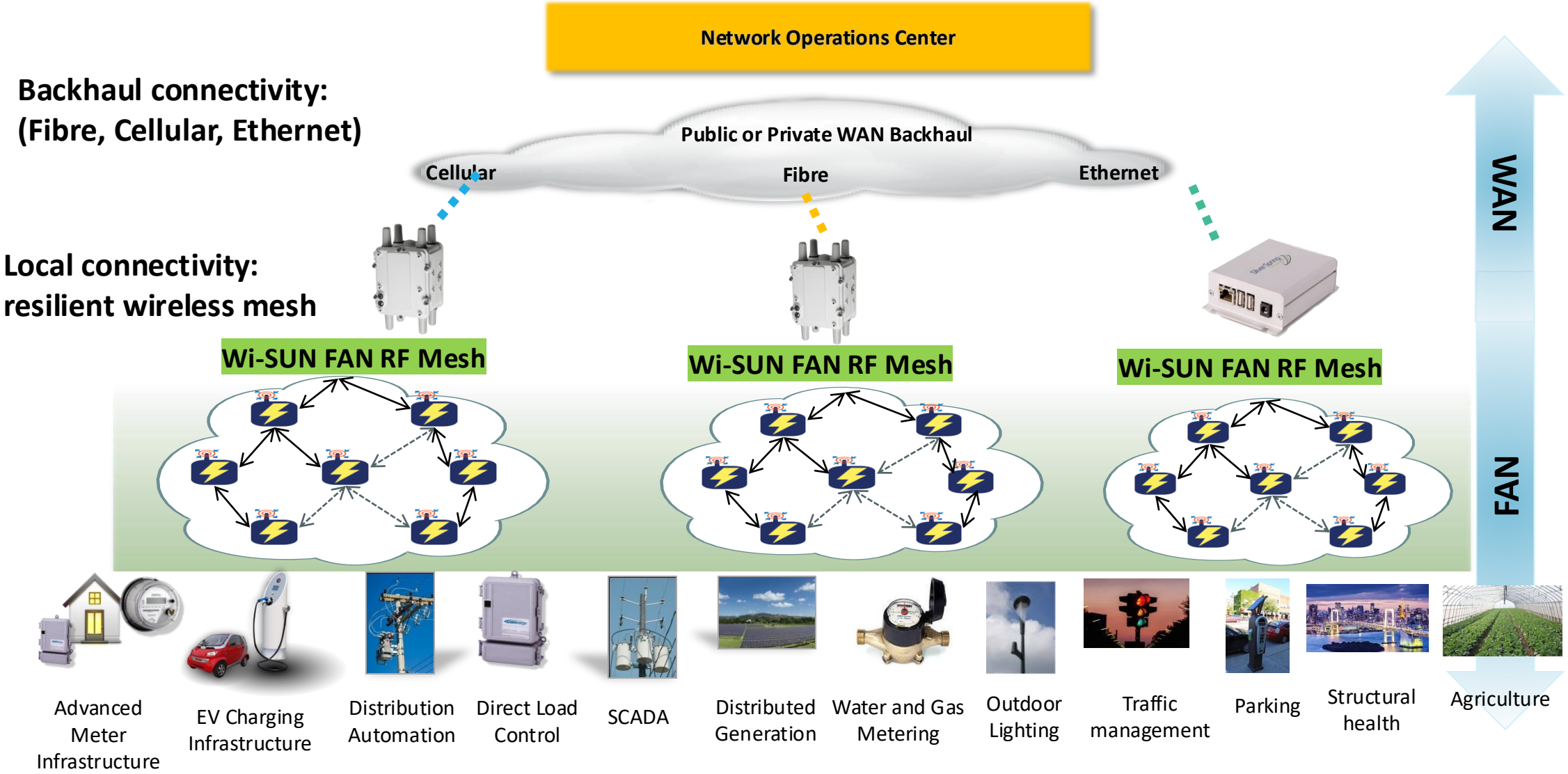
ISUW March 2025
SMART METERING PART B – DISCOMs, AMISPs, OEMs and SIs

Phil Beecher,
President and CEO

AMI Architecture - Wi-SUN FAN
optimized for large scale, critical infrastructure networks



