Town Hall Innovation Series

broadband forum
Town Hall Innovation Series

Smart Home and IoT

Town Hall Innovation Series

Fall Member Meeting 2024

Smart Home and IoT Town Hall Innovation Series – Agenda

1. Town Hall Introduction & Welcome
   Mauro Tilocca, TIM
2. Smart Home as a Service for Telcos and ISPs
   Eric Smith, Oliver IQ
3. Integrating Next-Generation Quantum Encryption into Smart Home and IoT
   Marco van den Akker, Eight to Seven
4. IoT Large Scale Operations – Use of AI and Analytics
   Colin Grealish, Motive
5. Boosting Your Wi-Fi: Better Connections for Smart Homes
   Ofer Greenberg, Friendly Technologies
6. Secure and Resilient Connectivity for Tomorrow's Smart Cities
   Phil Beecher, WI-SUN
7. Making the Home Smart with FTTR
   Tom Starr, Futurewei Technologies
8. Open Discussion across the Forum: Impact and Conclusions
   John Blackford (BBF Chairman), Mauro Tilocca (Town Hall Innovation Series Co-Chair), Jason Walls (BBF BUS Work Area Co-Director)

Time	Smart home and IoT Town Hall Innovation Series Agenda
8:45	Welcome from Mauro Tilocca
8:50 - 9:20	'Smart Home as a Service for Telcos and ISPs' - Eric Smith, Oliver IQ
9:20 - 9:50	'Integrating Next-Generation Quantum Encryption into Smart Home and IoT' – Marco van den Akker, Eight to Seven
9:50 - 10:20	'IoT Large Scale Operations - Use of AI & Analytics' - Colin Grealish, Motive
10:20 - 10:50	BREAK
10:50 - 11:20	'Boosting Your Wi-Fi: Better Connections for Smart Homes' - Ofer Greenberg, Friendly Technologies
11:20 - 11:50	'Secure and resilient connectivity for tomorrow's smart cities' - Phil Beecher, Wi-SUN
11:50 - 12:20	'Making the home smart with FTTR' - Tom Starr, Futurewei Technologies
12:20 - 13:00	Open Discussion across the forum & Closing

Intelligent Living

OliverIQ™

Who are we? Deep experience in networking and smart home.

Control4™

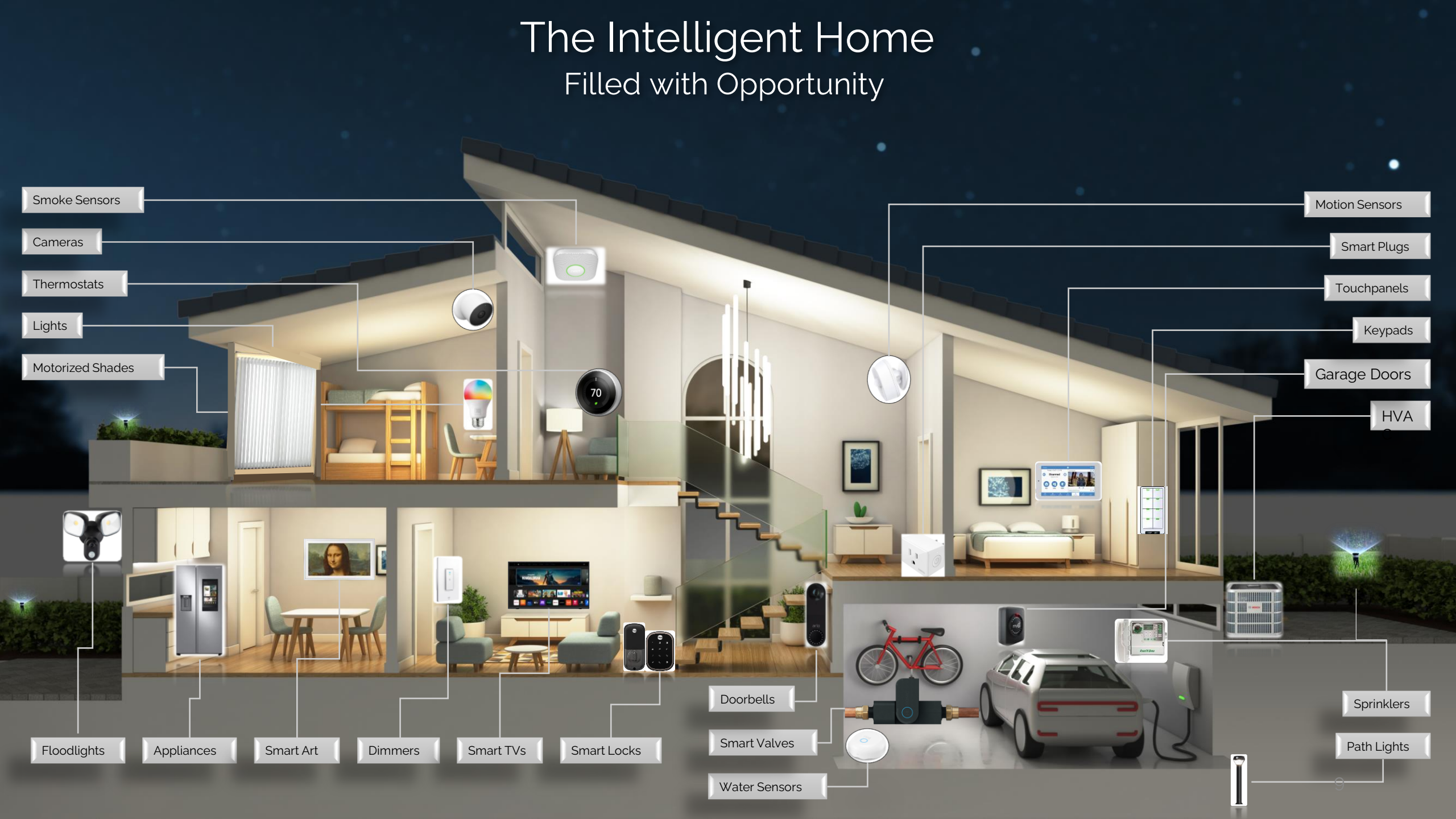
iBAHN®

What is a Smart Home?

Intelligent Living

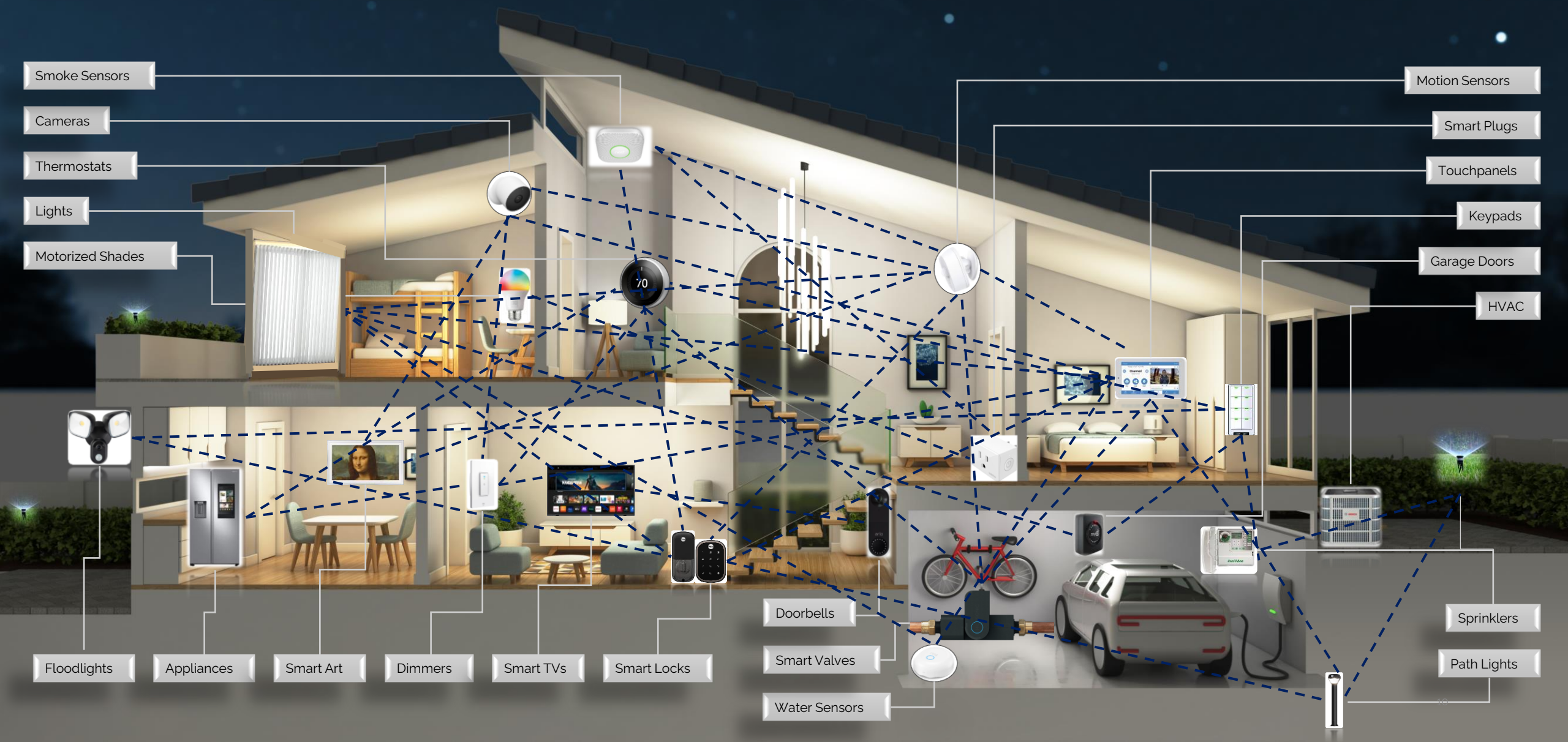
The Intelligent Home

Filled with Opportunity



The Connected Home

Filled with Challenges

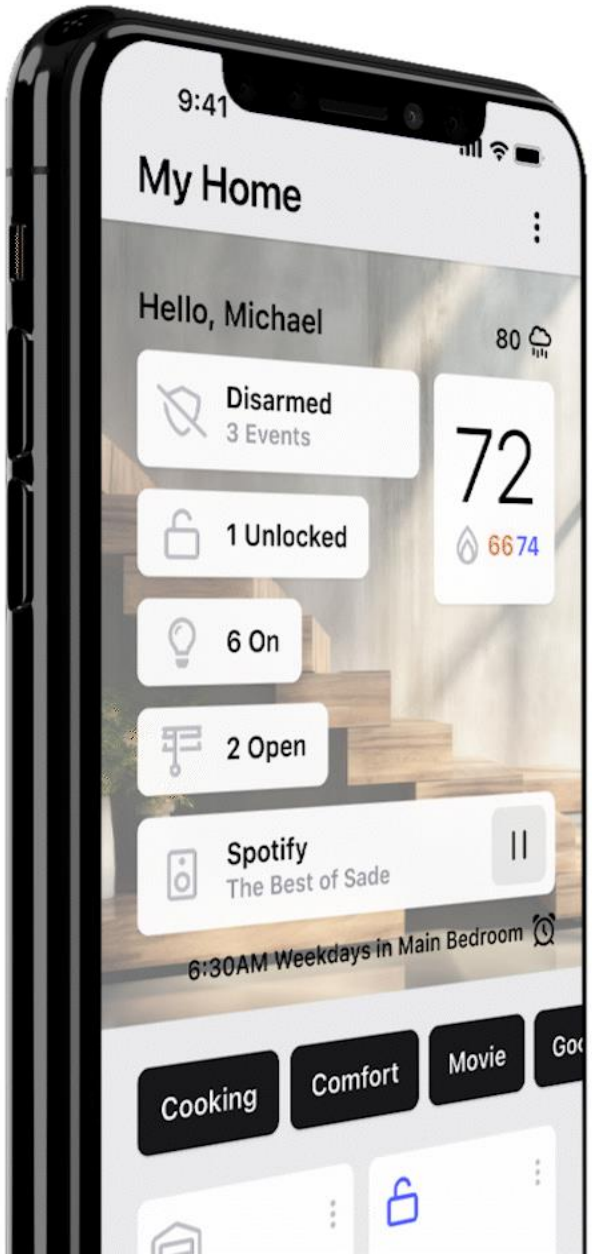


How do consumers get a Smart Home today?

