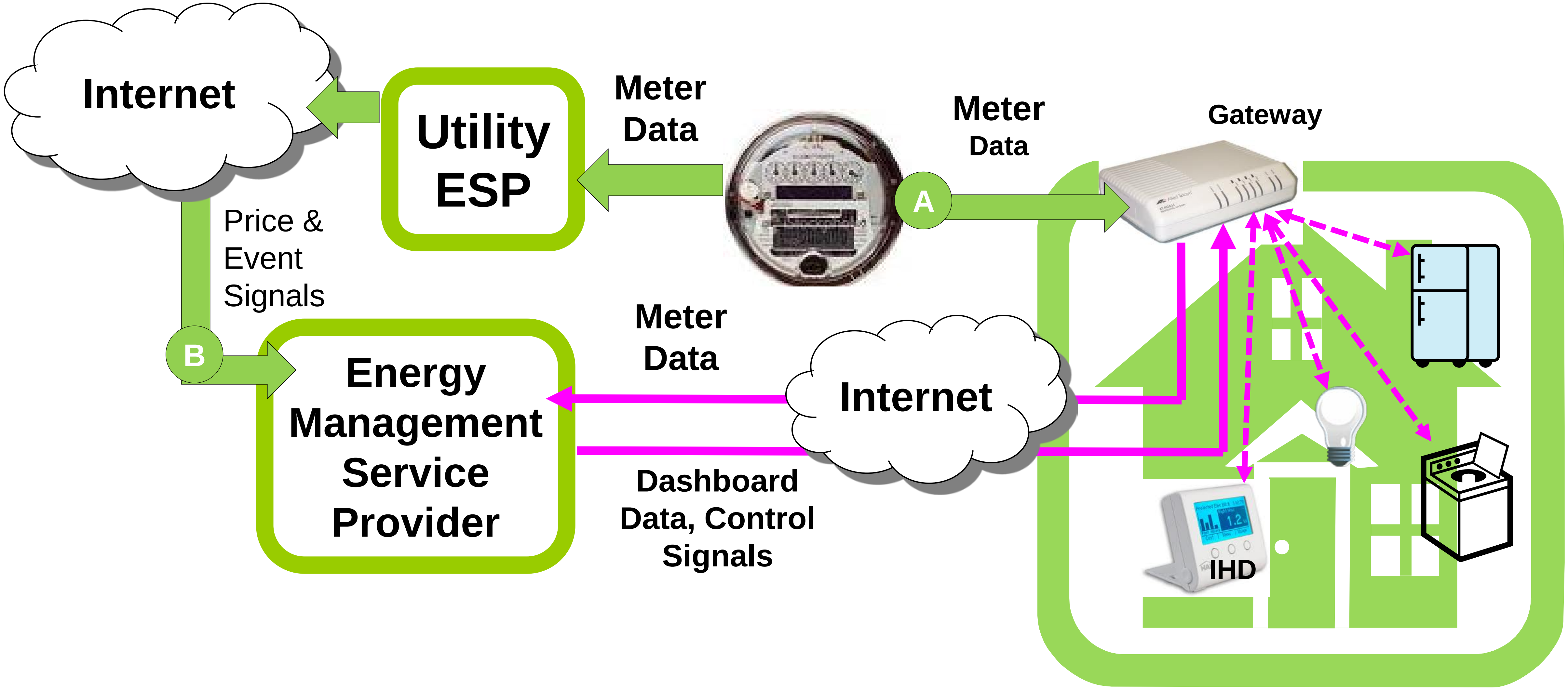
B3 OpenADR: Broadcast + Broadband



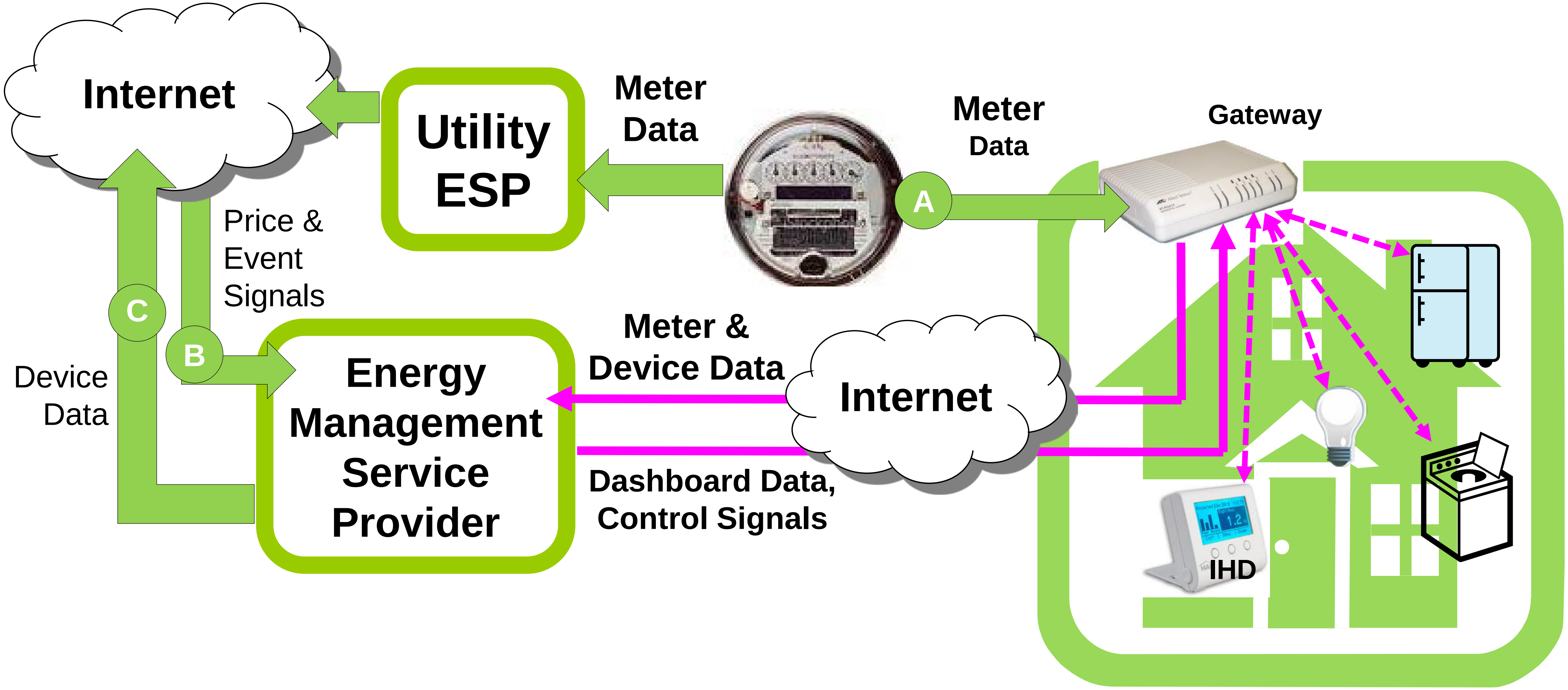
* e.g. RDS, cellular, pager

B4 Packaged Internet-Based Systems

- ❑ **Meter Data:** Sent to a service provider via the Internet, processed, and sent back to the customer.
- ❑ **Price/Event Signals:** Posted by the utility, picked up by the Service provider, combined with meter data, and sent back to the customer.



C Retrieve Device IDs, Settings, Event Overrides



Contact Information

Ron Hofmann

CaRon Energy Strategies

Email: Caron10@aol.com

Phone: 510-547-0375

Roger Levy

Levy Associates

Email: RogerL47@aol.com

Phone: 916-487-8559

Karen Herter

Herter Energy Research Solutions

Email: Karen@HerterEnergy.com

Phone: 916-397-0101

References

Title	
1	Herter, Karen and Seth Wayland. 2008. *Technology Evaluation of Programmable Communicating Thermostats with Radio Broadcast Data System Communications.* California Energy Commission, PIER Energy Systems Integration Program*. http://drrc.lbl.gov/project/technology-evaluation-programmable-communicating-thermostats-radio-broadcast-data-system-com*
2	Herter, Karen, Josh Rasin and Tim Perry. 2009. *Development and Demonstration of the Open Automated Demand Response Standard for the Residential Sector.* California Energy Commission, PIER Buildings End-Use Energy Efficiency Program. http://drrc.lbl.gov/project/development-and-demonstration-openadr-standard-residential-sector
3	Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review, ZigBee Smart Energy Profile Specification 1.0, July 18, 2011. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_SEP_1_0_Review_final.pdf
4	Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review, ZigBee Smart Energy Profile Specification 1.1, July 18, 2011. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGStandards/CSWG_Standards_SEP_1_1_Review_final.pdf
5	OpenADR Communication Standards, http://openadr.lbl.gov/
6	Preliminary Specification for Residential Smart Meter Gateway Device, Lawrence Berkeley National Laboratory, Demand Response Research Center, Spring 2011, http://drrc.lbl.gov/system/files/prelim-han-lan-gateway-spec.pdf