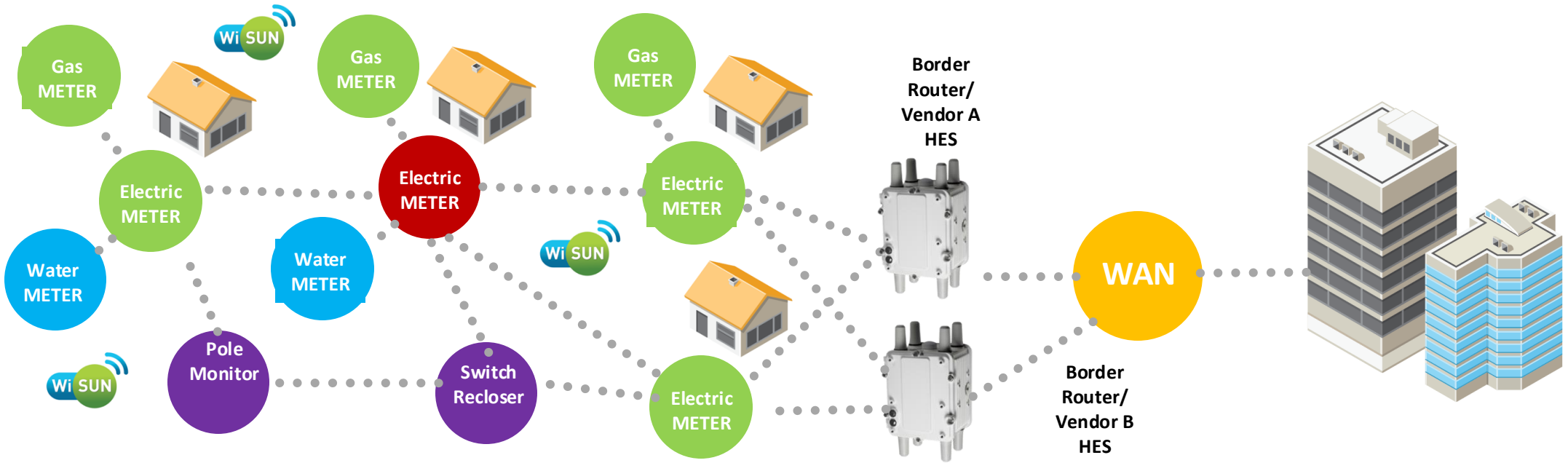
Criteria for meeting Utility SLAs

1. Reliable, resilient communications – works well in adverse conditions, (i.e. geographic, architectural, interference, cyber-attacks)
2. Scalability – how does the network behave with millions of nodes?
3. Low latency data transmission, (point to point and across the network)
4. Fast network recovery after power outage
5. Fault tolerance, detection and self healing
6. Interference mitigation
7. Robust enterprise grade cybersecurity

Cybersecurity measures

1. Certificate-based device authentication – device verification
2. Strong link layer message encryption (AES-128, AES-256), prevents man-in-the-middle attacks, meets privacy requirements.
3. End-to-end application message encryption (support multiple service, including in-meter applications for AMI 2.0
4. Over the air upgrades and firmware signing – allows security updates, and prevents hacker hijacking devices.
5. Robust key management protocol.
6. Interference mitigation (protection against signal jamming)
7. Network traffic anomaly detection - use AI to monitor traffic on the meter / distribution network.

Reliable, Secure, Interoperable Data Interchange



Robust IPv6 Wireless Communications
Wi-SUN FIELD AREA NETWORK (FAN) Profile

- IEEE802.15.4-SUN PHY/MAC, 6LowPAN, and IPv6
- Multi-hop dynamic routing
- Frequency hopping RF
- Fast network recovery
- Message encryption (AES)
- Certificate Based Authentication (X509)
- Standardized as IS18010-4-1 , IEEE Std-2857

Reliable and secure Data Interchange
DLMS / COSEM Standard

- Certificate Based Authentication (X509)
- Specification is standardized by DLMS UA
- Adopted by IEC

Network Management System functionality

Requirements

- Use a standard protocol and Object Model
- Protocol/Object Model must address all of the following:
  - Mutual authentication of devices and networks;
  - Device registration and inventory management (HW and FW revision inventory);
  - Device service discovery;
  - Device configuration management;
  - Device status monitoring;
  - Secure placement of large binary objects (config files, FW, certificates) on devices;
  - IP address management;
  - Time distribution for monitoring and reporting (independent of NTP time distribution for protocol message synchronization)

Candidate Technologies

- LwM2M (OMA)
- CSMP (IETF)

Questions?

धन्यवाद, क्या कोई प्रश्न है?

Phil Beecher
pbeecher@wi-sun.org