Custom Install Channel

Smart Security Offerings

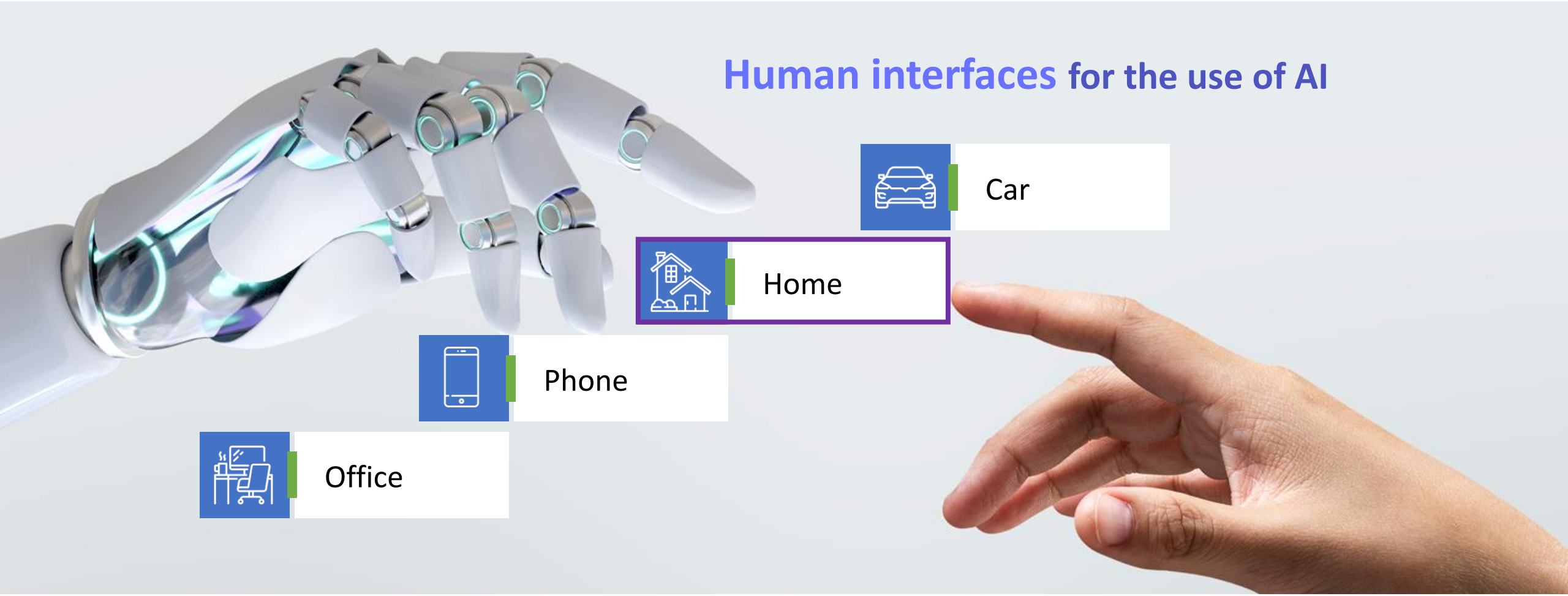
DIY

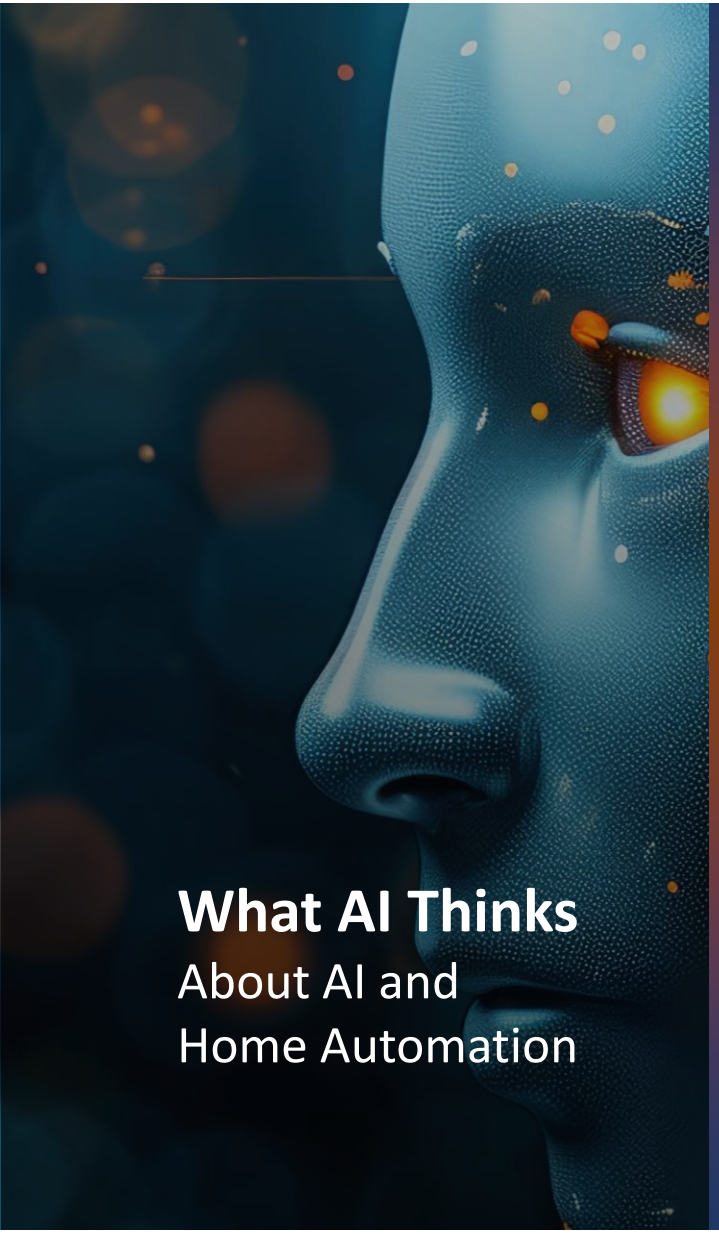


One App to Rule Them All

august
Yale
Roku
ECOLINK
WiZ
nest
alula
Google
LEVITON
Honeywell
ring
SONOS
GENIE ALADDIN CONNECT
HunterDouglas
LUTRON

Home - one of the Most Important UI/UX "devices" of the future





What AI Thinks

About AI and Home Automation

Gemini

Here's my ranking of AI interface importance for consumers in the next decade, along with the reasoning:

1. **Car**: AI is already significantly impacting the automotive industry with advanced driver-assistance systems (ADAS). In the next 10 years, we'll likely see a surge in AI-powered features like:
   - Enhanced Autopilot Systems: Moving towards higher levels of vehicle autonomy, potentially even Level 4 autonomy in certain areas.
   - Personalized In-Car Experiences: AI will curate entertainment, communication, and comfort settings based on individual preferences and driving habits.
   - Predictive Maintenance: AI will analyze vehicle data to anticipate potential issues and recommend proactive maintenance.
2. **Home**: AI is poised to transform our living spaces into truly smart homes. Key areas of impact include:
   - Seamless Automation: AI will optimize lighting, temperature, appliances, and security systems based on learned behaviors and preferences.
   - Personalized Entertainment: AI will power intuitive and interactive entertainment systems that cater to individual tastes.
   - Enhanced Communication: AI-powered assistants will facilitate effortless communication within the home and with the outside world.
3. **Office**: While AI is undoubtedly transforming the workplace, its interface for the average consumer in an office setting might be less direct compared to cars or homes. We'll see AI advancements in:
   - Productivity Tools: AI will assist with scheduling, email management, and task prioritization.
   - Collaboration Platforms: AI will facilitate more efficient and effective teamwork through intelligent meeting summaries and action item tracking.
   - Personalized Learning: AI will provide tailored training and development opportunities for employees.
4. **Other**: This category encompasses a broad range of areas where AI interfaces will play a significant role, such as Wearables, Public Spaces, Retail, etc.

ChatGPT

Here’s a ranking for the importance of AI interfaces for consumers in the next decade:

1. **Home**: As AI technology advances, smart home systems will likely dominate consumer interfaces. From climate control and security to personalized entertainment and health monitoring, AI will become the hub of home management. Consumers will rely on AI to automate and optimize daily tasks, enhance convenience, and even monitor health, making the home the top space for impactful AI use.

2. **Car**: With the growth of autonomous driving and connected car technology, vehicles are becoming mobile smart spaces. AI interfaces in cars will go beyond navigation to offer predictive maintenance, enhanced safety features, personalized in-car experiences, and seamless integration with mobile devices and home systems. This will transform cars into extensions of smart homes and offices, especially as self-driving technology advances.

3. **Office**: AI in the workplace is evolving rapidly, assisting with productivity, decision-making, and collaboration. While tools like AI-driven virtual assistants, data analytics, and real-time language translation are already common, AI will increasingly shape personalized workflows and automation. However, its impact may be more industry-specific and tailored to roles that depend on technology and data.

4. **Other**: This category includes wearable devices, retail experiences, and public spaces. AI interfaces here will focus on health monitoring (e.g., wearables), personalized shopping experiences, and convenience features in public spaces like AI-powered kiosks and automated customer support. Although essential, these interfaces will likely be supplementary to home, car, and office interfaces.

Homes and cars are set to lead in importance because of their potential for deep integration with consumers' daily routines, followed by offices, where AI will enhance productivity and workflows.

Historical Progression of Smart Homes

OliverIQ

Basic Home (Pre-2000s)

- Manual
- No maintenance

Smart Devices (2000s)

- Connected Devices
- Expensive

Smart Systems (2010s)

- Full Integration
- Expensive

AI & Powerful IoT (2020s)

- Affordable Intelligent Device
- Emergence of AI

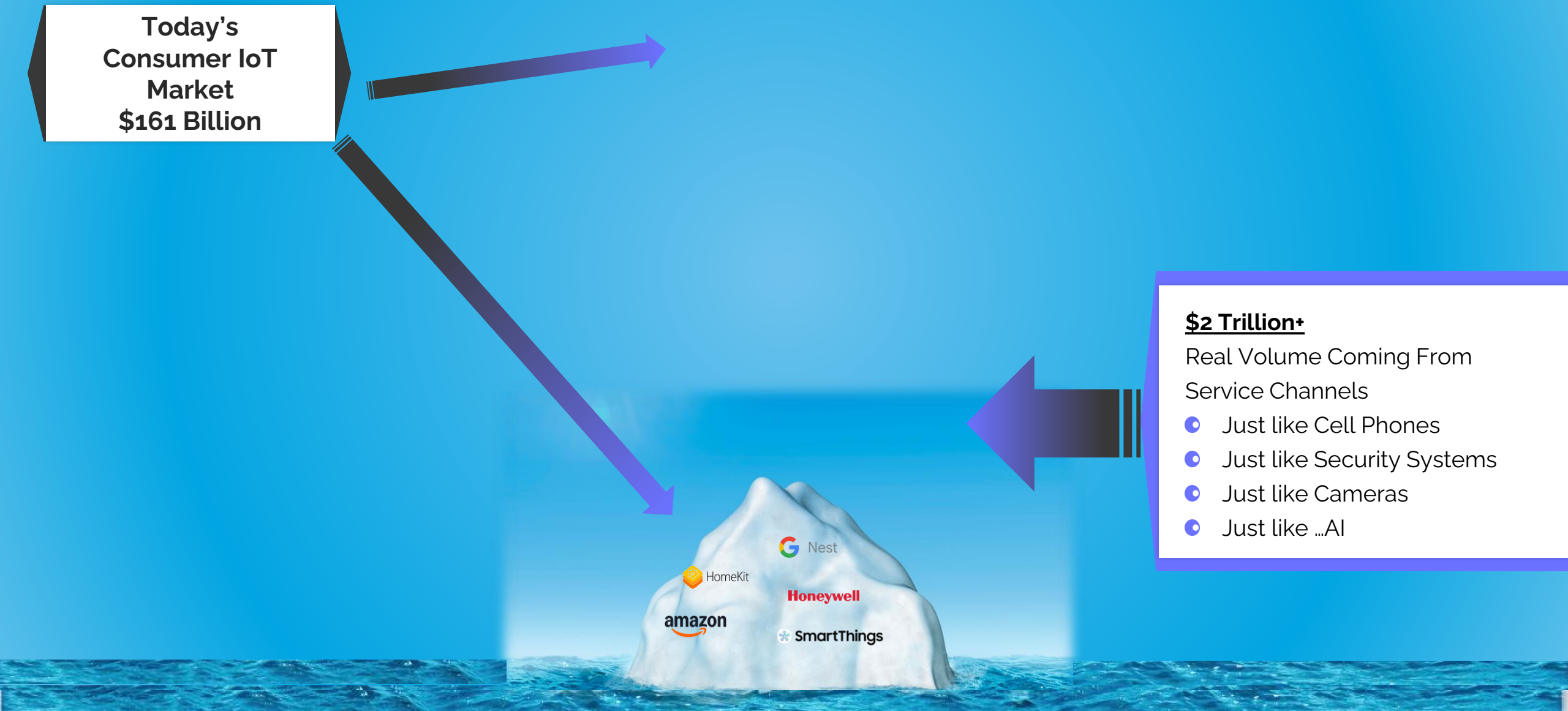
Today's $158 billion market Growing at 28%

Fully Autonomous Smart Homes (Near Future)

- Affordable
- Serviceable
- YOUR Home

OliverIQ

Today's Consumer IoT Market $161 Billion



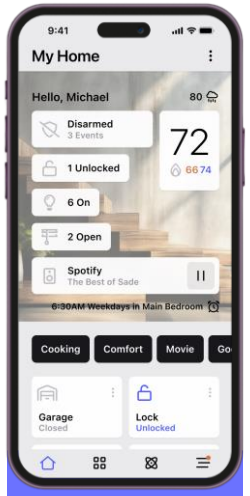
$2 Trillion+

Real Volume Coming From Service Channels

- Just like Cell Phones
- Just like Security Systems
- Just like Cameras
- Just like …AI

Smart Home as a Service subscription

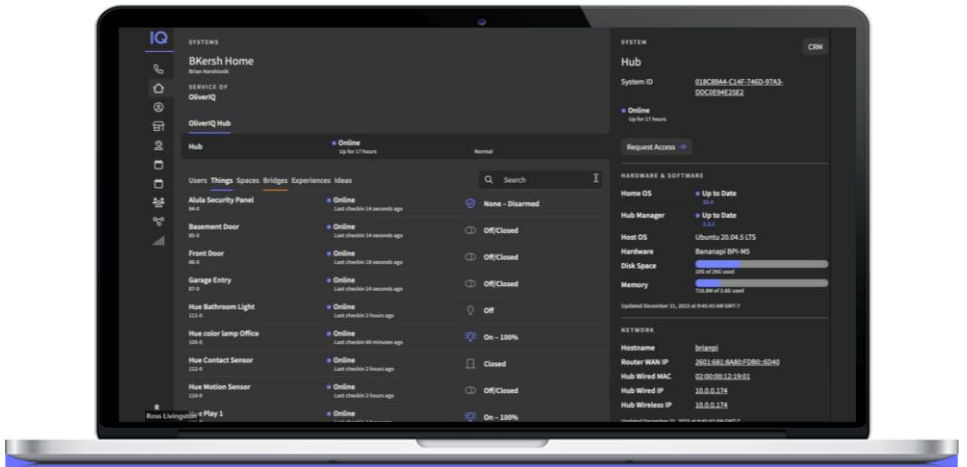
OliverIQ



Best In Class

Every Important Smart Device

Every Communication Platform



Comprehensive Knowledge Base & Support Plus Professional Security Monitoring

Consumer Application

Automation Platform

Backend Support

AI

AI

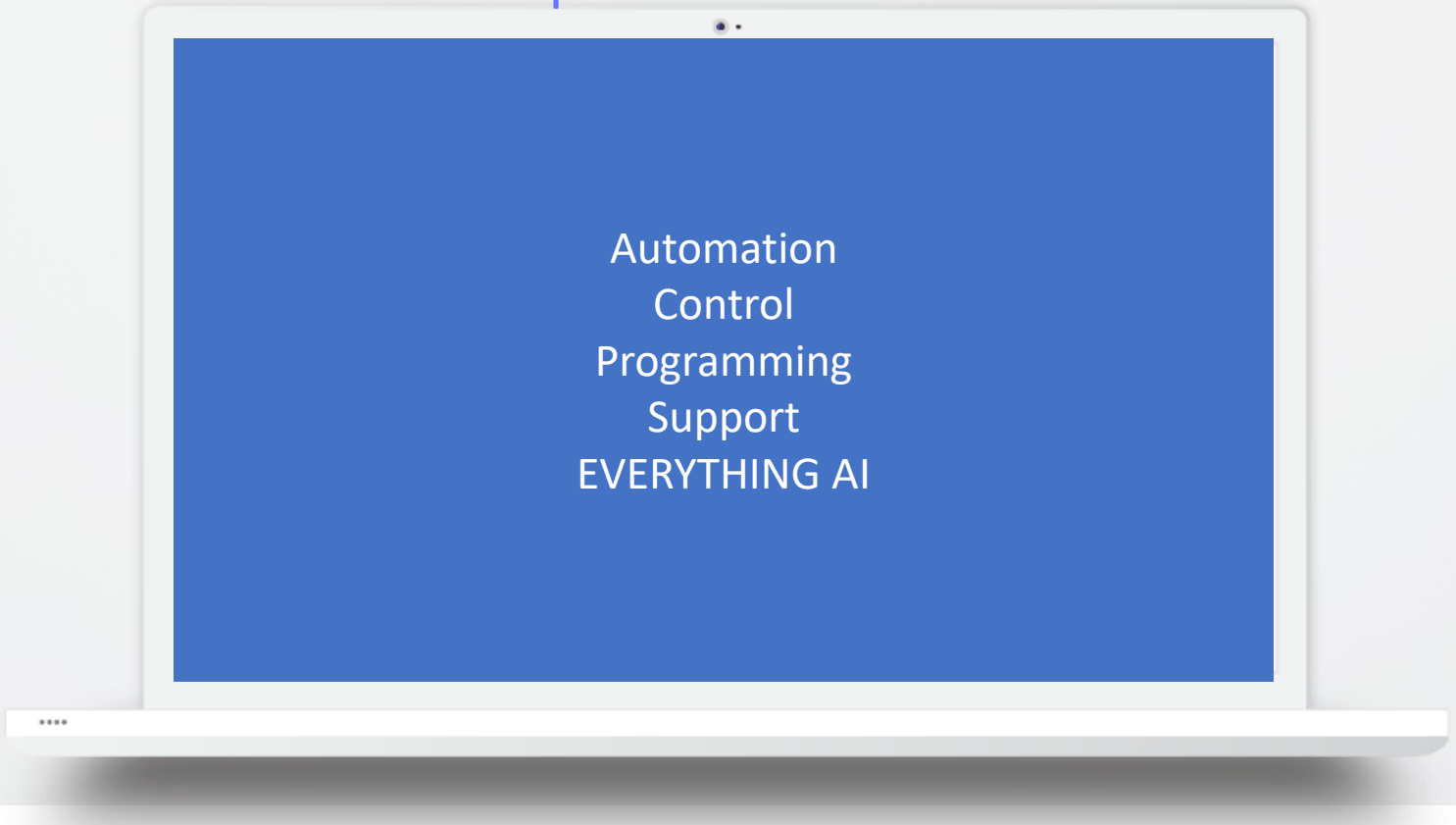
AI

Online Support

Truck Roll Support

The Magic Sauce
AI + Automation + Service

AI is magical in the home … once you know
how to deal with the complication of the Home



Intelligent Living – The Ollie AI

Welcome Home

Flood Prevention

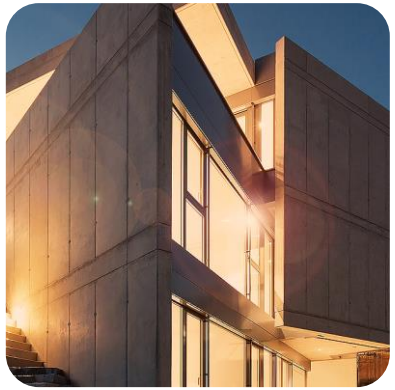
Good Morning

Sunset

home to its fullest

Vacation

Timer



Away

Goodnight

Competition (the elephants in the room)

The consumer needs solutions beyond DIY and ISPs are uniquely positioned and qualified to be the delivery mechanism for the AI enabled Smart Home.

Timing is PERFECT

- Consumers buying IoT at Scale
- Consumers aware of AI at Scale
- Consumers need Support at Scale

Business model

Smart Home Subscription

- Amazon charging for advanced Alexa
- Chamberlain charging for every door
- August is charging for every lock
- High end is forcing subscriptions

Firmware as a Service

- ISP: Routers
- Security: Panels
- Retail: Various
- Builders: Various

Huge volume of related solutions happen via these channels

… Including: Home Services, Home Products, Car Services, …. HUGE

eighttoseven

Welcome to Next-Generation Security for Smart Homes and IoT

broadband forum
Town Hall Innovation Series

Session Topic: Smart Home and IoT

eight*to*seven

8to7, is a Quantum Encryption as a Service solution designed to deliver an effective, speedy, and resilient data protection mechanism that prevents unauthorized access to sensitive information

www.eighttoseven.com

Our Company

eighttoseven

Eight to Seven was founded in 2023, headquartered in Rotterdam, Netherlands

Team of 4 members with a cumulative experience of over 25 years experience

We offer cutting-edge data encryption using a revolutionary 8-to-7-bit encoding method for superior security and compression

Team expertise in security design and architecture, cloud security, AI, risk and incident management, firewalls, IP networking, product management, and business development

IP Asset consists of several patents, related to the areas of data compression and data modeling whereunder GB201915851D0

Our Team

eighttoseven

Marco van den Akker

CEO

Founder member of the Cloud Security Alliance NL; is a seasoned expert on technology. He's renowned for optimizing sales strategies to drive company growth

Ive Bester

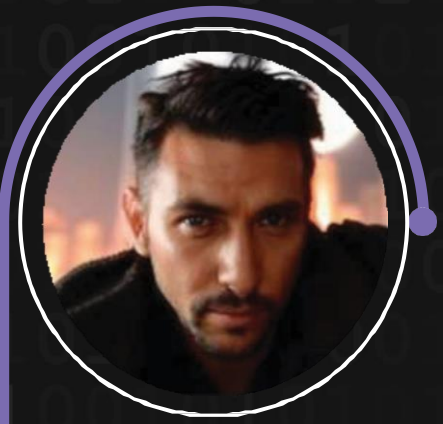
CTO

35 years of experience in IT, specializing in encryption & compression. Senior algorithm developer. Engineer developer of a proprietary algorithm . Matrix code Engineer. Deep data compression developer

Prof. John Fox

Mathematical engineer

He also serves as a lecturer at Far Eastern State Agricultural University, specializing in AI and emerging scientific fields



Coen Smith

Sales & Marketing

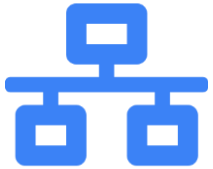
Ex HP, ex IBM, encryption enthusiast engaged in developing advanced Post Quantum Encryption solutions

eight*to*seven

The Need for Enhanced Security in Smart Homes and IoT

broadband forum
Town Hall Innovation Series

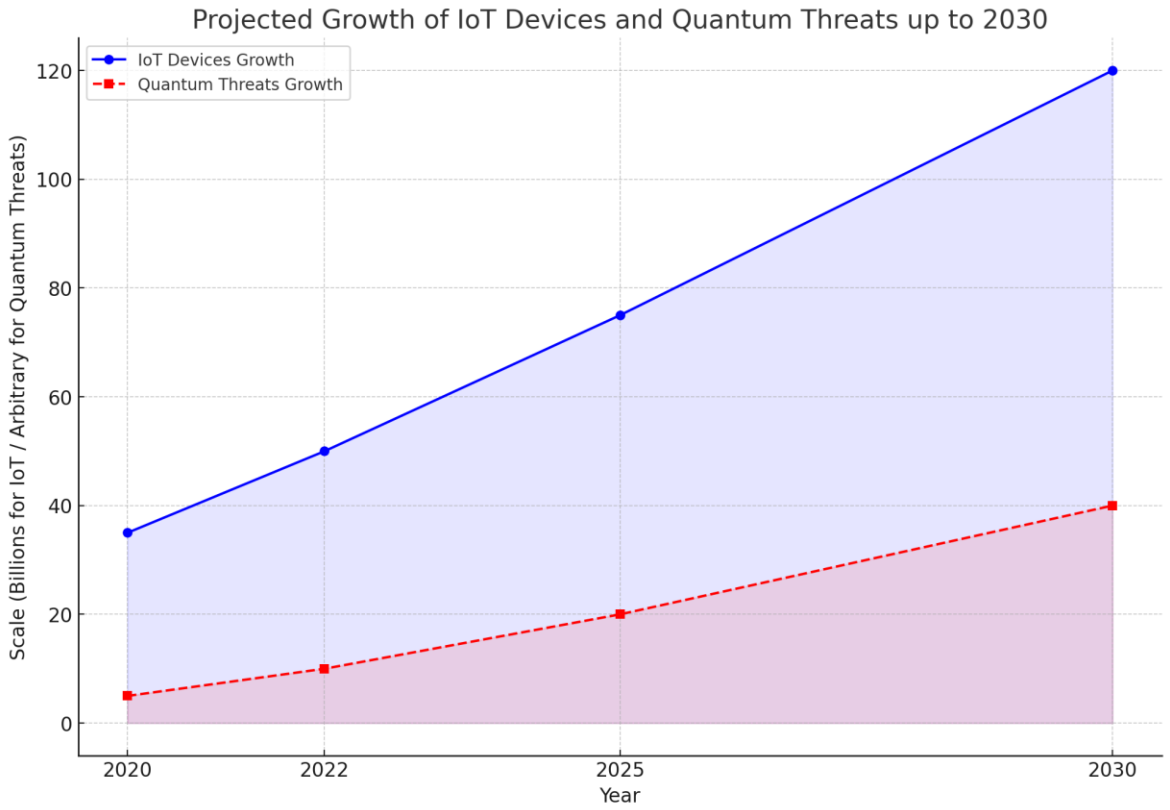
Session Topic: Smart Home and IoT



Overview of IoT Landscape
With over 75 billion connected devices expected by 2025, the need for robust security is paramount.

Introduction to Quantum Threats
As quantum computing advances, traditional encryption methods become increasingly vulnerable.

Eight to Seven's Role
"At Eight to Seven, we provide cutting-edge quantum-resistant encryption solutions designed for any operating system, ensuring your data remains secure."



IoT Devices Growth: IoT connections are set to nearly double, from 15.9 billion in 2023 to over 32.1 billion by 2030, driven by continued technological adoption (Statista). This surge underscores the expanding presence of IoT in daily life.

Quantum Threats: As quantum computing advances, it poses a significant risk to current cryptographic systems. In response, the National Institute of Standards and Technology (NIST) released post-quantum cryptography standards in 2024, signaling a crucial shift toward quantum-resistant security (Deloitte).

Implications: The simultaneous growth of IoT devices and quantum capabilities highlights an urgent need for quantum-safe encryption to protect data across the expanding IoT ecosystem. Transitioning to quantum-resistant measures will be essential to mitigate these emerging threats (World Economic Forum).

The State of Quantum-Resistant Cryptography

broadband forum
Town Hall Innovation Series

Current Adoption and Standards

As quantum computing advances, businesses and organizations are increasingly looking toward quantum-resistant cryptography to protect sensitive data.

A notable milestone is seen in **adoption statistics**, where, as of August 2024, **17.1% of Cloudflare clients have implemented CRYSTALS-Kyber**, a leading quantum-resistant encryption algorithm.

This growing uptake indicates a rising awareness and commitment within the industry to safeguard against future quantum threats.

The State of Quantum-Resistant Cryptography

Meanwhile, **NIST (National Institute of Standards and Technology)** continues to drive standardization efforts in post-quantum cryptography. By collaborating with international experts and industry leaders, NIST aims to establish universal protocols that are effective and widely adoptable.

These efforts ensure that post-quantum cryptographic standards will be both secure and practical across various sectors.

Current Challenges for Wireless Networks

Addressing Security Challenges in 6G and Wi-Fi 7 Networks

The advent of 6G and Wi-Fi 7 brings with it not only technological advancements but also significant security vulnerabilities that must be addressed to protect the increasing number of connected devices and data integrity.

According to MIT research ('Quantum Computing and Post-Quantum Cryptography,' MIT Review, 2023), Quantum computers can break current encryption methods due to their exponential computing power.

Current Challenges for Wireless Networks

Research from the University of Oxford shows that quantum computers can theoretically crack RSA encryption within seconds, indicating vulnerabilities in traditional networks.

The National Institute of Standards and Technology (NIST) highlights the urgent need for quantum-resistant encryption in critical infrastructures, especially due to quantum computing threats.

Current Challenges in IoT Security

The rise of quantum computing presents a serious threat to IoT security by compromising traditional cryptographic methods.

Quantum computers can efficiently break asymmetric encryption algorithms like RSA and ECC, rendering them vulnerable to attacks.

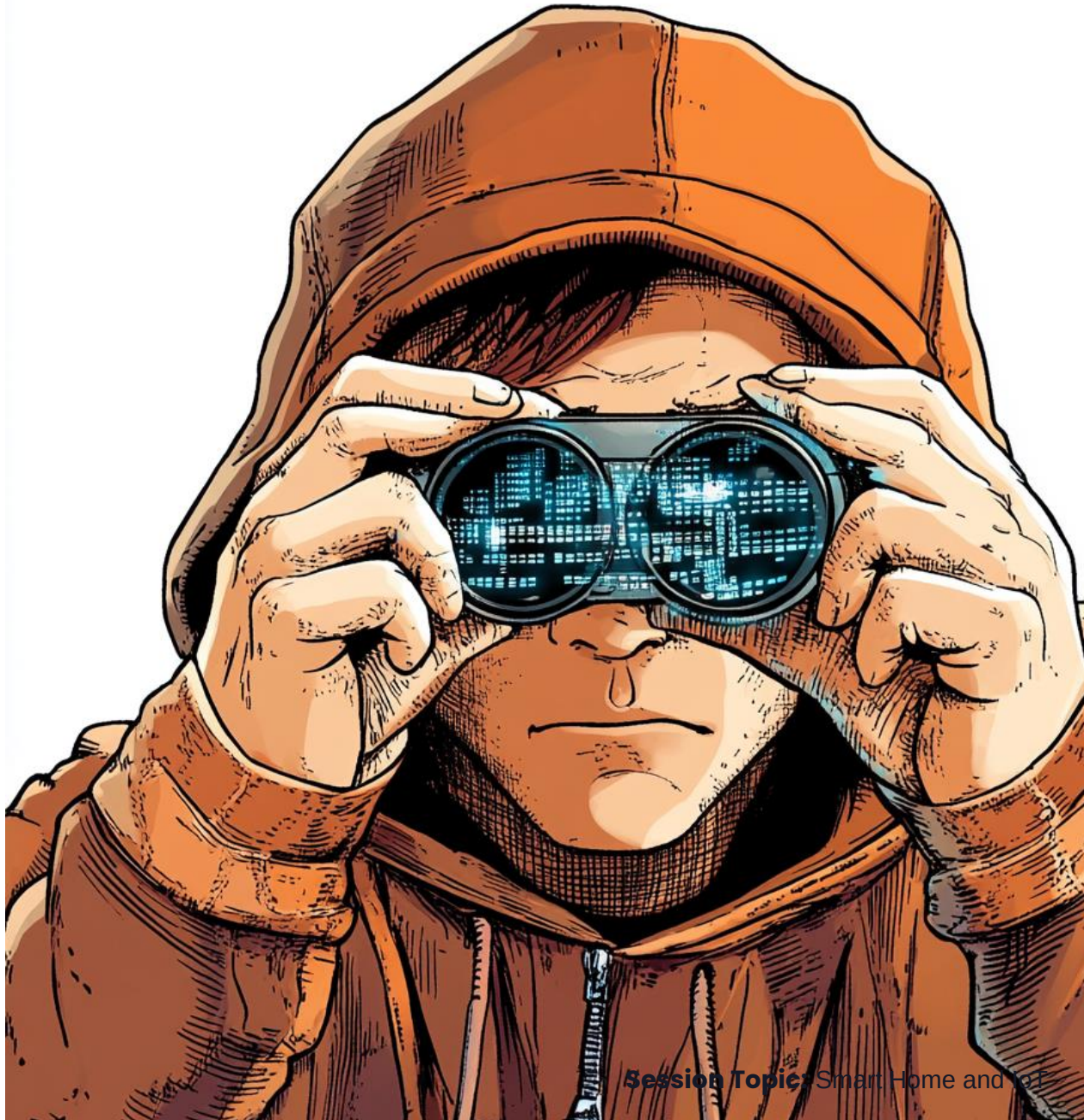
As more devices connect to the Internet, each new IoT device increases the potential attack surface, making it easier for cybercriminals to exploit weaknesses. This highlights the urgent need for quantum-resistant encryption solutions to protect sensitive data in an expanding IoT landscape.

The Quantum Challenge

Vulnerability of Current Encryption
Asymmetric encryption methods (e.g., RSA, ECC) are susceptible to quantum attacks using Shor's algorithm.

Increased Attack Surface
Every connected device introduces potential vulnerabilities; even your smart toaster could be an entry point.

Decryption Risks
Traditional encryption could be compromised, exposing sensitive data to cyber threats.



The Need for Quantum-Resistant Solutions in Smart Homes and IoT

As the number of connected devices is projected to exceed 75 billion by 2025, the importance of robust security measures for IoT ecosystems has never been greater. With quantum computing advancements threatening traditional encryption methods, such as RSA and ECC, there is an urgent need for quantum-resistant solutions.

broadband forum
Town Hall Innovation Series

Session Topic: Smart Home and IoT

The Need for Quantum-Resistant Solutions in Smart Homes and IoT

Protecting Sensitive Data: IoT devices handle vast amounts of personal information, making them prime targets for cyberattacks. Quantum-resistant encryption is essential to safeguard this data from unauthorized access.

Ensuring Long-term Security: The rapid growth of IoT necessitates encryption solutions that can withstand future quantum threats. Transitioning to quantum-safe measures will help maintain the integrity of IoT systems over time.

Addressing Resource Constraints: Many IoT devices have limited processing power and energy resources. Effective quantum-resistant solutions must be efficient and lightweight to implement them without compromising device performance.

Key Considerations for Quantum-Resistant Encryption in IoT

To secure the future of smart homes and IoT, adopting quantum-resistant encryption is critical. This shift will protect sensitive data, ensure long-term security, and accommodate the resource constraints inherent in many IoT devices.

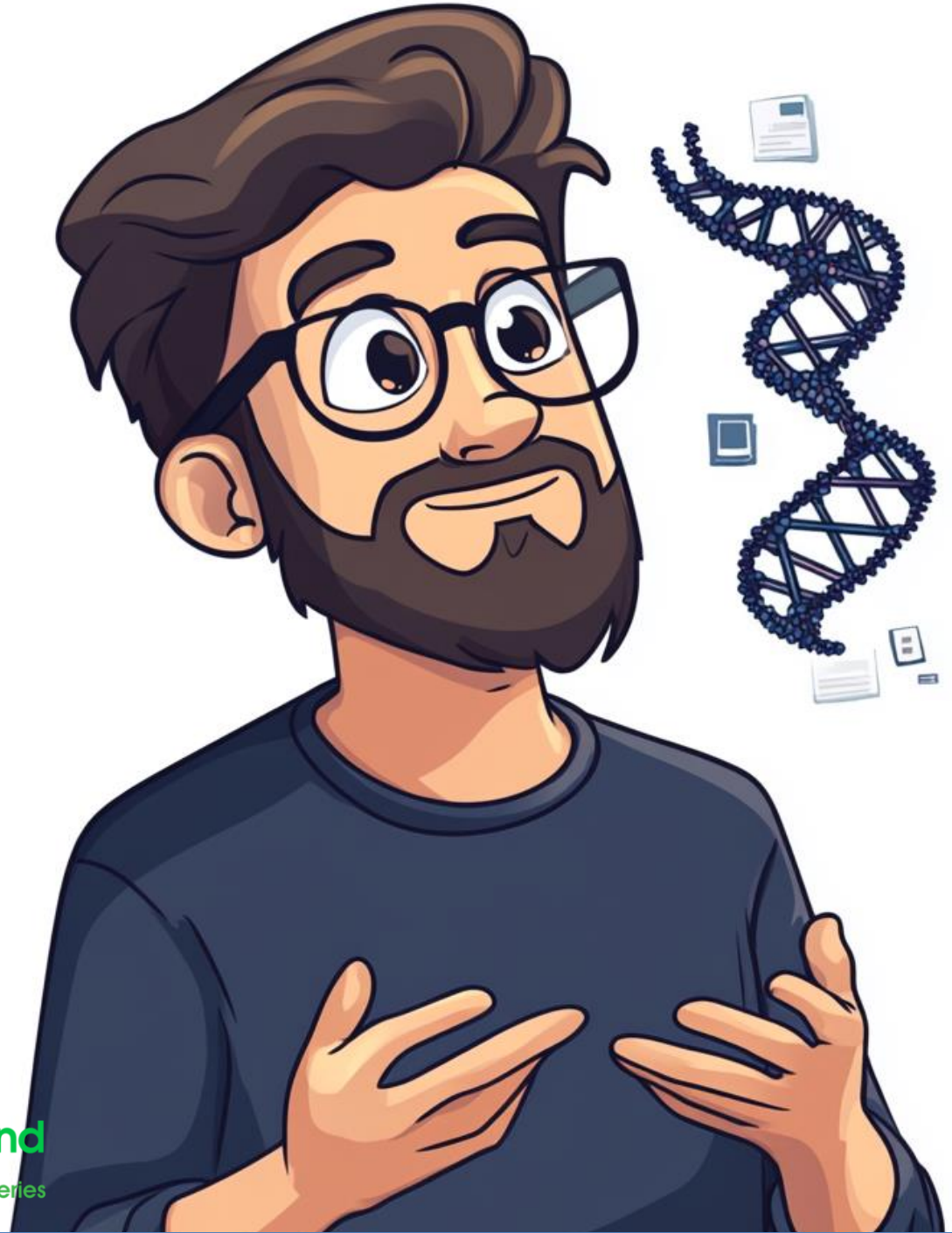
Also, it needs to minimize the overhead of energy consumption while protecting the users against this kind of thread.

Prepared for the future.

In the **rapidly** evolving landscape of Internet of Things (IoT) technology, three key factors are crucial for the successful implementation of security solutions: efficiency, scalability, and interoperability. Let's explore how these elements are addressed in modern quantum-resistant encryption solutions.

1. **Efficiency**
2. **Scalability**
3. **Interoperability**

broadband forum
Town Hall Innovation Series



Efficiency

Efficiency in IoT security is paramount, given the limited processing power of many devices. Advanced encryption algorithms have been developed to minimize computational overhead.

PQCS solutions use only 4-7% of CPU capacity, significantly improving over traditional methods.

This efficiency translates to 53% faster encryption and decryption processes, which is critical for real-time data protection. Moreover, the reduced computational demands lead to lower energy consumption, a crucial factor for battery-operated IoT devices that must operate for extended periods without recharging.

Scalability

Scalability is essential in the diverse IoT ecosystem, which encompasses a wide range of devices with varying capabilities. Modern encryption solutions are designed to adapt to this diversity, functioning effectively on both high-powered systems and low-processing devices. This flexibility allows for seamless implementation across different network architectures, from simple smart home setups to complex industrial IoT environments. As the IoT landscape continues to grow, with projections reaching 32.1 billion connections by 2030, scalable security solutions ensure that protection can keep pace with this expansion.

Interoperability

Interoperability is the third pillar of effective IoT security. New encryption solutions are engineered to be compatible with existing network infrastructure, requiring minimal adjustments for implementation.

This compatibility is crucial for widespread adoption and ease of integration. Importantly, these solutions have a negligible impact on network performance, with less than 5% effect on speeds.

This ensures that security measures don't compromise the functionality of IoT applications across various sectors, including smart homes, healthcare, and industrial IoT.

Minimizing Overhead

Furthermore, the forward-looking design ensures that these security solutions are prepared to work with emerging technologies like 6G and Wi-Fi 7, future-proofing IoT networks against evolving threats and technological advancements.

By addressing efficiency, scalability, and interoperability, modern quantum-resistant encryption solutions are paving the way for a more secure and robust IoT ecosystem, capable of meeting both current and future security challenges.

Future Considerations for Enhanced Security

Leveraging 6G and Wi-Fi 7 Technologies

Increased Bandwidth: Utilize Wi-Fi 7's 320MHz bandwidth and 4K-QAM modulation for faster encryption processes.

Lower Latency: Enhance real-time security measures, ensuring seamless connectivity for IoT devices.

Proactive Threat Detection Using AIAI-Driven Security: Implement advanced algorithms to anticipate and mitigate potential threats before they impact users.

Training Resources: Develop comprehensive guides and training sessions for ISPs and end-users on quantum-resistant encryption. Learn the importance of security in smart home environments to foster user engagement and compliance.

The Road Ahead

As quantum computing advances, the need for quantum-resistant encryption grows urgent. Eight to Seven stands ready to secure the future of IoT, offering a solution that's not just theoretically secure, but practical and efficient.

Together, we could update TR-069 and USP specifications to incorporate quantum-resistant encryption protocols. This integration is crucial as the industry shifts towards protecting data against quantum threats.

By leveraging molecular-genetic encryption technology, we can provide insights into developing robust standards that ensure data security across all connected devices.

Enhancing Device Management Standards

With extensive expertise in security design and architecture, we could together come to a design which can contribute to improving device management aspects of TR-069 and USP. This includes defining secure methods for firmware updates and configuration changes that utilize quantum-resistant encryption.

Establishing guidelines for secure remote management of IoT devices will help service providers maintain the integrity of their networks while ensuring compliance with emerging security standards.

New Working Texts for Quantum-Safe Architectures

The Broadband Forum audience could create new working texts that outline quantum-safe home network architectures. These texts would provide a framework for implementing security measures that protect against both current and future threats.

The focus would be on ensuring that these architectures are scalable and adaptable to various IoT devices, accommodating the expected growth of connected devices.

Creating Quantum-Resistant Libraries

Together as group we can lead initiatives to develop (open-source) libraries for quantum-resistant encryption, making these resources accessible to developers and manufacturers in the IoT space.

By fostering collaboration within the Broadband Forum, these libraries can be integrated into existing products, enhancing overall security while promoting innovation in the field.

eighttoseven

Thank you very much for your attention.

Contact us at

Eight to Seven | Naveol
The Netherlands

info@eighttoseven.com

broadband forum
Town Hall Innovation Series

broadband forum
Town Hall Innovation Series

BREAK

Session starts at 10:45 PST

Town Hall Innovation Series

Fall Member Meeting 2024

Town Hall Innovation Series

Making Smart Home Wi-Fi Smarter: Overcoming Challenges with AI and DMP

Ofer Greenberg
VP, Friendly Technologies

broadband forum

vBASe

friendly technologies | The IoT & device management company

Friendly Technologies at a Glance

Software company
founded in

1997

Device Management Pioneer

Providing Unified Device Management
solutions around the world

Device Management
since

2006

Active Member

of Broadband Forum
& Open Mobile Alliance

Customers
worldwide

300+

The Most Friendly

Trusted by and Installed at
Tier 1, 2 & 3 Carriers and corporates

The Evolution of Smart Home Connectivity

Smart homes are transforming how we live, with **managed Wi-Fi** serving as the backbone that keeps everything connected and running smoothly.

As smart home devices increase, there's a **rising demand** for Wi-Fi that can handle a more **complex, dynamic** environment.

The Evolution of Smart Home Connectivity

Managed WiFi solutions are at the heart of the smart home, ensuring a stable, fast, and reliable network that keeps all devices running smoothly

AI and a **Unified Device Management Platform** (i.e. Friendly Unified Device Management) can enhance smart home Wi-Fi for a **more reliable and smarter** experience.

The Roadblocks of Managed Wi-Fi

- Network Congestion
- Security Risks
- Scalability
- Customer Experience and Support

Traditional = Reactive

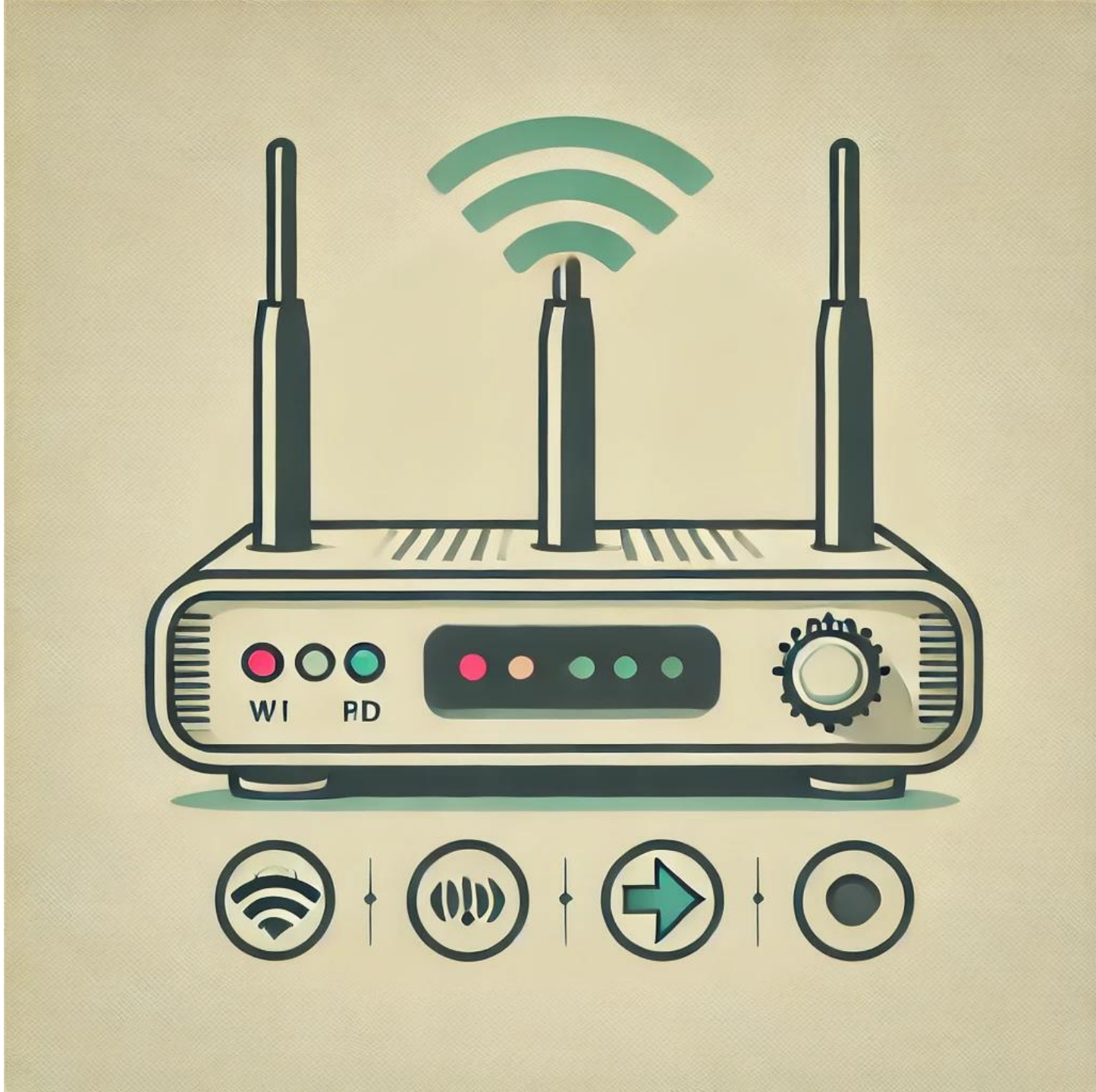
Troubleshoot basic connectivity issues

- Manually troubleshoot
- One-way data transmission
- Basic network checks
- Connection interferences

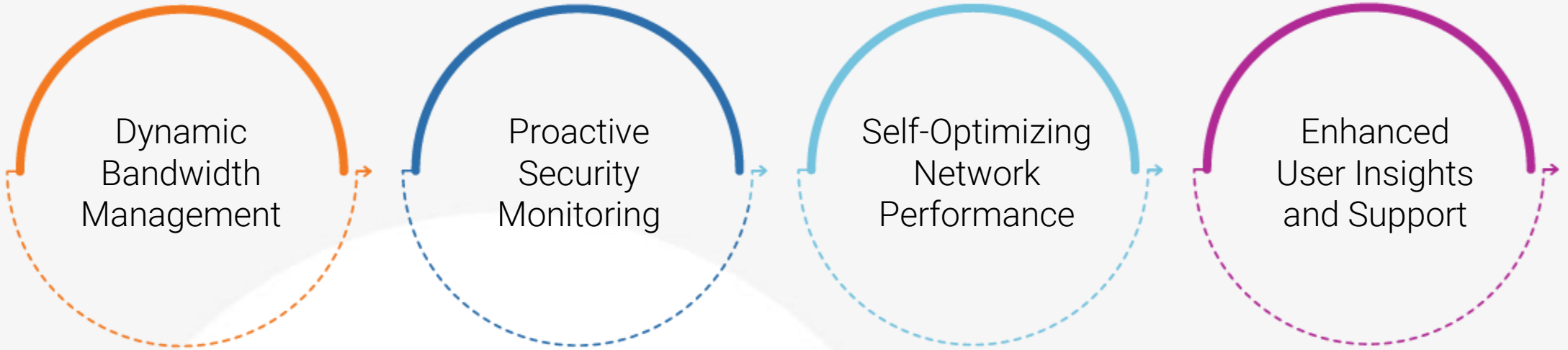
AI Driven = Proactive

Benefits of Friendly Wi-Fi Management

- Adapt in real-time
- Automated troubleshooting
- Predictive maintenance
- Enhanced reliability
- Improved customer satisfaction



The Future of Smarter Wi-Fi with AI



The Future: AI-Driven Wi-Fi and Friendly in Action

Data Collection and AI Analysis

- Predict Needs
- Detect Anomalies
- Optimize in Real-Time

Real-Time Self-Healing

- Automatically troubleshoot
- Seamless resolution

Enhanced User Insights

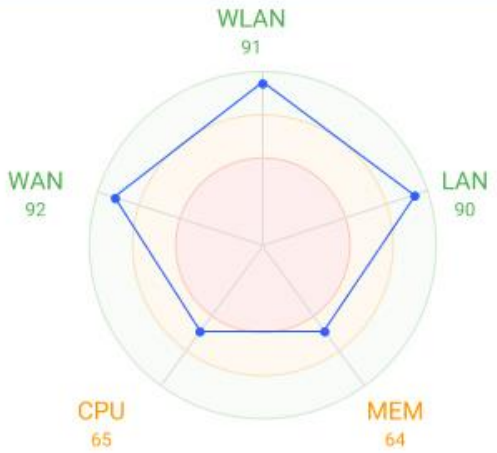
- Proactive recommendations
- User-friendly interaction

AI for Connected Home Optimization

- Tailored solutions for users' connected experience

Home Score

Home Score



Bad (0 – 33) Avg (33 – 67) Good (67 – 100)

User experience score: 81 Good

Home Score KPIs

KPI	Status	Suggested actions
WLAN	Good	
WAN	Good	
LAN	Good	
CPU	Avg	Multiple Actions
MEM	Avg	Multiple Actions

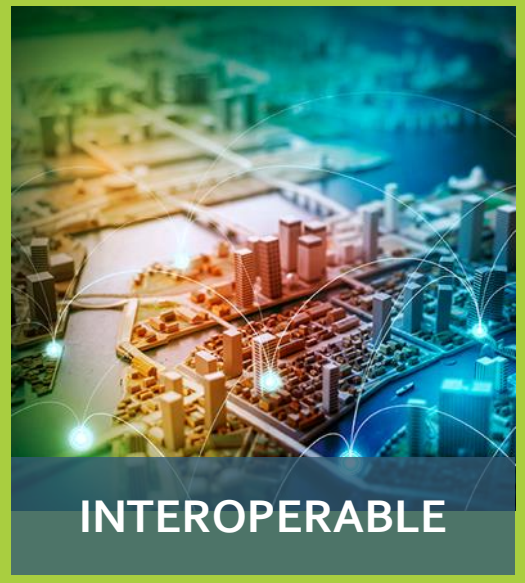
Thank You
For Your Time!

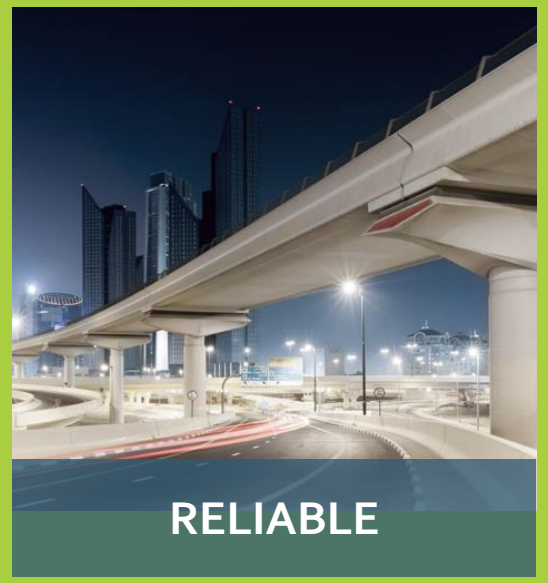
ofer.greenberg@friendly-tech.com

Wi-SUN Technology Overview
Broadband Forum - November 2024
Phil Beecher, President and CEO

Wi-SUN
Alliance Overview

What is Wi-SUN Alliance?





A global ecosystem of member companies seeking to accelerate the implementation of open standards-based Field Area Networks (FAN) and Internet of Things (IoT).

Wi-SUN Alliance was established in April 2012

- Incorporated as Not for Profit Organization (501c) in Delaware, US
- Regional representation in North America, Europe, India, Japan, Singapore
- Specification of wireless communications networks based on IEEE 802.15.4 Smart Utility Networks (SUN) PHYs and IETF ipv6 / 6lowpan for Field Area Networks (FAN), Home Area Networks (HAN) and other IoT
- Defines testing and certification programs for multi-vendor interoperable solutions for large scale IoT networks

About Wi-SUN Alliance

>300 members in 46 countries

Complete eco-system from silicon to solutions

Membership Levels

Promoter Membership

- Direct the activities of the organisation
- A seat on the Board of Directors
- Final approval of specifications

Contributor Membership

- Monitor and contribute to technical profile specifications and test specifications
- Input requirements to the certification program to ensure alignment with both currently deployed systems and future needs
- Attend member meetings and interoperability events
- Develop and certify interoperable products based on open standards
- Contribute to an eco-system of interoperable products

Adopter Membership

- Attend member meetings
- Participation in Alliance workshops and developers' conferences
- Approved use of Wi-SUN Alliance logo on promotional materials
- Access to Wi-SUN Alliance marketing collateral and e-newsletter
- Access to a world-class ecosystem of members

Observer Membership (Test Lab/Certification Body)

- Reserved for Test labs and certification bodies

>120 Million Wi-SUN Capable Endpoints Awarded Worldwide

– Navigant Research

>120 M

Guidehouse

Target Applications

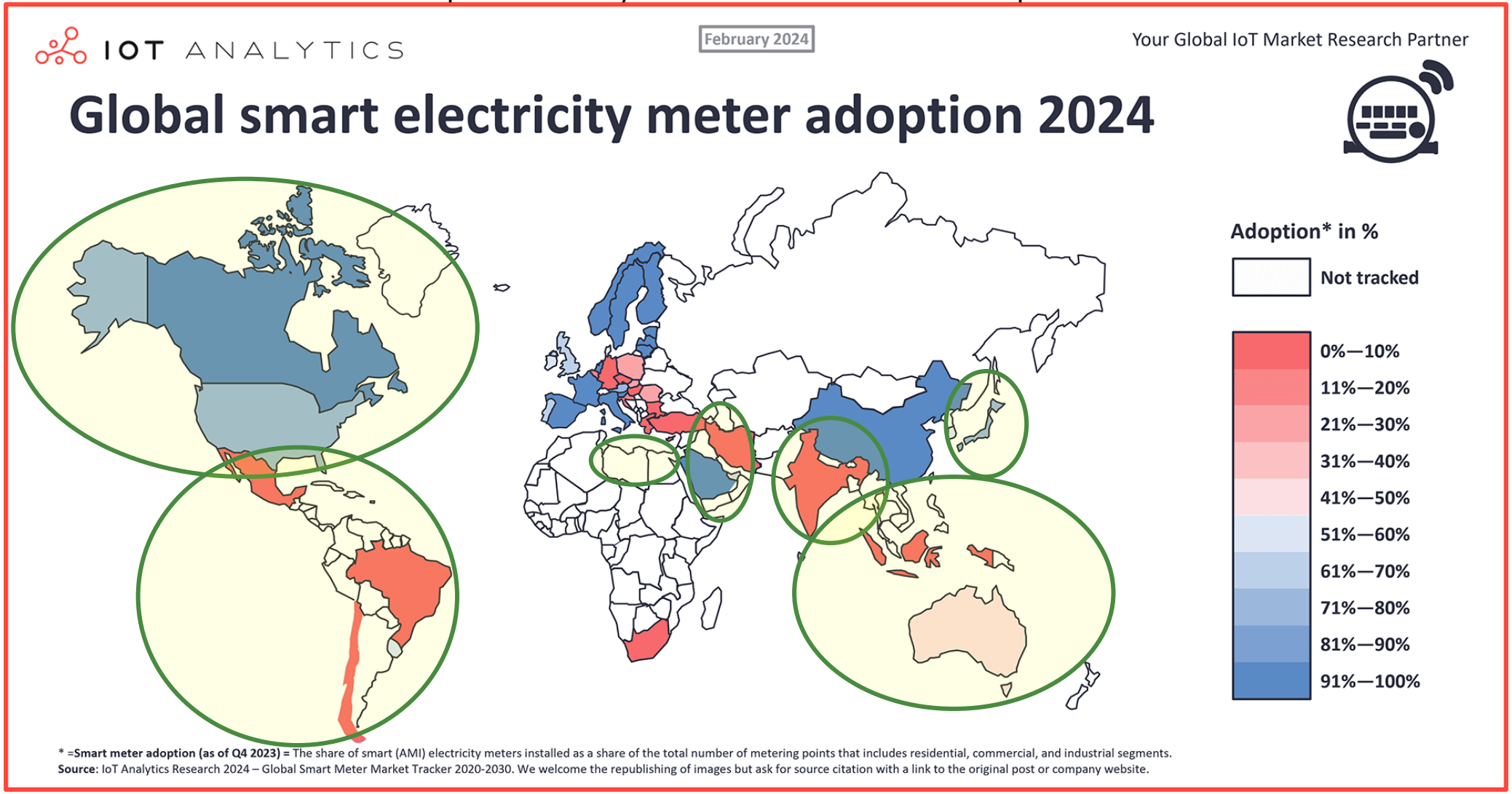
Wi-SUN technology supports large scale IoT applications including:

- ***Smart utilities***: Advanced Metering Infrastructure (AMI), Peak Load Management, Distribution Automation and Smart Metering, Water and Gas metering and infrastructure
- ***Smart cities***: Street lighting, infrastructure management, smart parking, environmental sensing, smart signs, traffic and transport systems
- ***Smart home***: in home displays, smart thermostats, air cond, heating, energy usage displays and health and well-being applications
- ***M2M***: Agriculture, structural health monitoring (e.g. bridges, buildings, etc.), monitoring and asset management

Global Smart Meter Adoption Research Data

Projected market size: 50 billion USD by 2030

https://iot-analytics.com/smart-meter-adoption/



Predominantly Wireless Mesh

Majority of existing deployments are IEEE802.15.4 SUN / Wi-SUN FAN 1.0

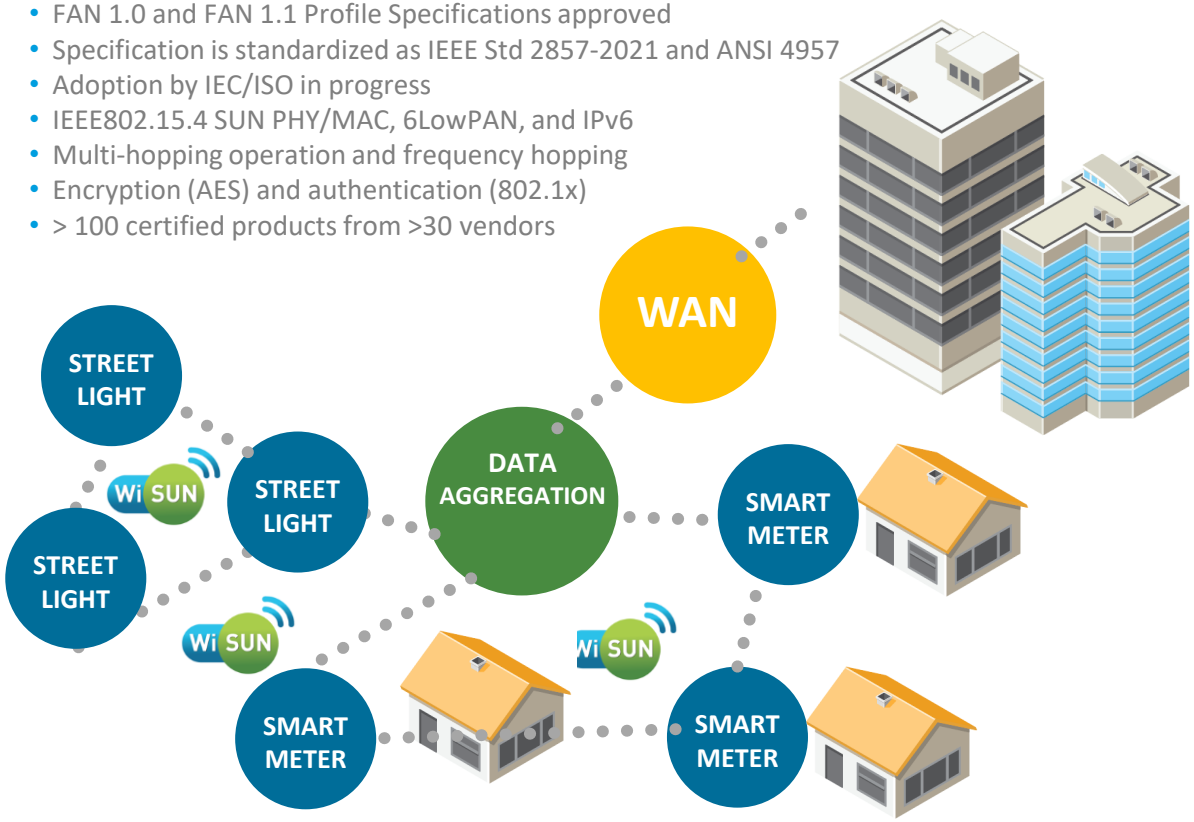
Majority of new deployments will be Wi-SUN FAN 1.0+ or FAN 1.1

Wi-SUN
Technical Profiles

Profile Specifications for Smart City/Utility Applications

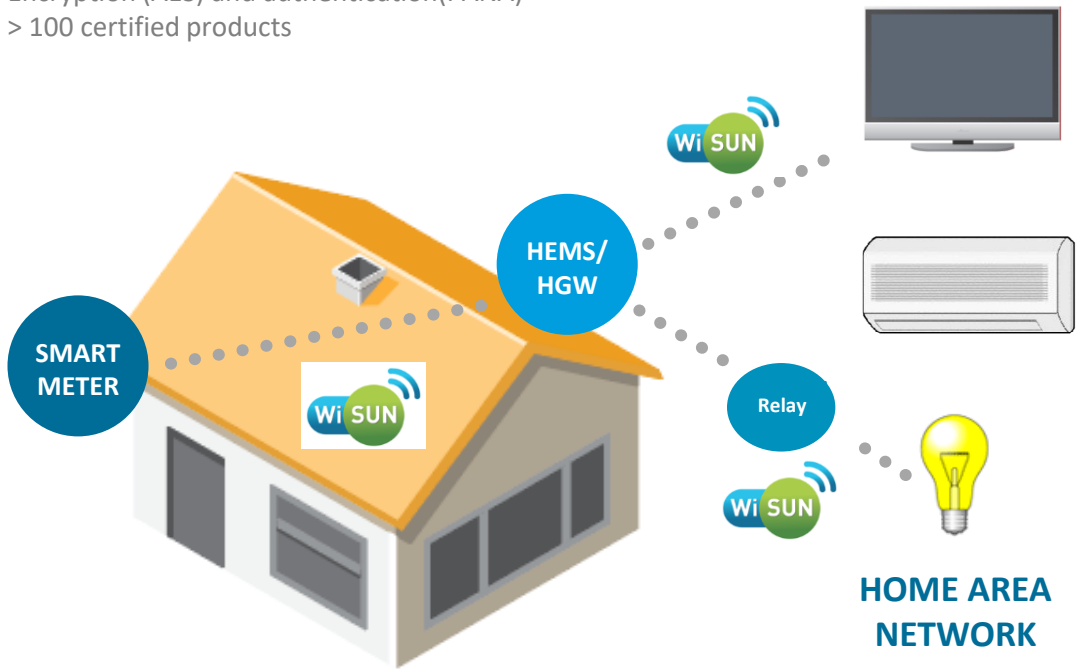
FIELD AREA NETWORK (FAN) Profile

- FAN 1.0 and FAN 1.1 Profile Specifications approved
- Specification is standardized as IEEE Std 2857-2021 and ANSI 4957
- Adoption by IEC/ISO in progress
- IEEE802.15.4 SUN PHY/MAC, 6LowPAN, and IPv6
- Multi-hopping operation and frequency hopping
- Encryption (AES) and authentication (802.1x)
- > 100 certified products from >30 vendors



HOME AREA NETWORK (HAN) Profile

- HAN profile Specification for Route B, HAN and Route IoT
- Specification is standardized as TTC JJ300.10
- IEEE802.15.4 SUN PHY/MAC, 6LowPAN, and IPv6
- Encryption (AES) and authentication(PANA)
- > 100 certified products



UTILITIES: Communication between Smart Meters and Distribution Automation equipment

TEPCO B-ROUTE: Communication between Smart Meters and HEMS

HAN: Communication between HEMS controller and HAN device

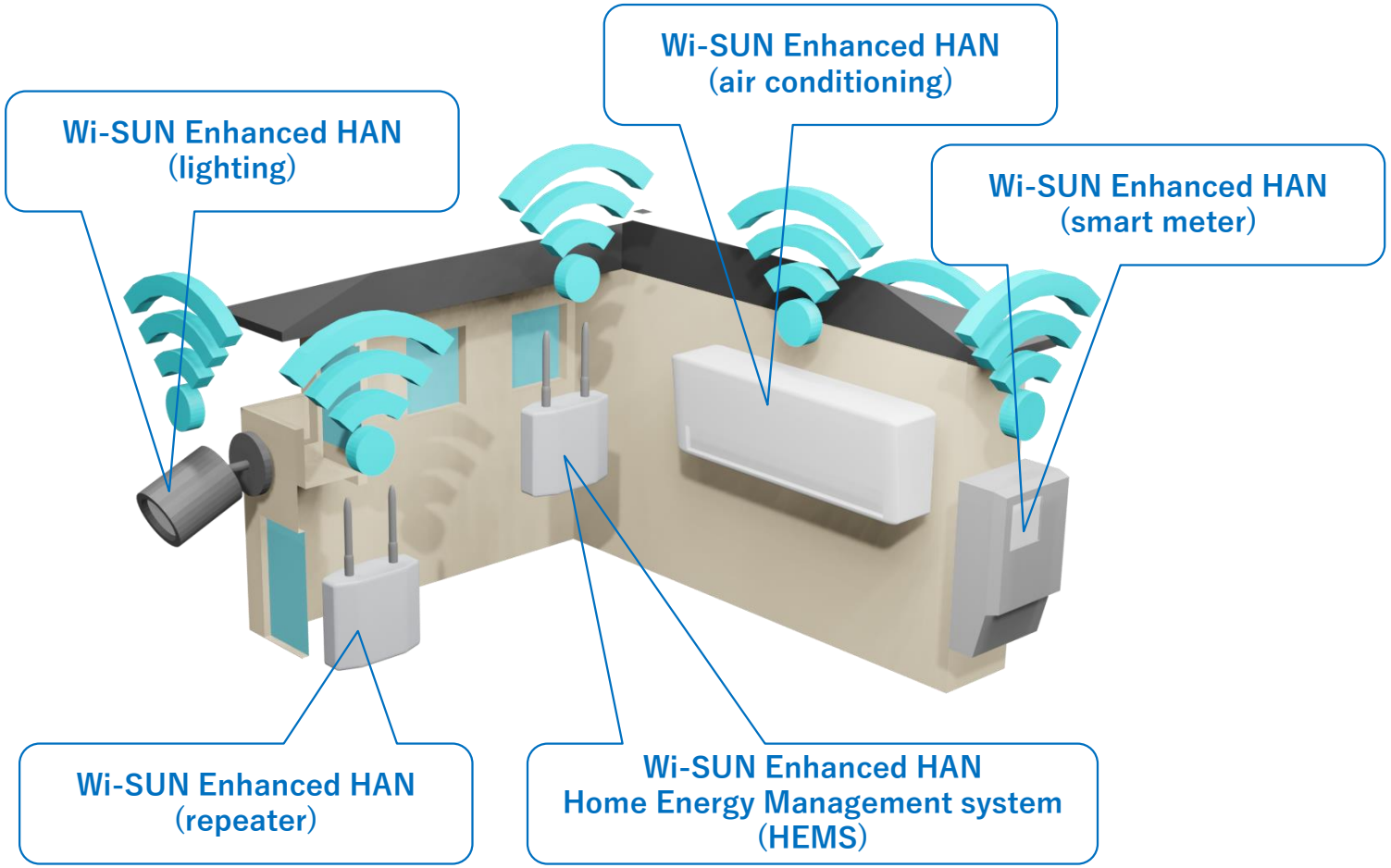
SMART CITIES: Communication between Streetlights, signage, parking, environmental sensors

IoT ROUTE : Multiservice network for Smart Meters and other devices

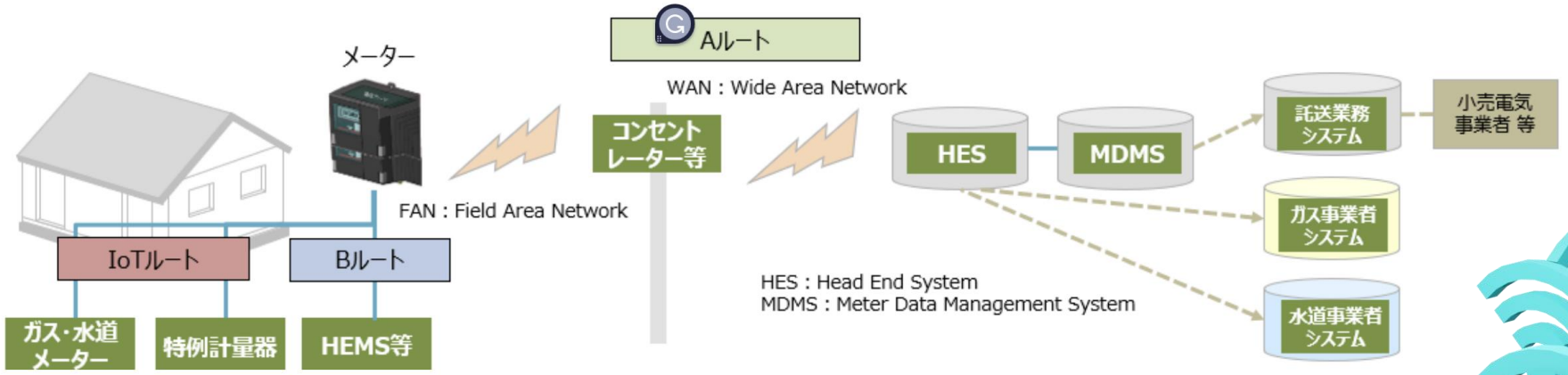
Wi-SUN HAN and IoT Route

Wi-SUN Enhanced HAN/”B” Route

Enhanced HAN： Enhancements to TEPCO “B” Route
Collaboration with Echonet Consortium for application layer



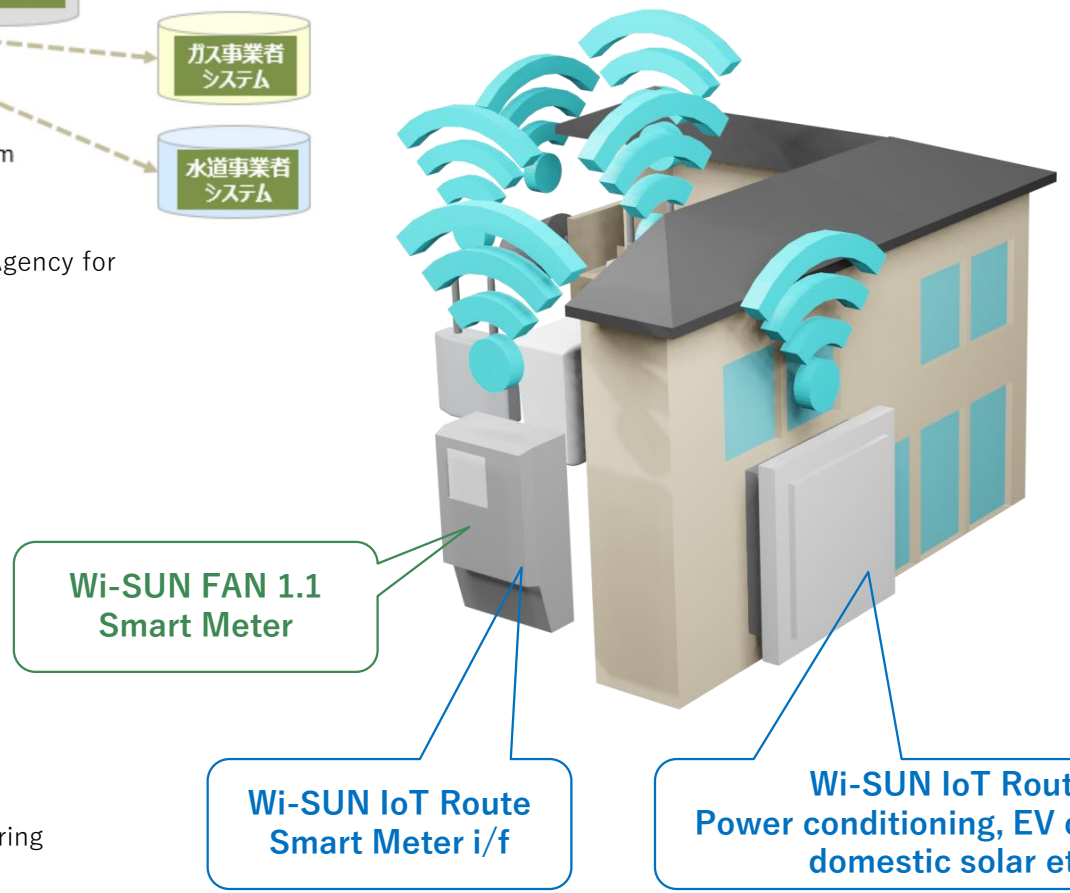
Wi-SUN Enhanced HAN/IoT Route、Wi-SUN FAN



Source: Next Generation Smart Meter System Review Committee Summary (Draft) (Agency for Natural Resources and Energy, Japan)

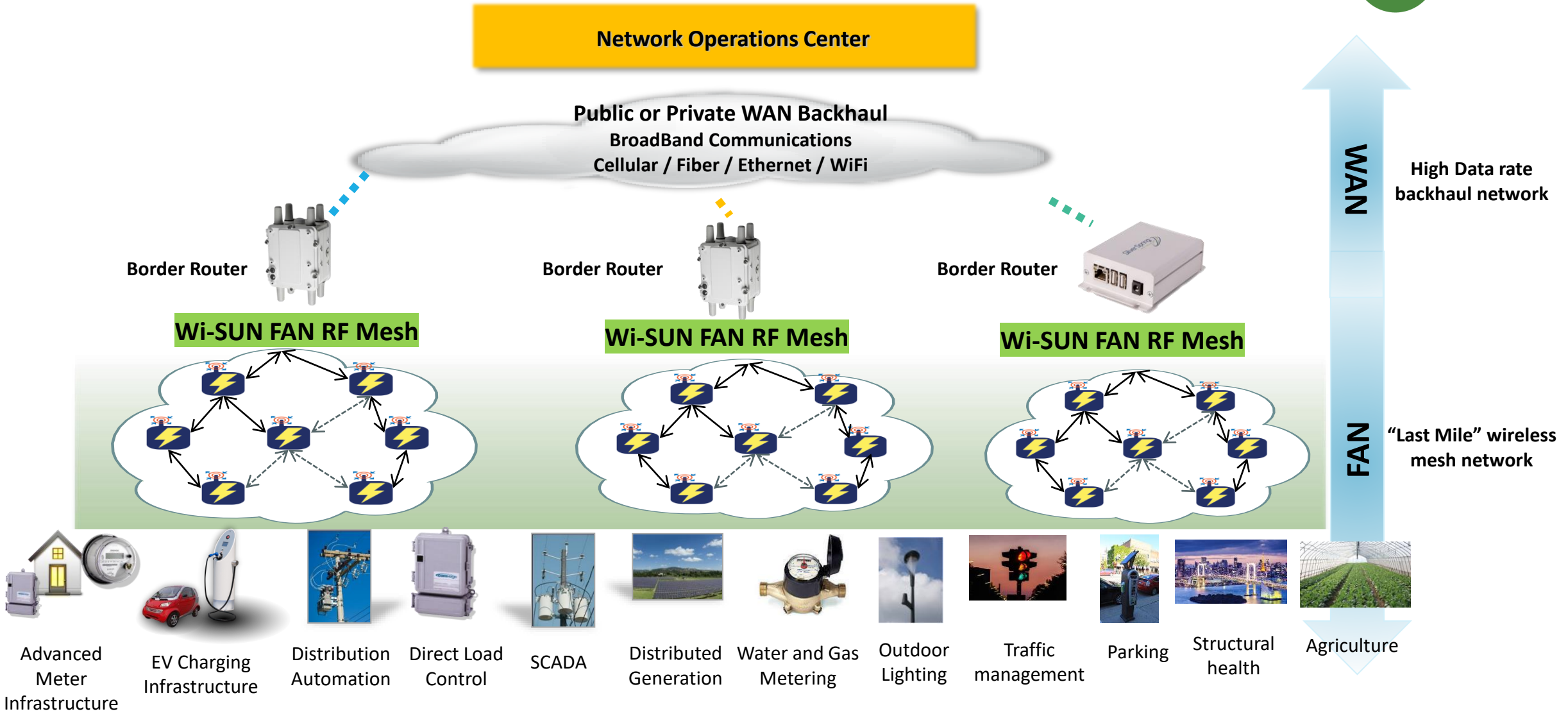
第７層	アプリケーション層	IoTアプリケーション（電文：DLMS／COSEM）
第６層	プレゼンテーション層	
第５層	セッション層	
第４層	トランスポート層	UDP
第３層	ネットワーク層	IPv6、ICMPv6
		6 LoWPAN
第２層	データリンク層	IEEE802.15.4
第１層	物理層	
無線方式		Wi-SUN Enhanced HAN

Source: Next Generation Smart Meter System Review Committee Document "Specific Metering (IoT Route) Operation Guidelines (Draft)"

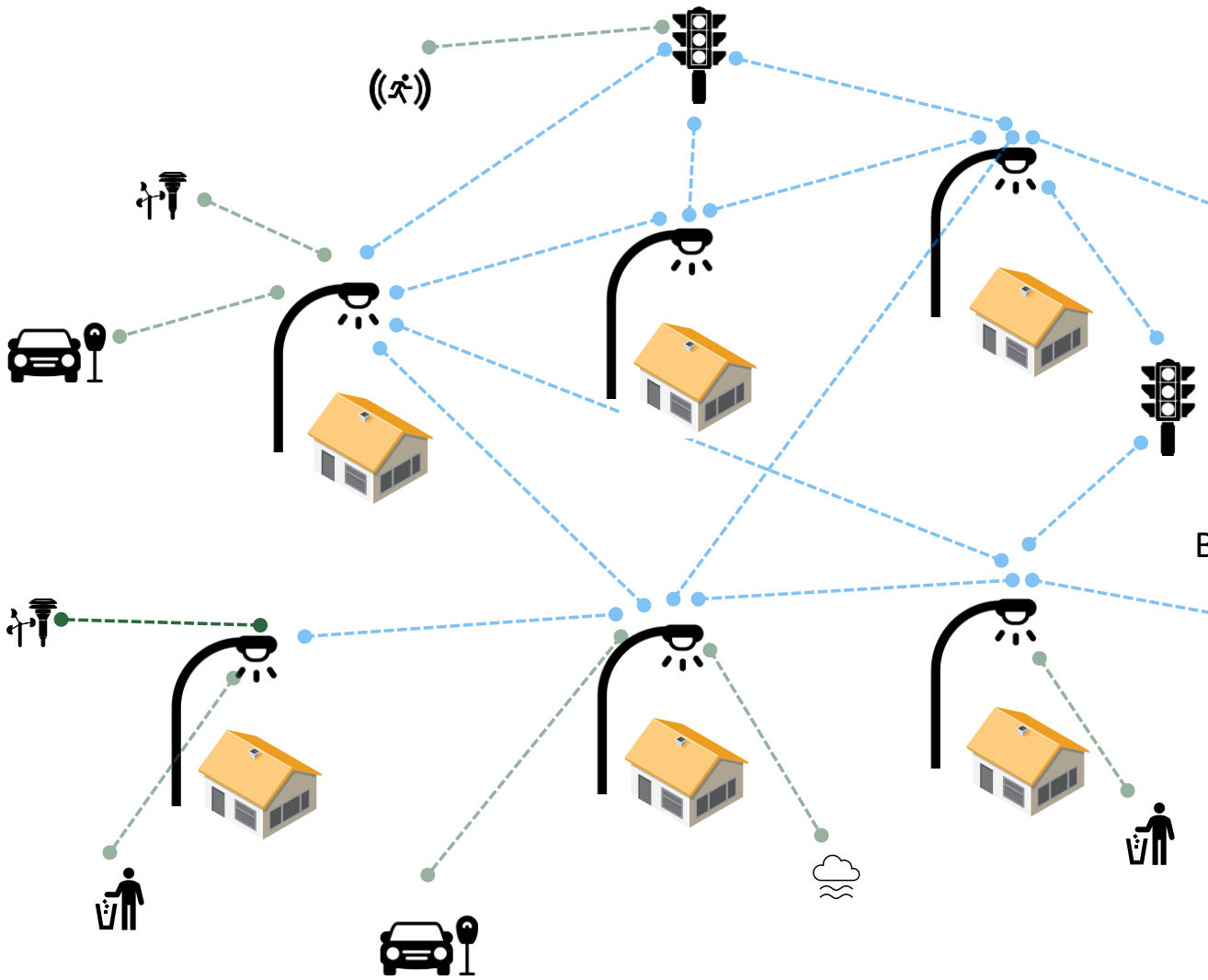


Wi-SUN Field Area Networks (FAN)

Wi-SUN FAN Use Cases

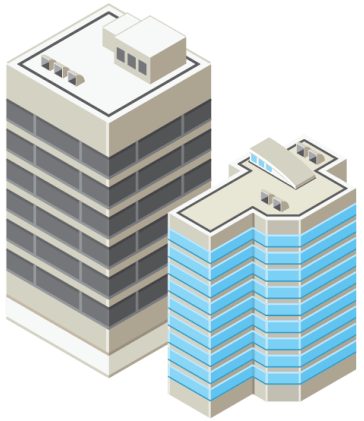


Mesh Network Topology in a Smart City



Local Authority / Municipality Back Office

Border Router



Broadband connection: e.g. cellular, fibre, ethernet

Border Router

- Install Smart Streetlights with Wi-SUN FAN comms
- Streetlights form a mesh network
- Install Wi-SUN FAN in traffic signals
- Traffic signals join the mesh
- Install battery devices e.g. trash cans, parking meters
- Low power devices connect as leaf nodes

Wi-SUN FAN Summary

- ***Radio Characteristics:***
  - Very low-cost radios
  - Symmetric radio link allows flexible network topology
  - Good performance in wide range of environments
  - Low power end nodes support 10-20 years battery life, and crystal aging
- ***Flexible Data rates and frequency hopping***
  - Optimal bandwidth utilization, even in dense networks
  - Resilient to interference
- ***Self forming / self healing mesh***:
  - Excellent coverage, even in challenging urban environments
  - Resilient to changing conditions (obstructions, faults etc)
- ***Security Architecture***
  - Robust authentication and encryption
  - Proven security protocols
- ***Open Standards***:
  - Globally available standards
  - Multiple vendors
  - Longevity of networks
- ***Testing and Certification***:
  - Multi-vendor interoperability
  - Supply chain resilience
  - Customer choice
  - Reduced time to market
- ***FAN Connectivity to Backhaul***:
  - Requires Broadband connection
  - Border Router connectivity using native ipv6

Standards and Industry Collaboration are key to success

- ***Open standards:*** Standards ensure security, promise multi-vendor interoperability, and speed up time-to-market of new devices and services.
- ***Importance of collaboration:*** Standards Development Organizations and Industry Alliances must work together to develop a clear roadmap for future network innovation.

For More Information

For more information or questions contact:

info@wi-sun.org
www.wi-sun.org

Follow us:

www.linkedin.com

Wi-SUN Alliance Group

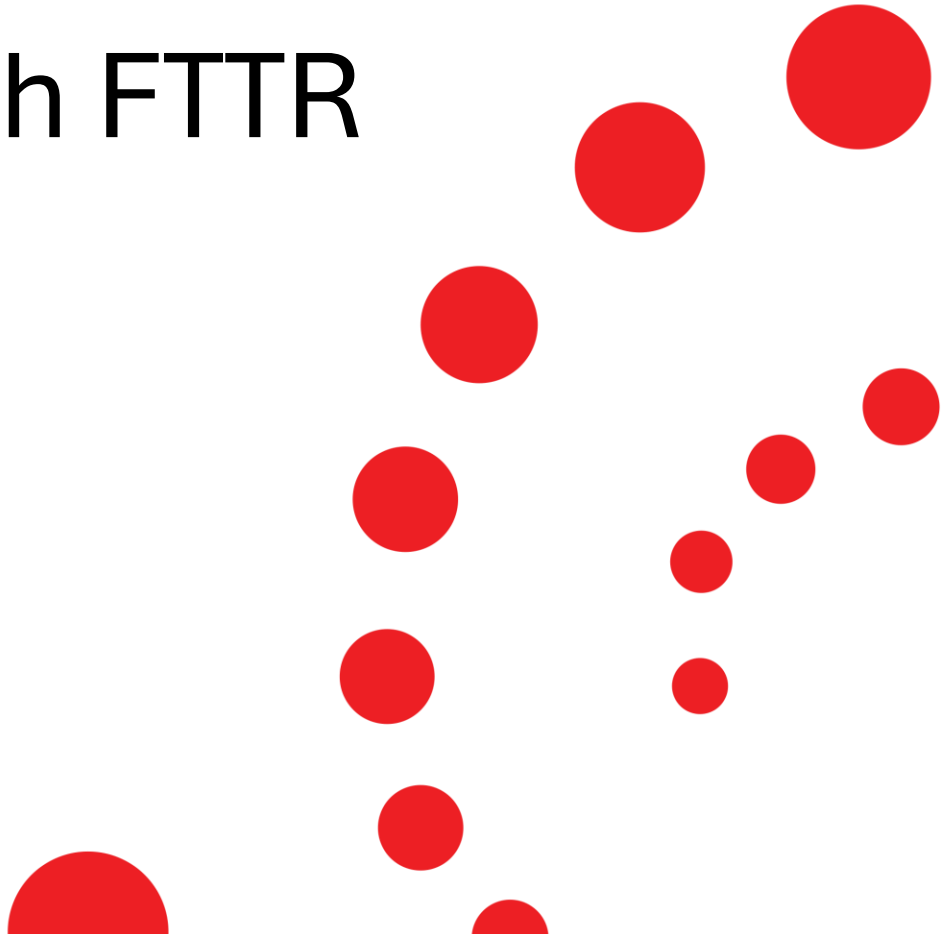
@WiSunAlliance

FUTUREWEI Technologies

Making the home smart with FTTR

Tom Starr

November 2024



FTTR (Fiber to the Room)
also known as (FIP) fiber in-premises

ITU-T FTTR Standards:

- **G.9940 FIP transceivers and architecture**
- **G.9941 FIP physical layer**
- **G.9942 FIP data link layer**
- **G.sup78 FIP for small business**
- **G.sup80 FIP for home application**

New Smart Home Requirements Call for Integration of FTTR and Smart Home Applications

Experience upgrade

Wi-Fi 2000M → 3000M, 8K naked-eye 3D/XR

Air interface latency 20 ms → 10 ms, cloud gaming

Device concurrency 128 → 256, IoT devices 5X↑ @ 2024

L2-1 experience → L2-2 experience

Intelligent upgrade

Smart home AI penetration rate 25% → 50% @ 2025

Separate cloud/local storage → converged cloud and local storage, with 400 million cloud disk users

Reactive response → proactive awareness, with 40 million home security service users

Smart product → Smart home

Ecosystem upgrade

Scattered smart home platforms → unified OS platform

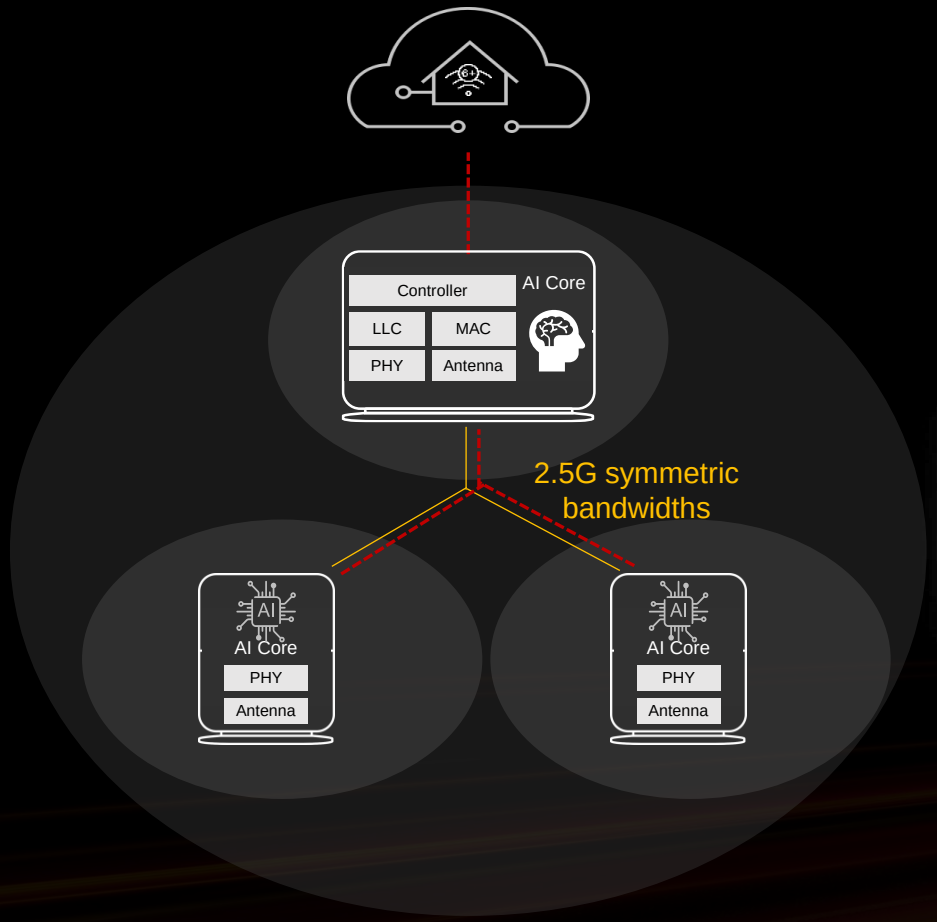
Multiple app entries → unified app

Time-consuming custom development → simplified delivery < 1 month

Separate → Interworking

Intelligent Connectivity Enabling Superior Experience

Optical +Wi-Fi Converged Architecture Delivers Optimal Performance



Optical +Wi-Fi Converged Architecture creates superior experience over one network

Collaborative scheduling of optical links and Wi-Fi through μs-level management channels to fully improve Wi-Fi performance

Ultra-high rate

2500 Mbps

Wi-Fi 6 → Wi-Fi 7

10 GB HD movie download within seconds

Seamless roaming

Zero packet loss

SRCN 1.0 → SRCN 2.0

Zero packet loss when users move at home

Ultra-low latency

10 ms

Innovative SDA latency assurance technology

8K/VR

Smooth running of 8K cloud VR and fast ticket booking

High concurrency

256

Multi-AP coordination and concurrency assurance technology

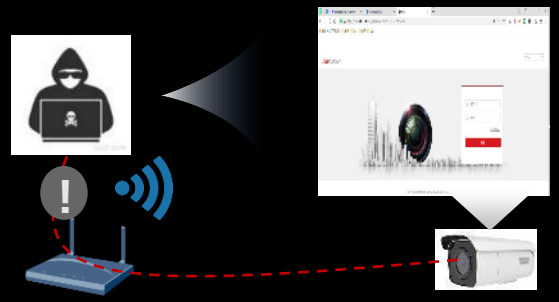
IoT

High-speed and stable running of smart home devices

IoT Coffer Builds High Home Security Protection for Smart Home service

User pain points

Hackers usually use home Wi-Fi network to scan device vulnerabilities to attack.

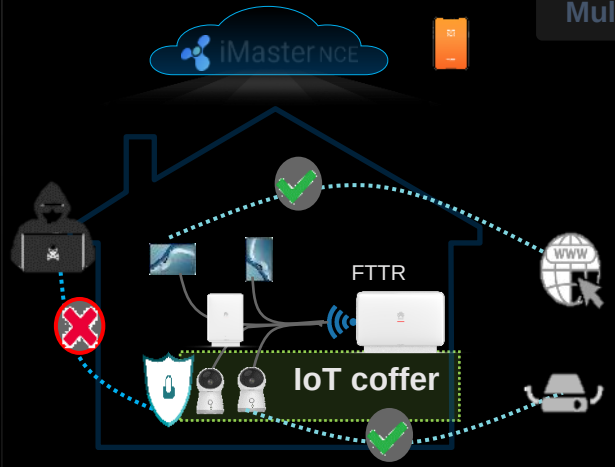


Hackers can directly open camera O&M web page after intrusion.

Home cameras are hacked frequently

Collaborative software and hardware protection, preventing privacy leakage

Multiple security protection modes



Message mode

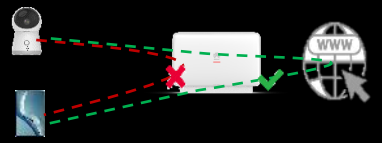
When a device on the FTTR LAN accesses a device in the IoT coffer, the app pushes a message to the user.

Security mode

When a device on the FTTR LAN accesses a device in the IoT coffer, if the access is unauthorized, the access is blocked and the app pushes a message to the user.

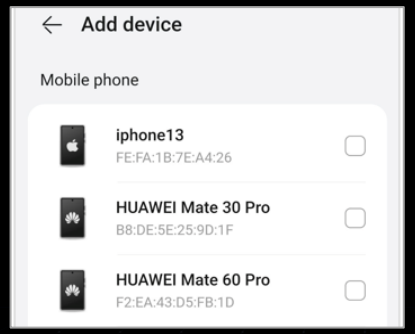
Isolation mode

Devices on the ONT LAN cannot access devices in the coffer.



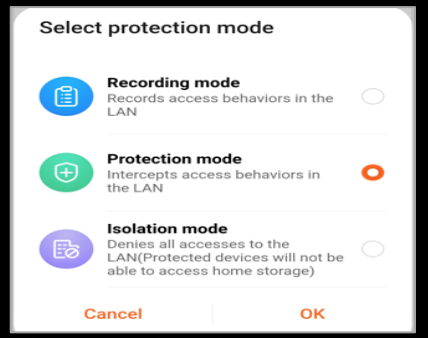
Easy app operations

Add to coffer in one click



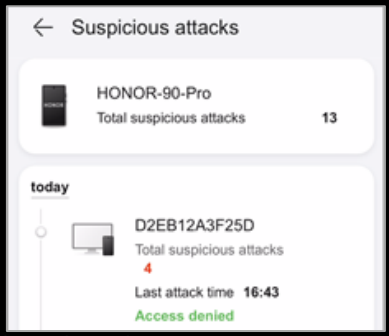
- Select devices and add them to the IoT coffer in the app.
- **Identified cameras are automatically added to the IoT coffer.**

Select a protection mode



- Multiple security protection modes

Protection records



- Detailed protection records are provided to identify possible attack sources.

Innovative Self-Bond Transparent Fiber Further Accelerates FTTR Deployment

Traditional: 40 minutes/information point

Difficult to deploy and inefficient

Messy and unreliable

15 minutes/ information point

Innovative self-bond transparent fiber

Free of tools, easy to use, and better looking

Innovative self-adhesive material

No wall surface flake-off and not easy to break or fall off

Ultra-thin transparent fiber + strong double-sided adhesive tape

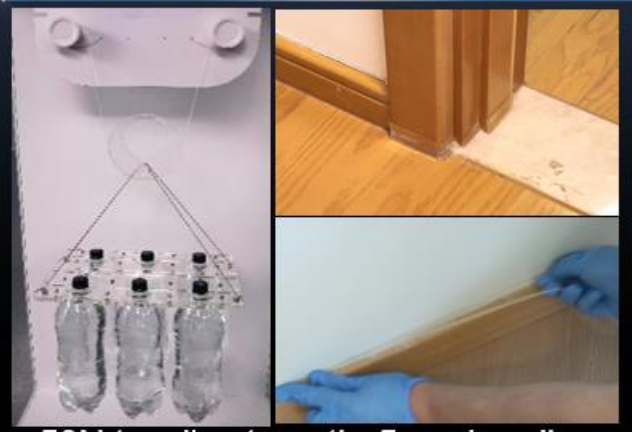
Self-bonding Transparent Fiber Support Fast Cabling in Building

(1) – Flame retardant

Continuous Innovation

Self-bonding transparent fiber

② High Strength Performance



50N tensile strength, 5mm bending

③ Quick Deployment

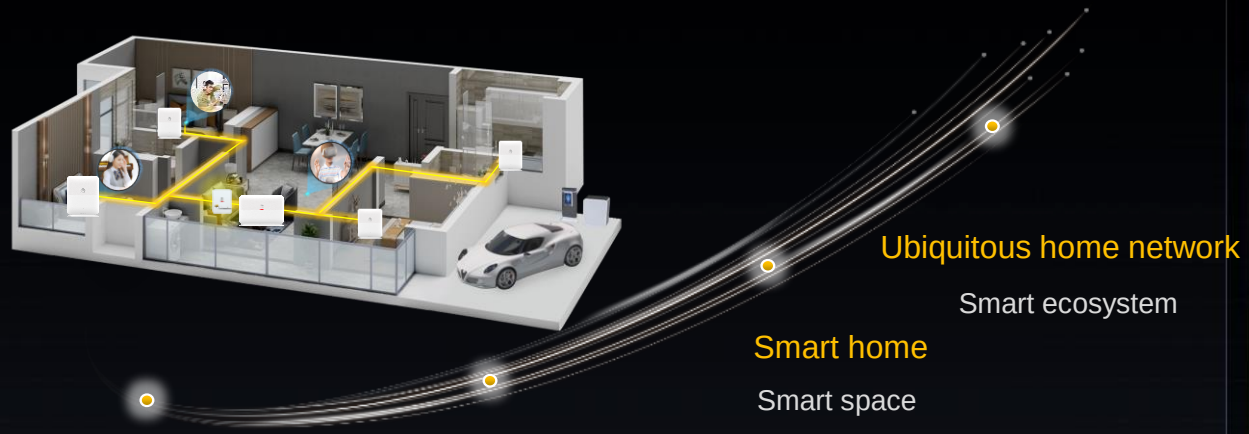
DIY installation

HB Unicom (China) Implements the Gigabit Smart City Development Strategy and Accelerates Home Digital Transformation

From one fiber to one home network

Development Objectives of 2023

100%	1.1 million	XXX K
Gigabit coverage	FTTR users	FTTR+X smart home services



One fiber
Gigabit acceleration

One home network
No FTTR, no gigabit

Smart home
Smart space

Ubiquitous home network
Smart ecosystem

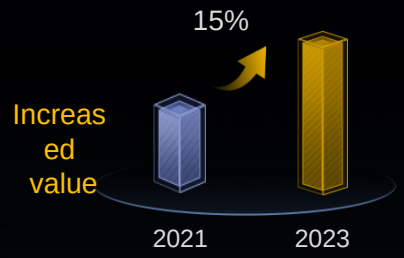
Foundation
F30 Convergent & multi-level products

Booster
Omni-channel & Digital marketing

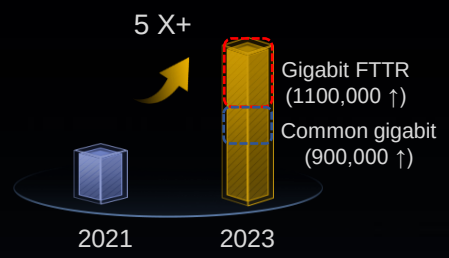
Core
Premium services & gigabit commitment

1.1 M FTTR users, No.1 in China

Revenue increase driven by FTTR



Gigabit user base promoted by FTTR



High package fulfillment rate in FTTR speed test

Customer satisfaction ↑ 0.6

No.1 in the industry

The NPS mechanism is used to evaluate satisfaction.

AIS (Thailand) Fiber Strategy:

Fastest growing fiber operator in Thailand

HBB users(AIS+3BB)

4.5 mn

households

First introducer of scenario-specific broadband

No. 1

Launched AI Powered gaming broadband in 2022

HBB service

77

Provinces

From one fiber to one smart home

Develop One Smart Home

Strengthen One Network

Accelerate One Fiber

FTTR service

1700subs/mth

Sales in All Cities

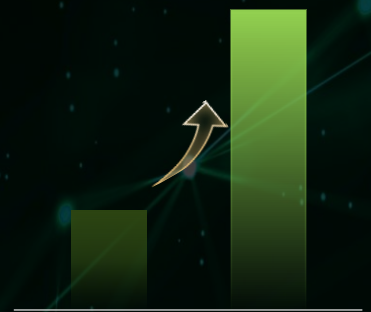
Home Network Challenges

Wi-Fi coverage and experience is poor

50%

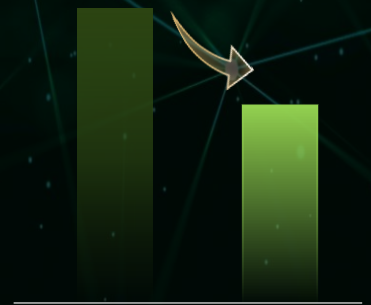
bandwidth suppression

Achievements: Greatly Improving User Experience in Gigabit and Digital home



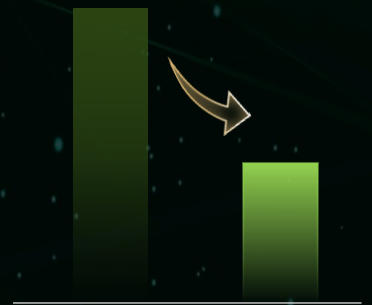
60%↑

Wi-Fi download speed



20%↓

Application Latency



40%↓

Packet loss rate

Case of Brazil Oi: the First Carrier with 1000+ FTTR users in Latin America

The best Wi-Fi experience with premium service

Value proposition will be delivered through the integration of product + caring + service

OI FIBRA X Strategy

OI FIBRA X PREMIUM

700M speed
1+1 FTTR points

600M speed
1+1 Wi-Fi mesh

Cost-effective FTTR package (>75m²)

Most satisfied fiber customers among major operators

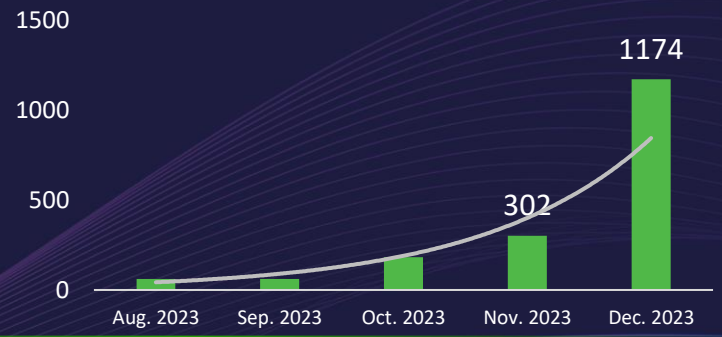
Lowest level of complaints among major operators

ANATEL
National Telecommunications Agency

Diversified **online and offline** marketing expansion

A NPS benchmark for Oi Fibra

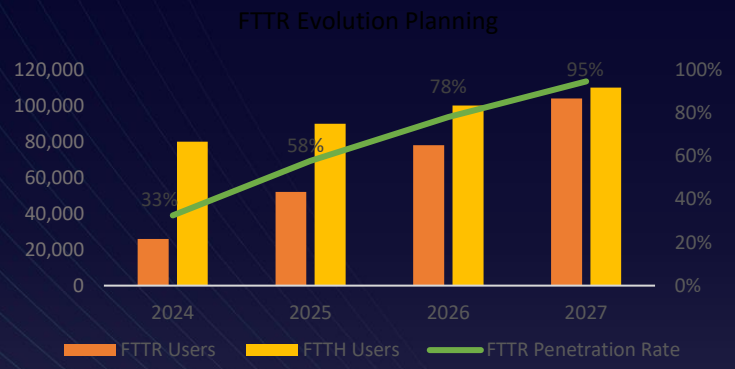
The number of reservation users exceeds 1000+.



FranceZEOP: Home Broadband Strategy: FTTR as NG ONT and Home Network for ALL Reunion Home and Users

FTTR is the evolution strategy of the next-generation ONT.

All the ONTs evolve to FTTR in 4 years



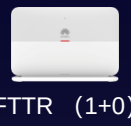
Advantage:

- FTTR as the next-generation hone networking technology, helps build **leading brand and competitive advantages**.
- Improve user acquisition and reduce the churn rate.

FTTR for ALL Broadband and Wi-Fi service

FTTR Package coverage rate: 100%

Contract Period



- Broadband connection and basic WiFi service

- Multi-Hotspot coverage, with WiFi Mesh/Ethernet Cable Mesh

- Fiber connection service is upgraded in need

Marketing Strategy:

- Step1: Seize the market by quick rollout and lightweight deployment
- Step2: Continuously improve ARPU through user operation
- Simplify the Branding, Package, Inventory Management, O&M.

FTTR with Digital Inclusion

Emmanuel ANDRE, CEO of ZEOP

"We decided to go on a large-scale business because we think that **everybody should be able to be eligible to FTTR**. So we decided to change our traditional plan to move to new plan with the same price but with a box FTTR ready. That's the first step of our strategy. "

- **100%** | All users can get a **FTTR ready** box
- **40%** | Users with coverage needs can ask for **more APs**
- **15%** | Users with higher demand on experience can get the **Fiber**

FTTR Enhances the Smart Home Experience

FTTR provides:

- Communication
- Local compute
- Local Storage
- Enhanced privacy and security
- Integrated optical+WiFi architecture
  - Higher speed
  - Lower latency
  - Reduced trouble rate

Smart Applications:

- Education
- Gaming
- Health
- Office
- Livestreaming
- Audio and video
- Security

broadband forum
Town Hall Innovation Series

Open Discussion across the Forum: Impact and Conclusions

John Blackford (BBF Chairman), Mauro Tilocca (Town Hall Innovation Series Co-Chair), Jason Walls (BBF BUS Work Area Co-Director)

Smart Home and IoT

Town Hall Innovation Series

Fall Member Meeting 2024

Town Hall Innovation Series